

MiVoice Business

Technician's Handbook

RELEASE 9.2

December 2021



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. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

®, ™ Trademark of Mitel Networks Corporation
© Copyright 2021, Mitel Networks Corporation
All rights reserved

Contents

Chapter: 1	Introduction	1
	About this guide	1
	What's new	1
	Intended audience	2
	Related Documents	2
	About the documentation set	3
	Mitel Product Documentation	3
	Product Bulletins	3
	Mitel Knowledge Base Articles	3
 Chapter: 2	 Getting Started	 4
	Documentation for Unsupported Controllers	4
	Migration	4
	Symbols Used in the Handbook	4
	Safety Instructions	4
	Start Here Guide	5
	What You Received	5
	3300 ICP Controller	5
	What You Need for Installation	5
	Preparation	6
	Initial Setup	6
	Install Hardware	6
	Install System Software	6
	Program System	6
	Maintain System	6
	Install and Replace Units	7
	About MiVoice Business Software	7
	Documentation - Mitel Document Center	7
	Access Your Mitel Options Password	7
	Contacting Mitel	8
	Order Desk	8
	Repair Services Department	8

Technical Support	8
-----------------------------	---

Chapter: 3	Initial Setup	9
	Overview	9
	Disk Drive Installation (3300 ICP Controller)	9
	Disk Installation on CX II /CXi II	9
	Disk Installation on MxIII/MxIII-L	10
	Connect PC to Controller	12
	PC Requirements	12
	Computer Recommendations	12
	Computer Requirements	12
	AX, MxIII/MxIII-L, CX II and CXi II Controller	12
	Establish Communication with Controller	13
	Power Up the Controller	13
	Set Network Configuration on 3300 ICP Controller with a New HDD	13
	Configure the Layer 2 Switch (MxIII, CXi II)	17
	Enable Licenses and Options	17
	3300 ICP System Requirements for AMC	18
	Automatic Sync via MiVB System Administration Tool	18
	Server Manager Requirements for Software Download-Blades	18
	Manual License and Options Entry	19
	Upgrade System to Required Software Version	19
	Verify the Operation of the Controller	19

Chapter: 4	Installation and Programming	20
	Install Hardware	20
	Determine Controller Module Configuration	20
	Identify Controller Component Options	23
	Remove Controller Cover	25
	Install Controller Modules	26
	MxIII/MxIII-L, CX II/CXi II	27
	AX	27
	Install Controller Stratum 3 Clock Module	28
	Install Controller Hardware	28
	Rack Mount the Controller	28
	MxIII/MxIII-L (Four-piece Bracket Installation)	28
	MxIII/MxIII-L (Two-piece Bracket Installation)	29
	AX	30
	CX II and CXi II	30
	Wall Mount the CX II/CXi II Controller	32
	CX II/CXi II	32
	Install Service Units and Cabinets	33
	Install Telephones	34
	Install Telephones, Consoles and Appliances	34
	Install Line Interface Modules	34

Register IP Devices from the Telephone	35
Install Music on Hold	36
Installing a DNIC Music on Hold/Paging Unit (DMP)	36
Program 5485 IP Paging Unit	37
Appendix-J Upgrade and Deploy VM	38
Upgrade applications on the same VM	38
Upgrading application by deploying a new VM	38
EX Controller Hardware Installation	44
Program System	44
Programming Tools	44
Log in to the Programming Tools	45
System Administration Tool	45
Server Manager	46
Mitel Integrated Configuration Wizard	46
IP Phone Analyzer	46
Program LS Trunk Settings via LS Measure Tool	46
LS Trunk Selection in the UK	46
Configure Analog Music On Hold (MOH)/Paging	47

Chapter: 5

Software Installation	48
Software installation on 3300 ICP controller	48
Install System Software using the Migration Tool	48
Install MiVB Software on a 3300 ICP Controller (Manually)	49
Install MiVB 9.0 or Later on a 3300 ICP Controller using HDD	55
Installation of the MiVoice Business Migration Tool	56
Overview	56
Procedure	56
DHCP Server Programming	56
Program the DHCP Server	56
Upgrade System Software (3300 ICP Controller)	56
Upgrading System Software: Notes, Tips, and Cautions	57
Upgrade Firmware of 3300 ICP Controllers	57
Change Number of IP User Licenses	57
Upgrading to more than 65,000 RDN users	58
Distributing New Firmware to IP Phones	58
Distributing Firmware to 69xx IP Phones	59
Load IP Phone Software Remotely	59
Downgrading to a Previous Software Release	59

Chapter: 6

Maintenance	60
Access 3300 ICP Controller Through the Maintenance Port	60
Determine 3300 ICP Controller Bootloader	60
Determine Last Known Active Partition using U-Boot	61
Overview	61
Before you Begin	62

Procedure62
Upgrade 3300 ICP Controller's Bootloader Without Using a Hard Disk .69	
Overview69
Before you Begin70
Contents of the Migrateflash.zip archive71
Setup71
Procedures72
Upgrade 3300 ICP Controller's Bootloader using the Migration Tool . 75	
Overview75
Before you Begin75
Procedure75
Configuring the Server using Server Console76
Overview76
Accessing Server Console77
Checking the server status80
Configuring the server80
Reboot or shut down the server81
Managing trusted networks82
Backing up the database82
Restoring a database83
Access the E2T Card console on MXe III/MXe III-L Controller85
Connect to the E2T Card console85
Connect through an SSH session of the RTC Card85
Connect through the Controller's Printer Port86
Disconnect from the E2T Card Console87
Disconnect from the E2T Card Console (RTC Card SSH Session) .87	
Disconnect from the E2T Card Console (Printer port)87
Modify Default Baud Rate of the System Console (3300 ICP Controller) .88	
Determine Bootloader of the E2T card88
Configure U-Boot Networking Parameters of the E2T Card89
DHCP89
Static IP89
Manually Upgrade E2T Card Bootloader from Bootrom to U-Boot91
Access the MIPS Console on MXe III Controllers96
Connect to the MIPS Console96
Disconnect from the MIPS Console97
Change IP Settings on 3300 ICP Controller97
Change IP Settings Of MiVoice Business System97
Change IP Settings of an Out-of-Service E2T Card97
Change IP Settings of an In-Service E2T Card97
Determine VLAN ID on Separate Subsystems99
Change VLAN ID for a 3300 ICP Controller	100
Recover the VLAN ID of a 3300 ICP Controller	101
Change IP Address of Internal L2 Switch (CXi II and MXe III Controller) 102	
Check System	102
Check Alarm State	102

Check System Health	103
Check Controller Hardware Profile	103
Maintain VoIP Security	104
Secure Sockets Layer (SSL) and Security Certificate	104
Securing Telnet Connections	104
Collect system Logs	106
View Maintenance or Software Logs	106
Collect System Logs	107
Collecting System Logs and Diagnostics Data	107
View Logs Remotely, TCP/IP Socket Numbers	107
View Login and Logout Audit Logs	108
Detect Device Moves for E911	108
Monitor Device Moves	108
Detecting Device Moves	111
Viewing Device Connectivity Logs	111
Analyze IP Phone Issues	111
Install the IP Phone Analyzer	111
Launch the IP Phone Analyzer	112
Enable Tool Analysis	112
Disable Tool Analysis	112
Disabling/Enabling Voice Encryption	112
Power Down the Controller	112
Perform a System Reset	113
Back Up a Database	113
Verifying if Anyone is Connected to the Voice Mail System	113
Database Verification and Backup Failure Notification	114
Verifying the Backup	114
Restore a Database	115
Logging in	115
Database Restore Procedure	115
Verify the Restore	115
Export Configuration Data	116
Import Configuration Data	116
Assign Static IP Addresses to IP Phones	117
Setting Static IP Addresses on Dual Mode Sets	117
Removing Static IP Addresses on the IP Sets	119
Providing Power Over Ethernet to Devices (CXi II)	120
Disabling the VLAN on Remote 53xx IP Phones	120
How to disable the VLAN on the 53xx Phone	120
Potential Effect/Impact on Upgrade to MCD 5.0 SP2	120
Troubleshooting Tips	121

Chapter: 7

Install and Replace Units	122
3300 ICP Controller Replacement	122
AX Controller Replacement	122
Replacing a CX II/CXi II or MXe III/MXe III-L Controller	122

Component Replacement Notes	123
Required Tools	123
Required Procedures	123
MXe III/MXe III-L	124
Accessing the MXe III/MXe III-L Carrier Board	124
Add or Replace Controller FRUs	127
Controller Modules	128
Adding or replacing controller modules	128
AX Controller	129
Controller Module Installation Notes	131
DSP Module	131
Dual Fiber Interface Module (FIM)	131
Echo Cancellor	131
Framers	131
Stratum 3 Clock Module	132
System i-Button/System ID Module	132
Analog Main Board	133
MXe III/MXe III-L	133
CX II/CXi II	134
Analog Option Board	135
CX II/CXi II	135
Configure Embedded Analog Boards	138
RTC Processor Card (MXe III/MXe III-L Controller)	139
Overview	139
Before you begin	139
Procedures	140
E2T Processor Card (MXe III/MXe III-L Controller)	142
Overview	142
Before you Begin	142
Procedure	142
Disk Drives (CX II/CXi II/MXe III/MXe III-L)	143
Disk Drive Replacement Overview	143
Disk Drive Replacement	143
CX II/CXi II (Single Hard Disk or Solid State Drive)	144
Replace a Single HDD or SSD in a CX II/CXi II Controller	144
MXe III/MXe III-L (Single Hard Disk or Solid State Drive)	145
Replace a Single HDD or SSD in an MXe III/MXe III-L Controller	145
MXe III/MXe III-L (Two disk drives in RAID Configuration)	147
Replace one disk drive in an MXe III/MXe III-L	147
Replace both disk drives in an MXe III/MXe III-L	148
Upgrade Software After Disk Drive Replacement	148
Overview	148
New Replacement Drive with MiVB 7.2 SP2 Software	149
Used Replacement Drive with Pre-9.0 Software	150
Used Replacement Drive with MiVB 9.0 or Later Software	151
Fan Complex	152

MXe III/MXe III-L	152
AX	153
CX II/CXi II	153
Power Supply Unit	154
MXe III/MXe III-L, AX	154
ASU II	155
Redundant Power Supply	155
AX, MXe III/MXe III-L	155
RAID Controllers	155
MXe III/MXe III-L	156
Line Cards	159
AX	159
ASU II	159
Controller Card (AX)	159
Before you begin	159
To replace the AX controller card	160
Compact Flash Cards (AX)	162
Before you begin	162
To replace a 16 GB Compact Flash Card in the AX:	162
Memory Module (AX, CX II, CXI II, MXe III)	164
Install Cabinet FRUs	167

Chapter: 8

Appendix A: Hardware Reference	168
System Configurations	168
Controller Hardware Details	168
Controller Components	168
Controller Cabinet Numbering	172
T1/E1 Combo Card	172
Dual T1/E1 Framer	175
Quad BRI Framer	175
RJ-45 Pin Orientation	176
Analog Board (CX II/CXi II and MXe III/MXe III-L Controllers)	176
Line Cards (AX Controller)	178
Controller Alarm Port Pinouts	178
Controller Remote Alarm Behavior	179
Analog Services Unit	179
5485 IP Paging Unit	186

Chapter: 9

Appendix B: Installation Planner	188
Reserved IP Addresses	188
Controller Configuration Settings (RTC)	189
System Administration Tool Settings	189
IP Phone Settings	189
Telephone Programming Guide	189
Increasing DSP Resources	190

About the DSP II Module	191
MXe III/MXe III-L Controller - DSP Resources	191
CX II/CXI II Configurations - DSP Resources	193
DSP Notes	194

Chapter: 10

Appendix C : Typical Network Configurations	196
Network Configuration Examples	196
DHCP Server Settings	196
DHCP Server Settings	196
Configuration 1: One DHCP Server per VLAN	197
Layer 2 Switch Settings (Example)	198
Configuration 2: One DHCP Server for Two VLANs	199
Layer 2 Switch Settings (Example)	200
Configuration 3: Router on a Stick	200
Layer 2 Switch Settings (Example)	201
LLDP-MED and IP Phone Network Policy	201
Cisco Discovery Protocol (CDP)	201
CXi/CXi II/MXe III Server Configuration	201
Firewall/Port Forwarding	201
PPTP Remote Access	202
WAN Settings (Internet Gateway)	202
Configuration B: MXe III/MXe III-L Typical Voice-Only Network	203
AX Configuration Procedures	204
AX Typical Voice-Only Network	204
AX Typical Voice and Data Network	205
CXi II, MXe III/MXe III-L and AX-Specific Guidelines	206
CXi II, MXe III/MXe III-L and AX VLAN Behavior	206
Implementing a Voice-Only Network	208
MXe III/AX/CXi II IP Settings	208
Implementing a Voice and Data Network	208
Using a CXi II ICP	208
Using an MXe III or AX ICP	210
CXi II and MXe III Configuration Requirements	211
Installing External Layer 2 Switches	211
Voice Only Networks	211
Voice and Data Networks	213
Windows 2000 FTP Server	214

Chapter: 11

Appendix D: Status LEDs	218
Overview	218
Controller LEDs	218
Controller Alarm LEDs (AX, MXe III/MXe III-L)	220
.	220
Controller Power LED (AX, MXe III/MXe III-L, CX II/CXi II)	220
Hard Drive or Flash Activity	221

RAID Controller	221
MXe III/MXe III-L	221
FIM	222
LAN Ethernet Ports	223
CIM, Embedded and Quad MMC	223
Controller Alarm	224
Power Supply Unit LEDs	225
Dual T1/E1 Framer Module	225
T1/E1 Combo Card	226
Quad BRI Framer Module	228
Analog Services Unit LEDs	229
Universal ASU, ASU, and ASU II CIM Status LEDs	230
Analog Services Unit II Alarm LED	230
Analog Services Unit II Activity LED	230
ASU II Card LEDs	231
ASU II ONS and Combo Card Alarm LED	231
ASU II ONS Card Activity LED	231
ASU II Combo Card Activity LED	231
IP Device LEDs	231
Peripheral Cabinet LEDs	232
Peripheral Cabinet FIM	232
In-Line Power Unit LEDs	233
AC Power	234
Power Unit Alarm	234
Power Unit Port Status	234

Chapter: 12 Appendix E: FRU Part Numbers 236

Hardware Part Numbers	236
Software Part Numbers	238

Chapter: 13 Appendix F: System Capacity and Parameters 239

Port Usage	239
Encryption Support	240
IP Set Features	241
IP Phone Power Consumption	242
Capacity	242
Hardware Capacity	242
System Capacity	244

Chapter: 14 Appendix G: MSPLogClient Installation and Configuration 248

About the MSPLogClient	248
Installation	248
Other Useful Commands	248
Installation	249
Configuration	249

	Log Location and Format	250
	LOCATION	250
	Format	250
	Definitions	251
Chapter: 15	Appendix H: Configure New/Used Controllers and Storage Devices .252	
	Greenfield Installations	252
	Installation for MXe III, MXe III-L, CX II and CXi II Controllers . .	252
	Installation for AX Controllers	254
	Controller Replacement	254
	Hard Disk Replacement	255
	AX Compact Flash Card Replacement	256
	RTC Card Replacement	256
	E2T Card Replacement	257
Chapter: 16	Set up an HTTP/HTTPS Server and a Custom Repository258	
	Before you begin	258
	Installing IIS	259
	Setting up an HTTP Repository	261
Chapter: 17	Set up a TFTP server and a custom repository268	

Introduction

About this guide

This handbook provides certified MiVoice Business technicians with instructions to install, upgrade, maintain and troubleshoot Mitel[®] MiVoice Business software and supported controllers. For information on programming, please refer to the System Administration Tool Help system.

What's new

Table 1.1: Issue 1.0 (Sheet 1 of 2)

Feature/Enhancement	Document Updates	Location
MiWalkThru information.	Included MiWalkThru information in the section Log Into the Programming Tools with the URL details.	MiWalkThru
HTTP server setup update.	Updated the section Set up an HTTP Server and a Custom Repository with the HTTPS support	Set up an HTTP/HTTPS Server and a Custom Repository
System Capacity and Parameters "Port Usage" section update.	Updated the port number for the function - PDA, Application communication to "3998".	Appendix F: System Capacity and Parameters
Updated the MIPS Console section.	Removed the Mx III-L reference in the MIPS Console section and updated the 3300 ICP Controller Replacement stating "Follow the instructions in KMS article S05142 for more information."	Access the MIPS Console on Mx III Controllers 3300 ICP Controller Replacement
Updated the Securing Telnet Connections	Removed the obsolete commands "serviceCloseAll, serviceOpenall, and setServiceTrustedIP" in the Securing Telnet Connection section.	Securing Telnet Connections
"Root certificate" update post database restore.	Added a note to describe the "root certificate update" during the software upgrade.	Upgrade System Software (3300 ICP Controller)

Table 1.1: Issue 1.0 (Continued) (Sheet 2 of 2)

Feature/Enhancement	Document Updates	Location
“Deploy the MPA Probe manually” after the MiVB upgrade.	Added a note to “deploy the MPA Probe manually” after the MiVB upgrade to ensure that the MPA will get back to its current status after the MiVB upgrade.	Install MiVB Software on a 3300 ICP Controller (Manually)

Intended audience

This guide is intended for certified MiVoice Business technicians who plan, install, configure, and upgrade MiVoice Business software on a 3300 ICP controller.

Related Documents

Document Title	Description	Location
MiVoice Business Migration Tool Help	Provides instructions to use the MiVoice Business Migration Tool to perform migration.	Available with the MiVoice Business Migration Tool. You can download the tool from the Downloads page on Mitel MiAccess .
MiVoice Business Hardware Technical Reference Manual	Provides technical information for Mitel® 3300 IP Communications Platform (ICP) hardware and supported peripherals. It covers hardware descriptions, specifications, and signaling parameters. This manual is intended for use by qualified technicians and system engineers planning an installation of the 3300 ICP system.	Document Center
MiVoice Business Migration Guidelines	Provides guidelines for preparing and migrating your MiVoice Business system to MiVoice Business Release 9.0 or later.	Document Center

About the documentation set

Mitel Product Documentation

To access the product documentation follow the steps:

1. Go to www.mitel.com.
2. Click **SUPPORT**.
3. On the left panel under **Customer Support**, click **Technical Documentation**.
4. Click **BUSINESS PHONE SYSTEMS > MIVOICE BUSINESS**.

Product Bulletins

To access Mitel Product Bulletins follow the steps:

1. Log on to the [Mitel MiAccess](#) Portal.
2. In the left pane, click **InfoChannel**.
3. In the select **InfoChannel** list, select **Mitel-Worldwide**.
4. In the left pane, click **Product Bulletins & Announcements**.

Mitel Knowledge Base Articles

To access Mitel Knowledge Base Article follow the steps:

1. Log on to the [Mitel MiAccess](#) Portal.
2. In the left pane, click **Knowledge Management System**.

Getting Started

This chapter describes the information required for getting started with the installation of 3300 ICP controllers or an EX controller.

Documentation for Unsupported Controllers

This document covers controllers supported by MiVoice Business Release 9.0 or later. For controllers, such as MX, CX, CXi, Mx, Mx-II 100-, 250-, and 700-user controllers, that are not covered here, refer to earlier versions of the *Technician's Handbook*.

Migration

For instructions on how to migrate a system that is running releases prior to Release 9.0, see the *MiVoice Business Migration Guidelines* document.

Symbols Used in the Handbook

NOTE: Provides important details.

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.

Safety Instructions

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

CAUTION: Read the safety instructions before performing the procedures in this handbook.

CAUTION: Failure to follow all instructions may result in improper equipment operation and/or risk of electrical shock. Refer to "3300 ICP 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.

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.

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

CAUTION: ISDN BRI Interface is not available in Taiwan. Use of this interface is prohibited.

CAUTION: When sold in Taiwan, the MxIII/MxIII-L Controller supports ISDN T1/E1 and Leased Line T1. However, it does not support Leased Line E1 and BRI in Taiwan.



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

3300 ICP Controller

- 3300 ICP Controller
 - Set of feet and rack mounting hardware
- Hardware Components
 - Hard drive (different for each of the controllers: MxIII/MxIII-L and CX II/CXi II) or Compact Flash Card(s) (AX only) ordered separately
- MiVoice Business Release 7.2 SP2/9.1 Software (see [Appendix E: FRU Part Numbers](#) for part numbers)
 - CX II, and CXi II: Provided on separately ordered data storage device
 - AX: Provided on separately ordered compact flash
 - MxIII: Provided on separately ordered data storage device
 - MxIII-L: MiVoice Business Release 9.1 provided on separately ordered storage device
- Optional Hardware, such as:
 - RAID Hardware and hard drives (2 nos.) (HDD or SSD)
 - Redundant Power Supply
 - ASU

What You Need for Installation

- Phillips screwdrivers
- Anti-static strap
- CAT 5 or better cable with RJ-45 connector
- Computer for configuring the MiVoice Business software
- IP addresses for the controller, E2T, and IP telephones
- List of purchased options and password

Preparation

- Review your purchase order
- Complete [Appendix B: Installation Planner](#)
- Review [Appendix C: Typical Network Configurations](#)

Initial Setup

- [Disk Drive Installation \(3300 ICP Controller\)](#)
- [Connect PC to Controller](#)
- [Establish Communication with Controller](#)
- [Enable Licenses and Options](#)

Install Hardware

- [Determine Controller Module Configuration](#)
- [Identify Controller Component Options](#)
- [Remove Controller Cover](#)
- [Install Controller Modules](#)
- [Install Controller Stratum 3 Clock Module](#)
- [Install Controller Hardware](#)
- [Rack Mount the Controller](#)
- [Install Service Units and Cabinets](#)
- [Install Telephones](#)
 - [Register IP Devices from the Telephone](#)
- [Install Music on Hold](#)

Install System Software

- Install the System Software:
 - [Software installation on 3300 ICP controller](#)
- Upgrade system software:
 - [Upgrade System Software \(3300 ICP Controller\)](#)

Program System

- [Log in to the Programming Tools](#)
- [Program LS Trunk Settings via LS Measure Tool](#)
- [Configure Analog Music On Hold \(MOH\)/Paging](#)

Maintain System

- [Back up a database](#)

- 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.
- [Export Configuration Data](#)
- [Import Configuration Data](#)
- [Assign static IP addresses to IP Phones](#)
- [Collect System Logs](#)
- [Detecting Device Moves](#)
- [Load IP Phone Software Remotely](#)
- [Assign static IP addresses to IP Phones](#)
- [Perform a System Reset](#)
- [Restore a Database](#)
- [Troubleshooting Tips](#)

Install and Replace Units

- [Add or Replace Controller FRUs](#)

About MiVoice Business Software

The 3300 ICP is a Voice over IP solution that runs MiVoice Business software to deliver robust call control, extensive features and support for a wide range of desktop devices and applications for medium-to-large enterprises. There are several system configurations:

- the CX II with embedded analog
- the CXi II with embedded analog and embedded Layer 2 switch for sites with 8-100 lines (150 on CXi II);
- the MXe III/MXe III-L base with embedded analog supports 300 users before expansion;
- the expanded MXe III/MXe III-L supports 1400 users;
- the AX controller delivers an increased density of analog devices;

Documentation - Mitel Document Center

For customer documentation, including Knowledge Base Articles, on all Mitel products go to the [Document Center](#).

TIP: You must have a Mitel Online (MOL) account to access technical documentation on the Mitel Document Center. Access to end-user documents, such as telephone user guides, does not require an MOL account.

Access Your Mitel Options Password

You must obtain your Mitel Options Password through Mitel Online (www.mitel.com). You will create your application record on the AMC via Mitel Online (see [Enable Licenses and Options](#)). This password is required during a software upgrade or installation procedure. A new password has been issued to you if you are purchasing new options.

Mitel recommends using online synchronization with the AMC to update your password. Using online synchronization will allow you to license your controller software and options immediately. Remember to print a record of your options for future reference.

If you do not have internet access where your controller is located:

Connect to AMC at Mitel Online and choose the manual licensing option. When you print your options page, it will include your password and Applications Record ID (ARID). Use this password when installing the options on your controller.

To upgrade software, confirm a current password, or purchase new options and receive a new password, use the AMC at Mitel Online any time.

Contacting Mitel

Order Desk

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

Repair Services Department

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

If you are in North America, you can reach the Repair Services Department at 1-888-222-6483.

If you are in any other region, contact your local regional support service.

Technical Support

Please contact Mitel Technical Support if you require technical assistance.

If you cannot resolve the problem by using the *3300 ICP Troubleshooting Guide*, please collect the required information listed in the applicable section(s) of the guide **before** calling Mitel Technical Support.

If you are in North America, you can reach Technical Support at 1-800-722-1301 or 1-613-592-2122.

If you are in any other region, contact your local regional support service. For regional contact information, follow the “Contact Us” link under “Support” at www.mitel.com.

Initial Setup

This chapter describes the initial setup information required prior to installation.

Overview

The storage device (see [What You Received](#)) shipped from Mitel may have either MiVoice Business 7.2 SP2 or MiVoice Business 9.1 software installed.

The controller (see [What You Received](#)) shipped from Mitel may have either U-Boot or Bootrom as its bootloader (see [Determine 3300 ICP Controller Bootloader](#)).

The initial setup procedures described in this chapter is applicable only to 3300 ICP controllers with U-Boot and a brand-new Hard Disk Drive (HDD)/Solid State Drive (SSD) with MiVoice Business Release 9.1.

To see the initial setup procedures for all other possible combinations of controller and hard disk components (example, a controller with Bootrom and hard disk with MiVoice Business Release 9.1), see [Appendix H: Configure New/Used Controllers and Storage Devices](#).

After you have performed the initial setup procedures described in this chapter (or Appendix H), continue with [Installation and Programming](#).

Disk Drive Installation (3300 ICP Controller)

This section describes the procedure to physically install a disk drive into a 3300 ICP controller.

Disk Installation on CX II /CXI II

NOTE: Read the Safety Instructions before performing the disk installation procedure.

To install a disk drive into a new CX II or CXi II controller:

1. Remove the controller cover.
2. Remove the two screws securing the mounting bracket.

3. Secure the new drive to the mounting bracket, and tighten the two screws into place; see (1) in the figure below.

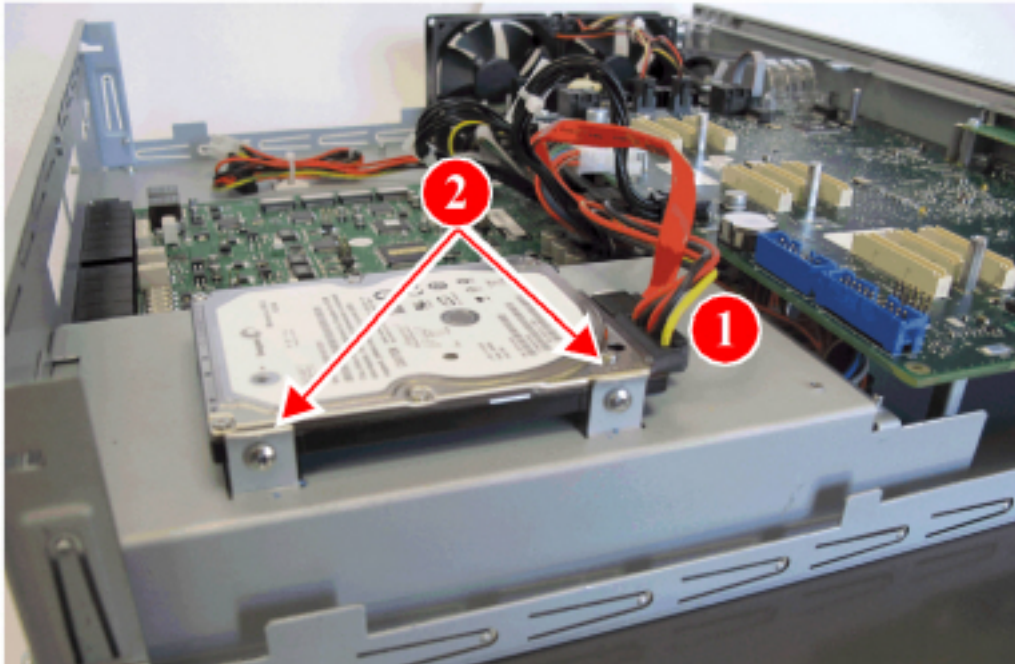


Figure 3.1: CX II/CXi II Hardware Installation

4. Connect the power cable and data cable to the drive; see (2) in the figure above.
5. Replace the controller cover.

Disk Installation on MXe III/MXe III-L

NOTE: Read the Safety Instructions before performing the disk installation procedure.

To install a disk drive into a new MXe III/MXe III-L controller for the first time:

1. Release the retaining screw securing the bottom drive carrier (HD1) to the controller, and remove the carrier.
2. Place the carrier and drive on a level and stable surface. Slide the replacement drive into the drive carrier:

- Initially, loosely install the top two screw.

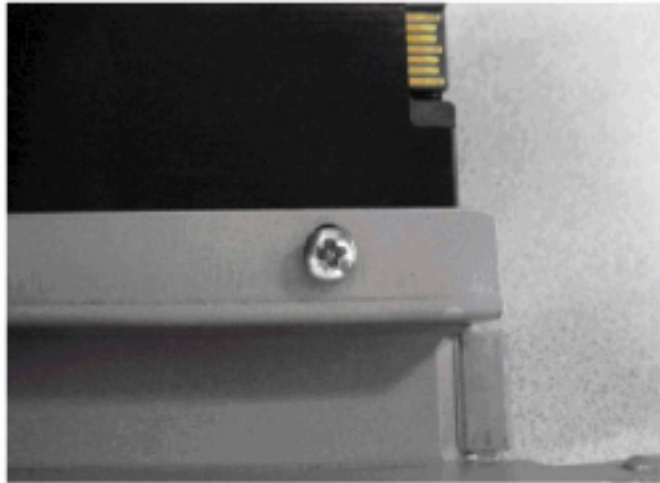


Figure 3.2: Drive Top Mount Screw

- Ensure that the drive is correctly oriented (i.e right side up).



Figure 3.3: HDD/SSD Installed in Drive Carrier

- Install and tighten both side mount screws.

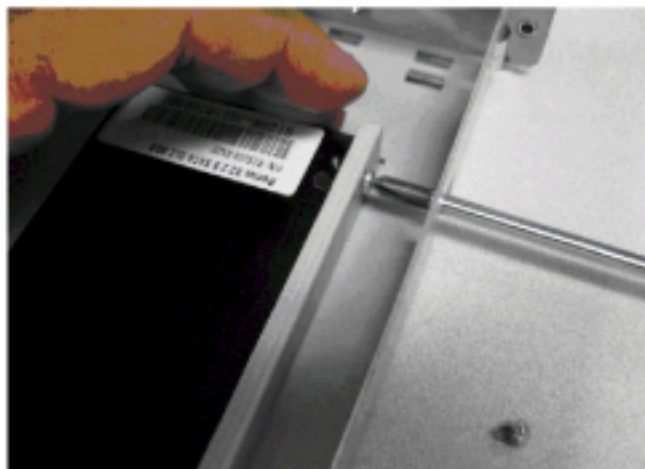


Figure 3.4: Drive Side Mount Screw

- Tighten both drive top mount screws, taking care not to twist or bend the mounting frame.

3. Push to seat the drive into the backplane.
4. Tighten the captive screw.

Connect PC to Controller

To configure the system, you must connect a PC to the controller using a serial cable (applies to 3300 ICP controller only).

NOTE: Remove the serial cable from the controller's end if the communications program on the PC is not in use, or if the cable is disconnected from the PC.

PC Requirements

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

Computer Recommendations

- A Microsoft® Windows® Vista (Business or Ultimate), Windows 7 (Professional, Ultimate, or Enterprise), Windows 8 or 8.1, or Windows 10 operating system with Mozilla Firefox 36.0.4 or later, Google Chrome 59 or later, Microsoft Edge 38 or later.
- 2GHz processor (minimum)
- RAM: 3300 ICP controller: 2GB (minimum)

Computer Requirements

- Network interface card (NIC)
- 1GB free disk space (minimum)
- Internet browser:
 - MiVoice Business 9.1 supports Google Chrome 59 or later, Mozilla Firefox 36.0.4 or later, and Microsoft Edge 38 or later.
 - JRE (Java Run-time Environment) 1.6.0_1 or later installed
 - VT100™ emulator program
 - Enable NetBIOS over TCP/IP
 - 7-Zip compression software (required during debugging)

AX, Mx III/Mx III-L, CX II and CXi II 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 PC's network interface card (NIC) to the port listed in the table below for the controller you want to connect to:

Controller	Ethernet port
AX	Port 1 or 2 of 10/100 LAN port
CX II	10/100 LAN Port
CXi II	10/100/1G LAN Port
MXe III	Port 1 of 10/100/1G LAN Port
MXe III-L	Port 1 of 10/100 LAN Port

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**

Establish Communication with Controller

Power 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. Turn on power switch. If there are two power supplies, ensure that both power switches are turned on. The controller starts up.

Set Network Configuration on 3300 ICP Controller with a New HDD

The **Bootstrap Console** is used to set the network configuration for a 3300 ICP controller (with U-Boot) that has a brand-new hard disk.

The Bootstrap Console is a variant of the Server Console that is only available through a controller's Maintenance port. It is used to initialize the network and database of a 3300 ICP server.

The Bootstrap Console opens only when the system software runs for the first time, that is, after you have:

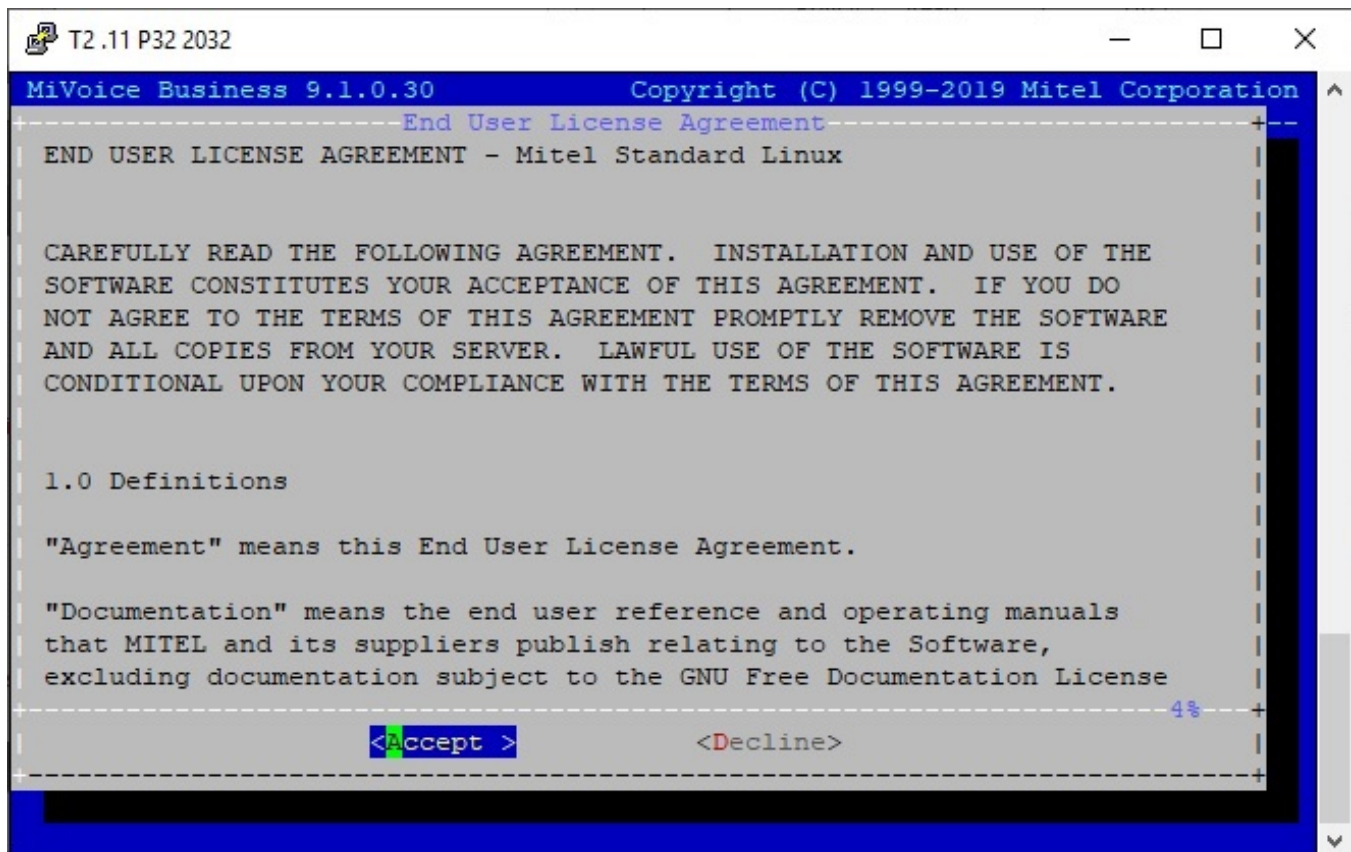
- installed a brand-new disk with MiVoice Business software Release 9.1 or later on a CX II or MXe III/MXe III-L controller; that is, you did not use the Migration Tool to upgrade the controller to 9.0 or later.
- installed a brand-new 16 GB Compact Flash card with MiVB 9.1 or later on an AX controller; that is, you did not use the Migration Tool to upgrade the controller to 9.1 or later.
- performed a full manual install of MiVoice Business Release 9.0 or later on a supported 3300 ICP Controller.

NOTE: The Bootstrap Console is applicable only to MiVoice Business Release 9.0 or later on a 3300 ICP Controller.

Procedure

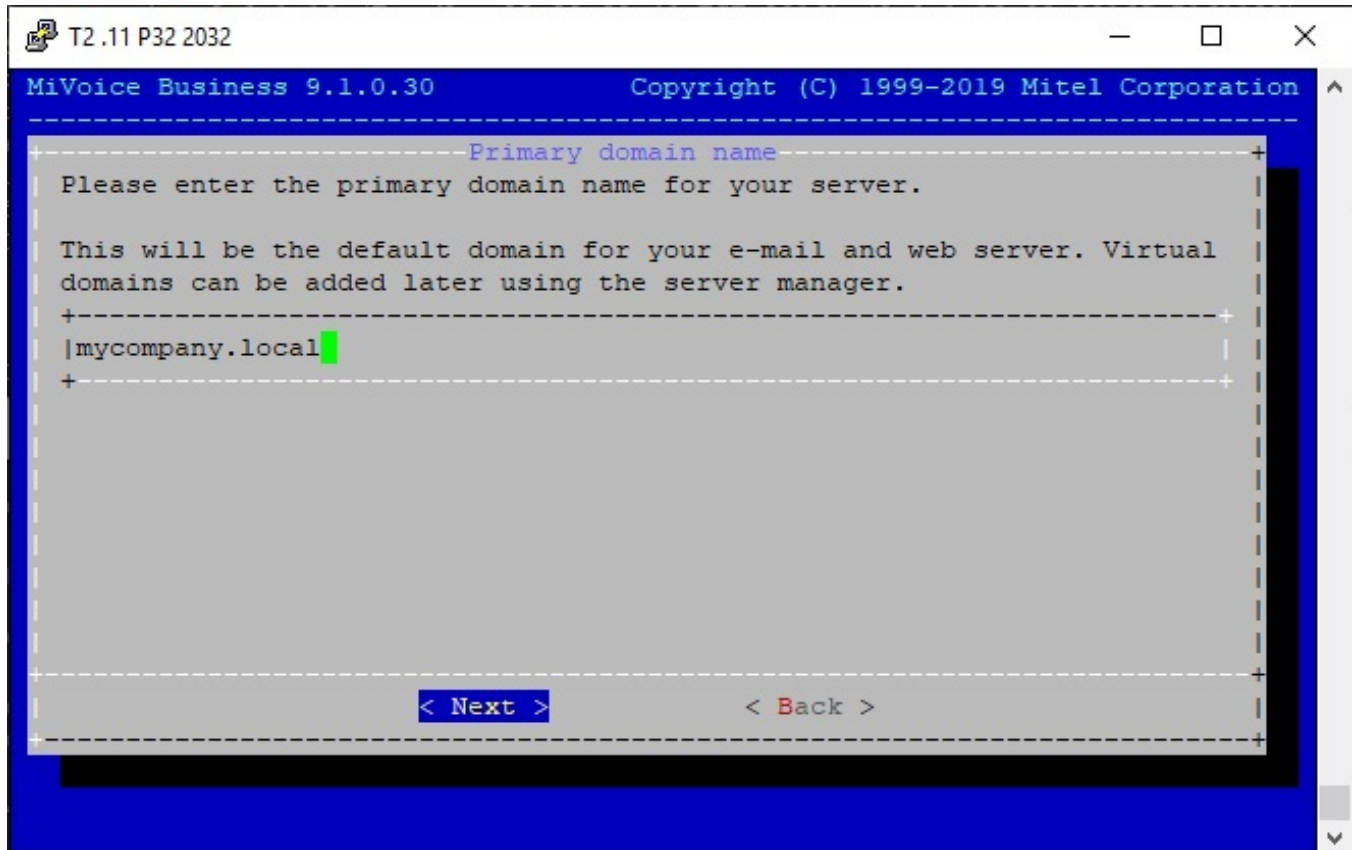
1. If you installed a brand-new hard disk drive on a 3300 ICP controller, do not power up the controller. [Access 3300 ICP Controller Through the Maintenance Port](#), and then power up the controller. Observe the output on the Maintenance Port.
If you are performing a full manual install of MiVoice Business Release 9.0 or later (9.1 or later on an AX controller), the installer reboots the system after initial install is completed. Observe the output on the Maintenance Port.
2. The End User License Agreement (EULA) screen is displayed in the communication application. Read the entire EULA text; if you agree with it, select **Accept** to proceed to the next step.

NOTE: If text indicating the status of services that are starting overlaps with the Accept/Decline buttons, press the ESC key twice to initiate a screen refresh. The screen refresh goes through an error screen with a **Next** button, but do not click it. This screen times out in 5 seconds and displays the original EULA screen.

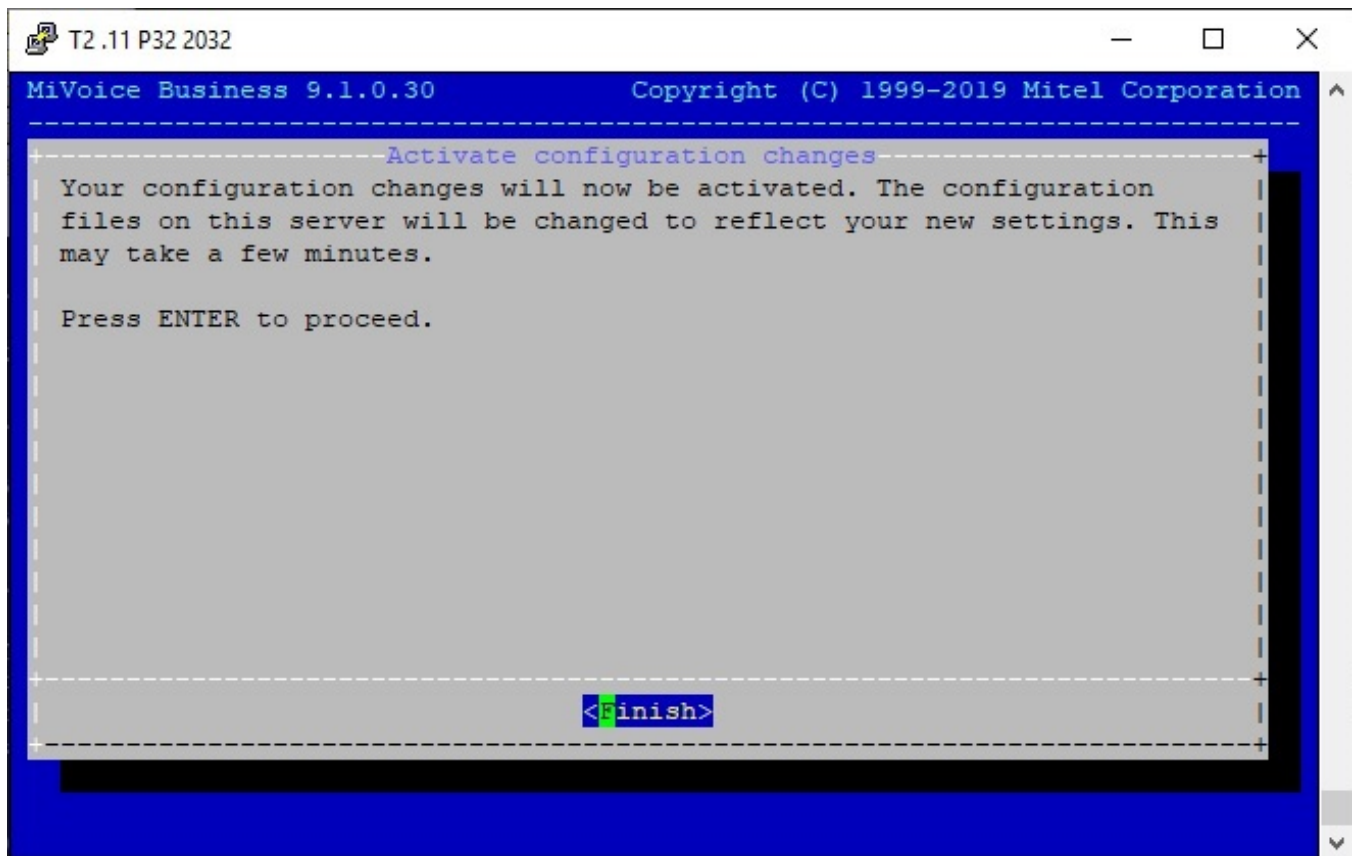


3. Type yes and click **Next** if you have a stored 9.0 or later MSL database backup file in a known location. Type no and click **Next** if you do not have a 9.0 or later MSL database backup file.

4. If you typed **no** in Step 3:
 - a. Enter a password that applies to both *admin* and *root* user IDs. After typing a password click **Next**.
 - b. Select the system timezone and click **Next**.
 - c. Enter the primary domain name for your server and click **Next**.



- d. Enter a system name for your server. The server name can be composed of letters, numbers and hyphens. Click **Next**.
 - e. Enter a local IP address that is unique in your network. Click **Next**.
 - f. Enter a subnet mask for your server. Click **Next**.
 - g. Enter a gateway IP address for your server and click **Next**.
 - h. Enter one or more comma-separated DNS server IP addresses and click **Next**.
 - i. To activate the configuration changes you have made, click **Finish**.



After the bootstrap console completes the server configuration, you should be able to log in to the Server Manager with as root user with the password you created in Step 4a. You may skip Step 5.

5. If you typed **yes** in Step 3:
 - a. Enter the local IP address and click **Next**.
 - b. Enter the subnet mask for your server and click **Next**.
 - c. Enter the IP address of the server containing your backup file and click **Next**.
 - d. Enter the gateway IP address to access the server containing your backup file and click **Next**.
 - e. Enter the domain name of the backup server and click **Next**.
 - f. Enter the name of the shared drive and click **Next**.
 - g. Enter a possible subdirectory where the backup file is stored and click **Next**.
 - h. Enter the username and password to access the server and click **Next**.
 - i. Select the backup file you want to restore the database from and click **Next**.
 - j. Confirm that you have selected the right database backup file and click **Yes**.

The database restore begins. After the database restore completes (including multiple system reboots), you may log in to the Server Manager with the username and password associated with the database backup.

Configure the Layer 2 Switch (MXe III, CXi II)

The internal Layer 2 switch in the CXi II, and MXe III must be programmed with an IP address in the same subnet as the RTC IP address, or the switch will not operate properly.

To set the Layer 2 switch IP address, complete the System IP Properties form, and then reboot the system.

NOTE: The 16 10/100 Mbps ports are disabled on the CXi II during bootup, as is the right-hand side (when viewed from the front) Gigabit port on the MXe III.

TIP: Refer to the System Administration Tool Help for detailed instructions on programming the IP Network Configuration forms associated with the CXi II and MXe III.

1. Connect an Ethernet cable between the Layer 2 switch on your network and one of the following ports:
 - LAN port on the CX II and CXi II controller using a straight-through cable
 - LAN port 1 of the MXe III/MXe III-L controller using a straight-through cable

2. Program the Layer 2 switch with the appropriate settings (see [Network Configuration Examples](#) 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.*

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

Enable Licenses and Options

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 or options are required.

To enable or upgrade licenses and options, you must connect to the Server Manager.

In order to transfer licenses and options between controllers, you must use the AMC to create an Application Group containing controllers with a System Type of "Enterprise" and license sharing enabled. Then, when you enable the licenses and options on the controllers, designate one controller as the Designated License Manager (DLM) for the Application Group. This enables you to deallocate licenses from one group member and allocate them to another, individual system limits permitting.

After completing changes to an account on the AMC, you can perform an automatic sync (recommended) with the AMC, which requires only that you enter the Application Record ID for each individual controller and, if license sharing is enabled, the Group Application record ID on the DLM.

To enable licenses and options on the controller, you need to complete one of the following procedures:

- [Automatic Sync via MiVB System Administration Tool](#)
- [Manual License and Options Entry](#)

TIP: It is recommended that you perform an automatic sync.

3300 ICP System Requirements for AMC

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 Properties 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.
4. **CXi II, MxIII-Specific WAN Considerations:** Program the Internet Gateway (WAN interface) IP address details (see MxIII/MxIII-L/AX/CXi II Requirements for IP Networking).

Automatic Sync via MiVB System Administration Tool

NOTE: The following procedure does not apply to MiVoice Business Release 9.0 or later. For MiVoice Business Release 9.0 or later, license activation is performed through Server Manager (**Service > Status**).

1. In the **MiVoice Business** System Administration Tool, access the **License and Option Selection** form and click **Change**.
2. Enter the **Application Record ID**, and then click **Retrieve Licenses**.
3. Click **Next** to display the In Progress screen. Click **Save** to commit your changes.
4. Click **Start**. After the reboot is complete, log into the System Administration Tool and issue the **DBMS Save** maintenance command.
5. Issue the **DBMS Stat** command to verify the DBMS Save and to ensure that the DBMS_Initialized Flag is on.

Server Manager Requirements for Software Download-Blades

Ensure that the firewall is configured to allow:

NOTE: Use DNC lookup to verify the IP address for **blades.mitel-amc.com**, **swdlgw.mitel.com**, and **swdl.mitel.com** before configuring the firewall rules.

1. SSH connections on port 22 to **blades.mitel-amc.com** to verify licenses associated with the ARID.
2. HTTPS connections on port 443 to **swdlgw.mitel.com** to download access tokens from the Software Download Center.
3. HTTPS connections on port 443 to **swdl.mitel.com** to download the software from Content Delivery Network (CDN). As static IP addresses cannot be guaranteed by CDN, firewall rules must be configured to allow FQDN.

Manual License and Options Entry

NOTE: This procedure does not apply to the MxIII Server.

1. In the System Administration Tool, access the **License and Option Selection** form, and click **Change**.
***NOTE:** In 3300 R6.0 and later, you will see an Application Record ID field at the top of the form. Leave this field blank.*
2. Select the appropriate Country variant and Configuration Options, 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 R7.0), an error message that references “sysid # 65535” means that the SysID or i-Button is not installed or not seated correctly.*
3. Click **Save** to commit your changes to the database.
***TIME:** The Save procedure can take approximately three minutes.*
4. **Reset** the controller (see [Perform a System Reset](#)).

Upgrade System to Required Software Version

Upgrade the MiVoice Business application to the required MiVoice Business software version (see **ServiceLink > System Upgrade** in the *Server Manager Help*).

Verify the Operation of the Controller

1. On the Maintenance PC, access the **MiVoice Business** 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 MxIII/MxIII-L system.
3. In **Maintenance and Diagnostics**, click **Alarm Details**. Verify that the following alarms do not appear (if you get an alarm, go to [Check Alarm State](#)):
 - E2T Com (not applicable to the AX and CX II/CXi II controller)
 - DSP***TIP:** The next four steps are optional.*
4. Connect two IP Phones directly to the controller's Ethernet ports. For controllers with one Ethernet port, an L2 switch will be required.
5. Program the IP Phones (refer to the System Administration Tool Help for details).
6. Make a call from one phone to the other.
7. Disconnect the IP Phones.

Installation and Programming

Install Hardware

Determine Controller Module Configuration

The following illustrations include available components for each controller. Refer to [Install and Replace Units](#) for installation instructions.

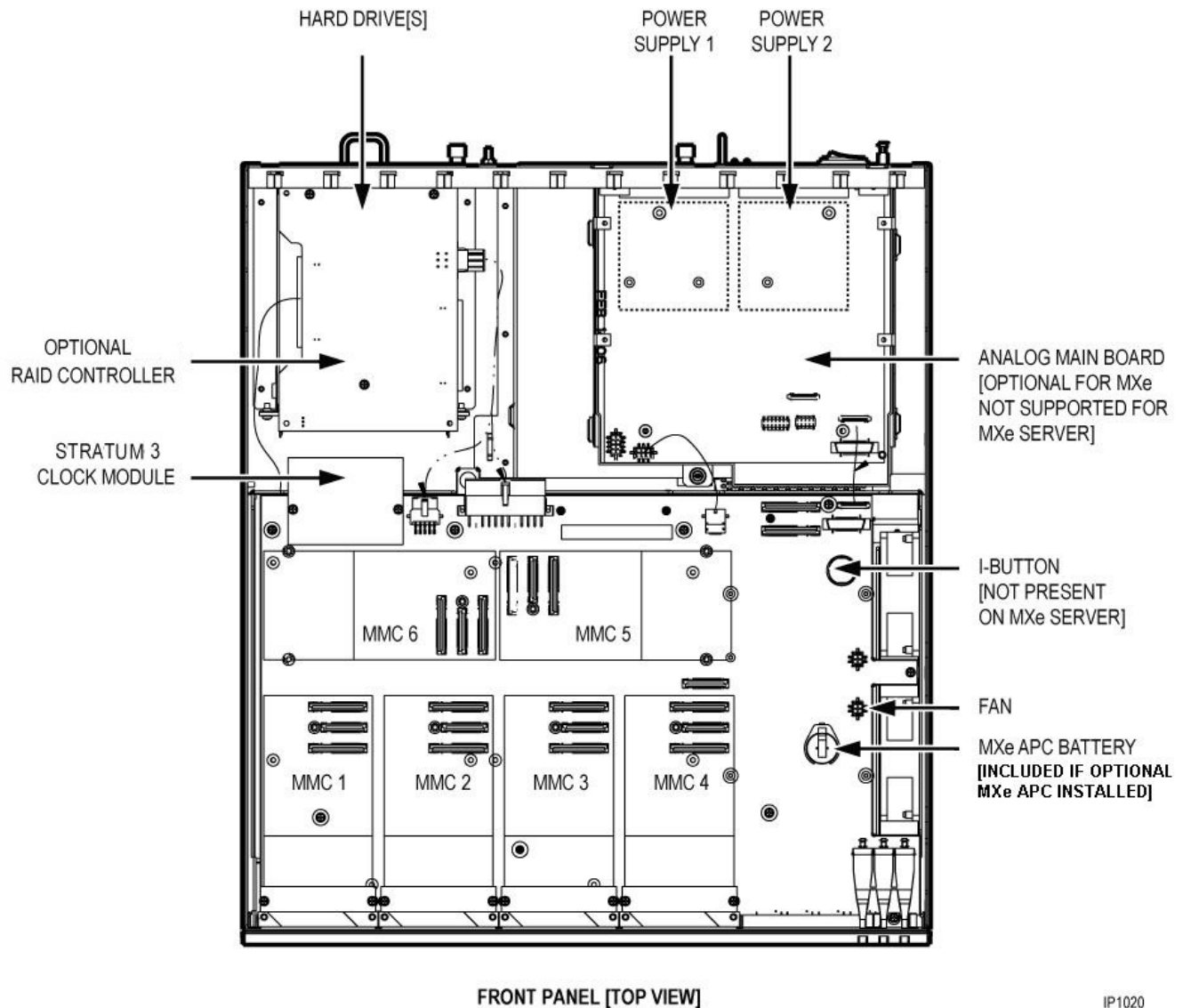
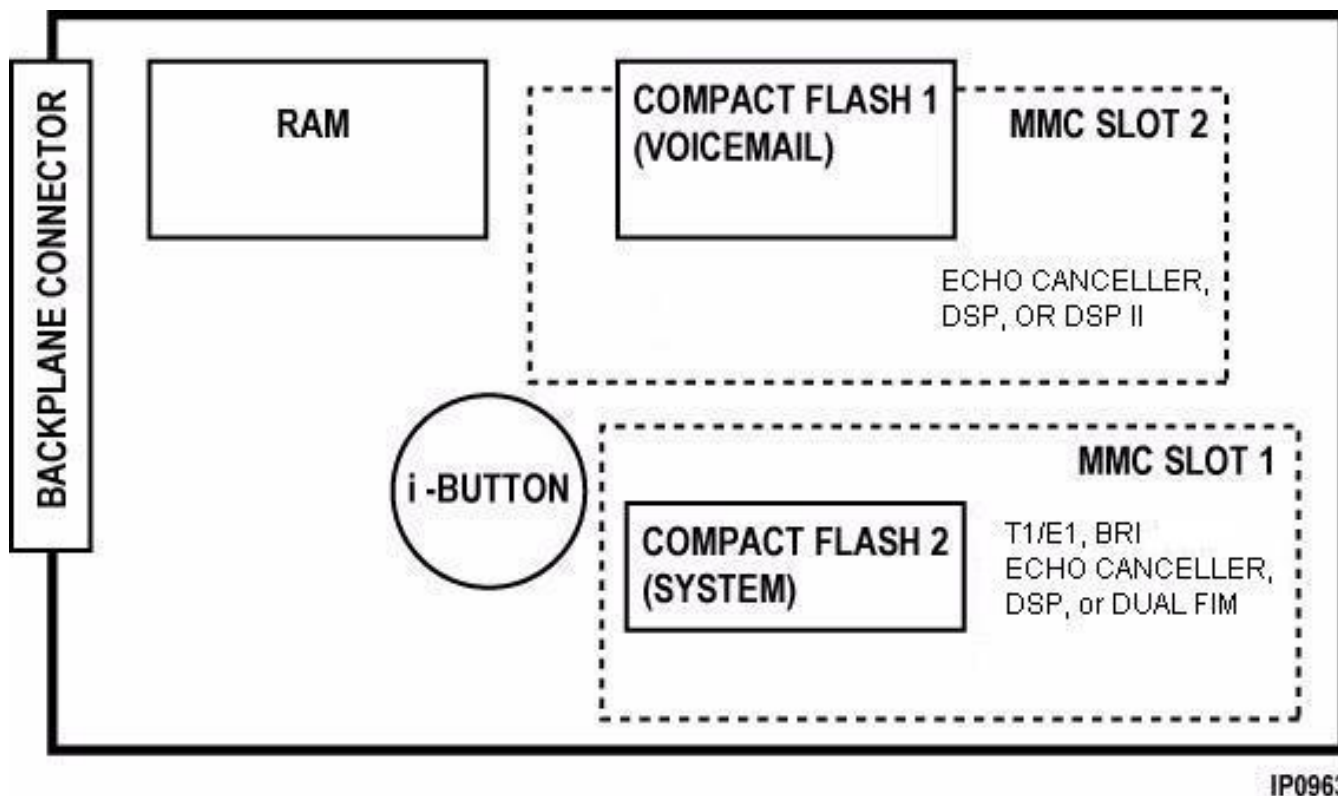



Figure 4.1: Slot Locations for the MxIII/MxIII-L Controller

Table 4.1: MxIII/MxIII-L Controller: Supported Modules

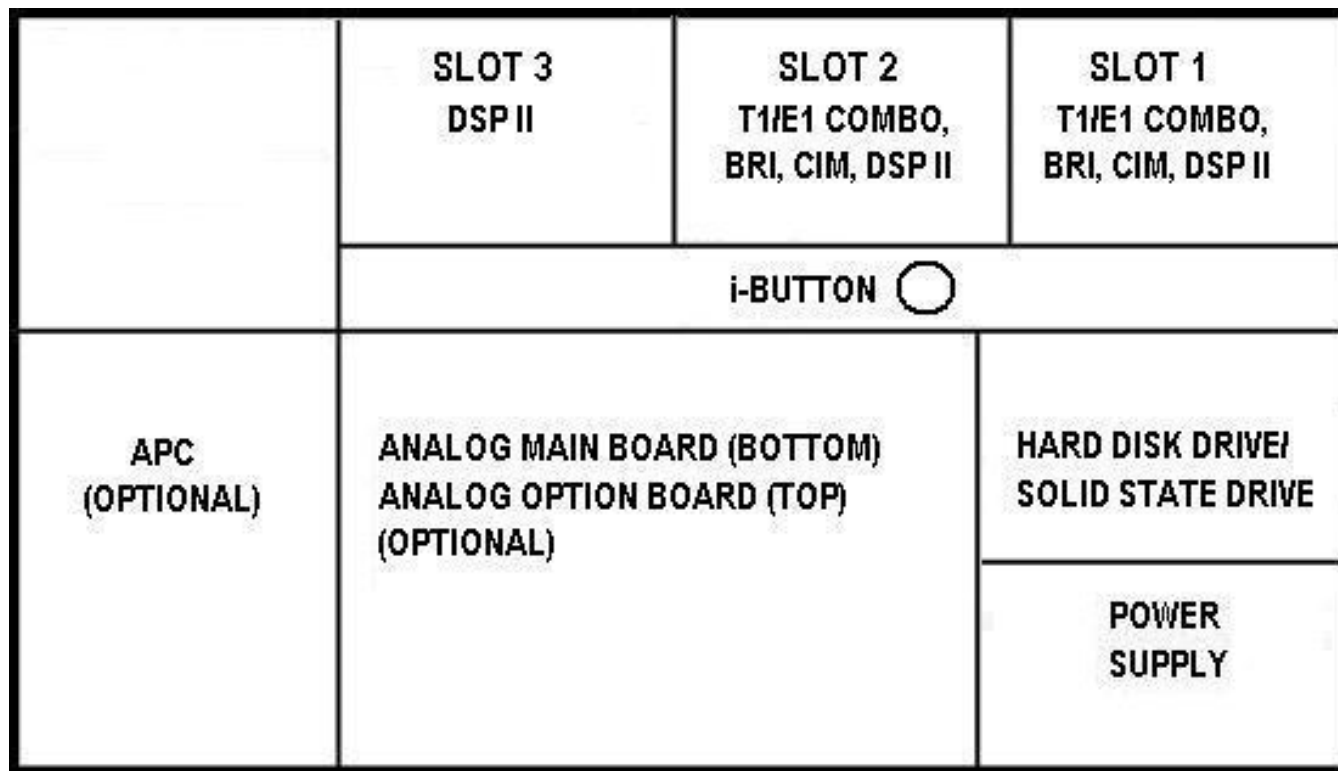
Module	MMC1	MMC2	MMC3	MMC4	MMC5	MMC6
T1/E1	Yes	Yes	Yes	Yes	No	No
BRI	Yes	Yes	Yes	Yes	No	No
CIM	Yes	Yes	Yes	Yes	No	No
DSP	Yes	Yes	Yes	Yes	Yes	Yes
DSP II	No	No	No	Yes	Yes	Yes
Echo Cancellor	Yes	Yes	Yes	Yes	Yes	Yes

**Figure 4.2:** Slot Locations on the AX Controller Card

16-PORT ETHERNET PoE MODULE	SLOT 3 DSP II	SLOT 2 T1/E1 COMBO, BRI, CIM, DSP II	SLOT 1 T1/E1 COMBO, BRI, CIM
	i-BUTTON 		
APC (OPTIONAL)	ANALOG MAIN BOARD (BOTTOM) ANALOG OPTION BOARD (TOP) (OPTIONAL)		HARD DISK DRIVE/ SOLID STATE DRIVE
			POWER SUPPLY

IP1358

Figure 4.3: Slot Locations for the CXi II Controller (with an Ethernet L2 Switch with POE)



IP1357

Figure 4.4: Slot Locations for the CX II Controller (without an Ethernet L2 Switch)

NOTE: The CX controllers support a maximum of three ASUs.

Identify Controller Component Options

Table 4.2: Controller Component and Upgrade Options (Sheet 1 of 3)

Processor Speed	450	533	266
Components	AX ⁶	MXe III ³ /MXe III-L ⁹	CX II/CXi II ²
Embedded CIM ⁵	—	√	—
<i>Quad CIM¹</i>	—	√	√
<i>DSP</i>	√	√	√ ¹⁰
<i>Echo Cancellor</i>	√	√	—

Table 4.2: Controller Component and Upgrade Options (Continued) (Sheet 2 of 3)

Processor Speed	450	533	266
Components	AX ⁶	MXe III ³ /MXe III-L ⁹	CX II/CXi II ²
<i>T1/E1 Framer</i>	√	√	—
<i>Quad BRI Framer</i>	√	√	√
<i>T1/E1 Combo</i>	√	√	√
<i>Line Cards (AX, ASU II)</i>	√	—	—
<i>AMB (MXe III/MXe III-L)</i>	—	√	—
<i>AMB (CX II/CXi II)</i>	—	—	√
<i>AOB (CX II/CXi II)</i>	—	—	√
<i>Redundant Power Supply</i>	√	√	—
<i>Hard Drives</i>	—	√	√
<i>RAID Controllers</i>	—	√	—
<i>Redundant Hard Drives</i>	—	√	—
<i>Stratum 3 Clock</i>	— ⁷	√	√ ⁷
<i>System ID Module</i>	—	—	—
<i>System i-Button</i>	√	√	√
<i>System Flash</i>	√ ¹¹	—	—
<i>Voice Mail Flash</i>	√ ¹¹	—	—
E2T	—	√	—

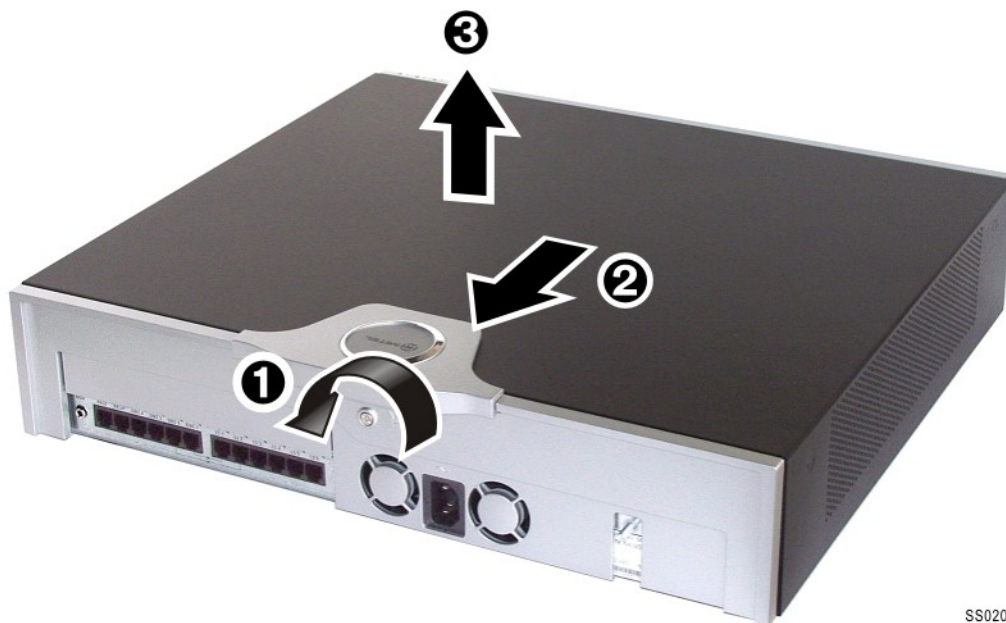
Table 4.2: Controller Component and Upgrade Options (Continued) (Sheet 3 of 3)

Processor Speed	450	533	266
Components	AX ⁶	MXe III ³ /MXe III-L ⁹	CX II/CXi II ²
Upgrading to a 1400-User System	—	√ ⁴	—
NOTES: <ol style="list-style-type: none"> 1. The Quad CIM requires 3300 R7.1 or later software. 2. The CX/CXi require 3300 R6.0 or later software. The CX II/CXi II require MCD 4.0 or later software. 3. The MXe III requires MCD 4.2 or later software. 4. Requires the installation of a second processor, the E2T. 5. The embedded CIM is not an option and is not field replaceable. 6. The AX requires 3300 R7.1 or later software. 7. The CX II, CXi II and AX controllers use an <i>embedded</i> Stratum 3 Clock, so it is not field replaceable. 8. The MXe III Server does not have any digital trunks, so it does not use a Stratum 3 clock. 9. The MXe III-L requires MCD 9.1 or later software. 10. The Dual DSP and Quad DSP are NOT supported on the CX II. (The CX is the only member of the 3300 ICP family that uses the Dual DSP module.) 11. Both flash cards are field installed. 			

Remove Controller Cover

To remove the controller cover:

1. [Power Down the Controller](#).
2. Disconnect all cables.
3. Remove cover as shown in [Figure 4.5](#) or [Figure 4.6](#).



SS0200

Figure 4.5: CX II/CXi II - Removing the Cover



P896

Figure 4.6: MXe III/MXe III-L/MXe III Server - Removing the Cover

Install Controller Modules

Read the Safety Instructions before performing the procedures in this chapter (see [Safety Instructions](#)).

NOTE: Before installing a 3300 ICP, **always** read the RN for the software you are installing (see [Documentation - Mitel Document Center](#)).

1. Shut down the controller. For more information, see [Power Down the Controller](#).
2. Disconnect all cables from the controller.

3. Remove the controller cover. For more information, see [Remove Controller Cover](#).
4. Remove the module from its packaging.

MXe III/MXe III-L, CX II/CXi II

1. Remove the blank module cover at the front of the controller, and insert the module in an appropriate slot.
2. If you are replacing a defective module, remove the screws and lock washers and pull up on the module to remove it.
3. Secure the module to the controller using the screws and pillars provided with the module.
4. Tighten the controller faceplate screw nearest the MMC slot.
5. Replace the controller cover.
6. Reconnect the cables to the controller.
7. Power up the controller.

AX

1. Remove the blanking plate (or the old MMC) from the controller by removing the screws that hold the standoffs to the controller (the screws are on the back side of the controller card).
2. Back off the controller faceplate screw nearest the MMC slot a couple of turns (because the screw interferes with the removal/insertion of T1/E1, or Quad BRI).
3. Slide the blanking plate out of the opening from the back of the controller faceplate.
4. Remove the two standoffs (closest to the face plate) from the blanking plate (or old MMC). Retain the standoffs and screws.
5. Fasten the standoffs to the front of the new MMC.
CAUTION: Proceed with extreme care to avoid damaging components on the controller card.
6. Carefully slide the MMC face plate under the lip of the controller face plate. See . Do not push the MMC past the controller face plate as shown in [Figure 4.7](#).
7. Re-install and/or re-tighten the screws.

8. Continue with procedure as described in the specific FRU instructions.

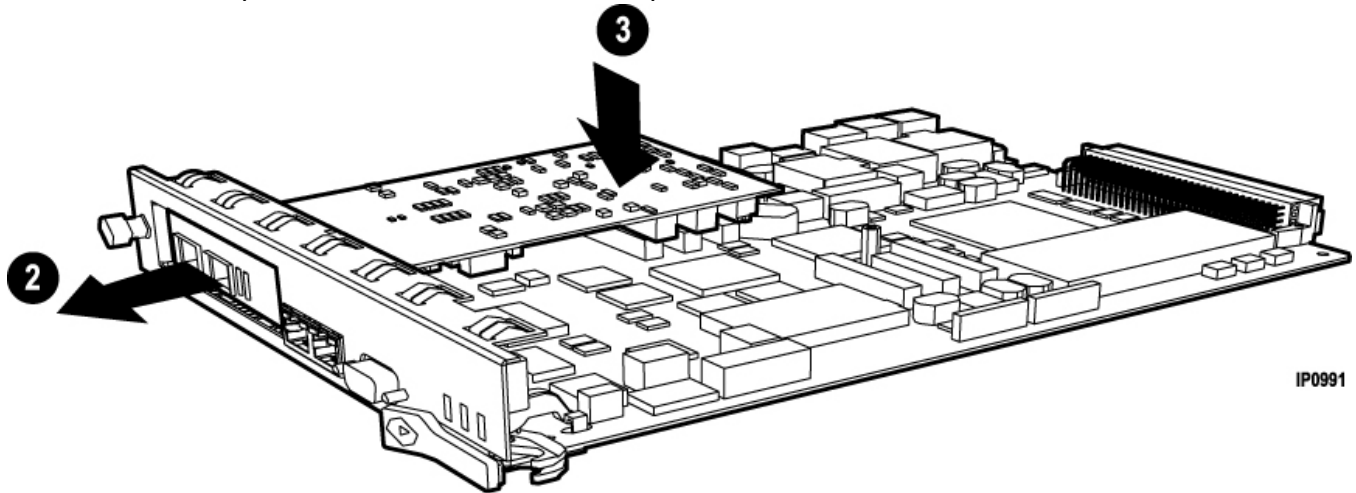


Figure 4.7: Slide in and seat module (AX)

Install Controller Stratum 3 Clock Module

To install the clock module in the MXe III/MXe III-L:

NOTE: The other controllers use the Stratum 3 Clock, but in each case, the clock is embedded and is not field replaceable.

1. Power down the controller (see [Power Down the Controller](#)).
2. Remove the controller cover (see [Remove Controller Cover](#)).
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, and power up the controller.

Install Controller Hardware

Refer to [Add or Replace Controller FRUs](#) for controller hardware installation procedures.

Rack Mount the Controller

The rack-mount hardware secures the controller to the rack. The mounting hardware is shipped with the controller.

MXe III/MXe III-L (Four-piece Bracket Installation)

1. Position a mounting bracket inside the rack frame at the desired height. Fasten the mounting bracket to the front of the rack frame with two screws—one in the top hole, the other in the bottom (see 1 in

- Figure 4.8*). Then do the same to fasten the other mounting bracket on the other side of the rack frame at the same height.
2. Fasten the angle brackets on each side of the cabinet. Align the brackets with the pre-drilled holes located near the front panel. Use two screws to fasten each bracket (see 2 in *Figure 4.8*).
 3. Set the controller cabinet onto the mounting brackets and slide the controller cabinet into the cabinet (see 3 in *Figure 4.8*).
 4. Fasten the angle brackets to the rack frame. Install two screws in each bracket (see 4 in *Figure 4.8*).

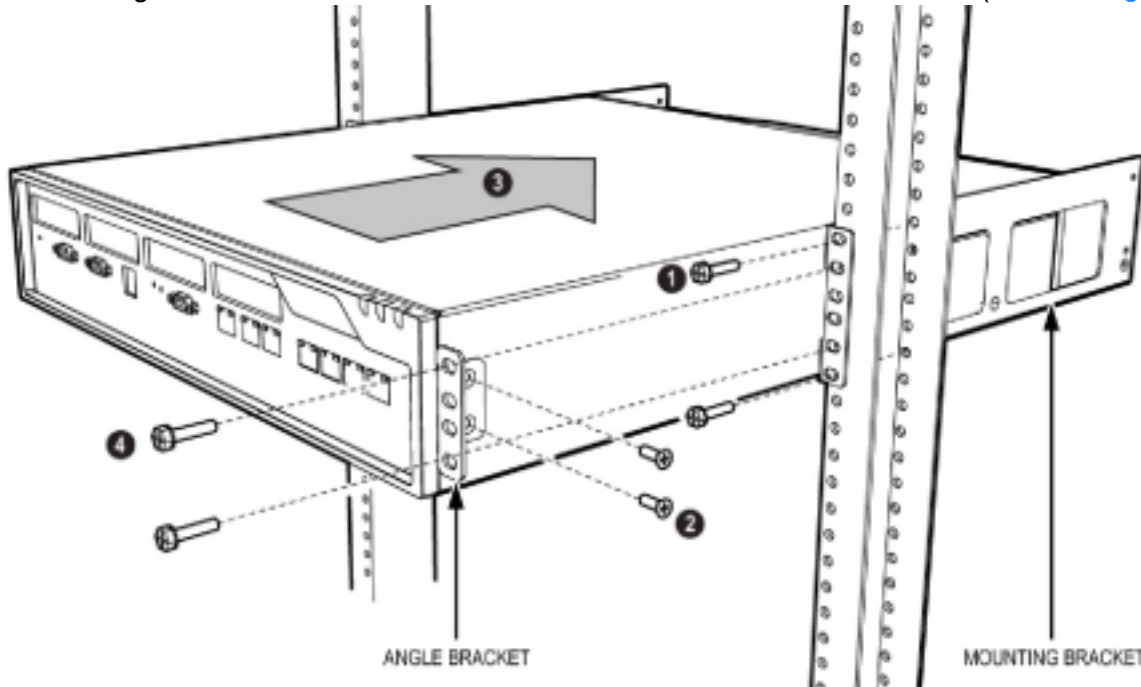


Figure 4.8: MXe III/MXe III-L and CX II/CXi II Controller Rack-Mount 4-Piece Bracket Installation

MXe III/MXe III-L (Two-piece Bracket Installation)

1. Attach the mounting brackets to the MXe III/MXe III-L 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 III/MXe III-L will occupy.
 - loosely enough that the frame mounting bracket can be dropped into position, resting on the screw thread (see *Figure 4.9*).
3. Position the MXe III/MXe III-L on the frame, resting the MXe III/MXe III-L mounting brackets on the frame mounting screw thread.
 - The MXe III/MXe III-L 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.

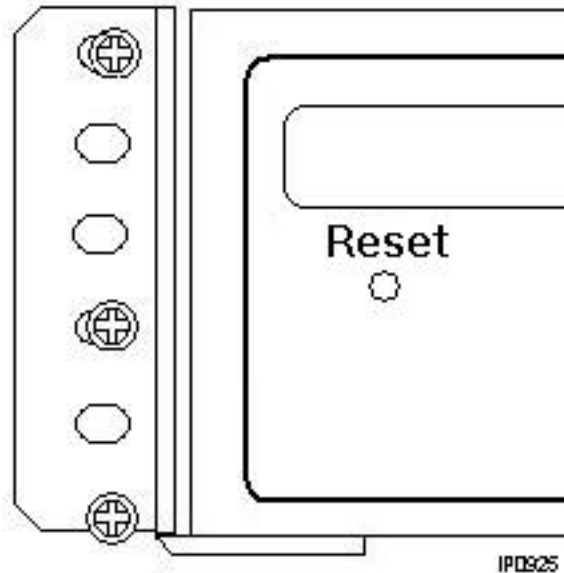


Figure 4.9: MXe III/MXe III-L Rack-mount Screw Placement (2-piece Bracket Installation)

CAUTION: Remove the MXe III/MXe III-L 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.

AX

TIP: The AX controller must be rack-mounted. The chassis is shipped empty and is light enough to be installed by one person.

1. Mount the rack ears to the chassis front or rear facing, centre or face-mounted.
2. Attach the other part of the rack-mount kit to the rack.
3. Lift the chassis into the rack and bolt it in place.
4. Install power supplies, controller card, and line cards into the chassis.
5. Attach a permanent ground connection.

TIP: Refer to [Controller Card \(AX\)](#) (p. 159) for installation instructions.

CX II and CXi II

1. Position a mounting bracket inside the rack frame at the desired height. Fasten the mounting bracket to the front of the rack frame with two screws—one in the top hole, the other in the bottom (see [Figure](#)

4.10). Then do the same to fasten the other mounting bracket on the other side of the rack frame at the same height.



Figure 4.10: CX II/CXi II Controller Rack-Mount Installation - Attaching Brackets to Rack Frame

2. Remove the cover from the controller.
3. Fasten the angle brackets on each side of the cabinet. Align the brackets with the pre-drilled holes located near the front panel. Use two screws to fasten each bracket (see [Figure 4.11](#)).



Figure 4.11: CX II/CXi II Controller Rack-Mount Installation - Attaching Brackets to Controller

4. Replace the cover on the controller.
5. Set the controller cabinet onto the mounting brackets and slide the controller cabinet into the cabinet.
6. Fasten the angle brackets to the rack frame. Install four screws in each bracket (see [Figure 4.12](#)).



Figure 4.12: CX II/CXi II Controller Rack-Mount Installation - Fastening Angle Brackets to Rack Frame

Wall Mount the CX II/CXi II Controller

Required parts and tools:

- Wall mount bracket (supplied)
- Two #4 metric screws (CX II/CXi II) (supplied)
- Drill, screwdriver(s), and two #10 screws for anchoring bracket to backer board
***CAUTION:** Make sure the wall material is capable of supporting the weight of the unit. It is recommended that you mount the supplied bracket onto a backer board of 3/4" plywood that is securely fastened to the wall studs. DO NOT mount the bracket directly onto drywall (sheetrock). Mitel is not responsible for units damaged as a result of improper wall mounting.*

CX II/CXi II

To wall mount the CX II/CXi II controller:

1. Turn the controller upside down.
2. Fasten the mounting bracket to the bottom on the controller using the supplied screws (see [Figure 4.13](#)).

3. Secure the backer board to the wall studs.



Figure 4.13: Wall-mounting the CX II/CXi II - Attaching the Mounting Bracket to the Controller

4. Pre-drill two pilot holes spaced 11.25" (28.58 cm) apart into the backer board.
5. Insert a screw into each pilot hole.
6. Hang the controller onto the screws.

Install Service Units and Cabinets

This section contains detailed information on installing and configuring the Analog Services Unit for the 3300 ICP. This section also contains information on configuring embedded analog.

This procedure applies to the ASU, the Universal ASU, and the ASU II (compatible only with R7.0 or later software). 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.

All ASUs:

1. Mount the ASU. Refer to [ASU II](#) 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.

***TIP:** The 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 [ASU 25-Pair D-Type Connector Pinout](#)).
4. For the Universal ASU, complete the Music on Hold and Paging cabling if required. See [Universal ASU Music on Hold Connector Pinout](#) and [Universal ASU Pager Connector Pinout](#).
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.
6. Using the System Administration Tool, program the ASU settings on the controller. Refer to the *System Administration Tool Help* for instructions.

***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 (refer to the System Administration Tool Help).

Next: Install any other required services units. When all the services units are installed, go to [Install Telephones](#).

Peripheral Cabinet, SUPERSET HUB, and Digital Service Unit

TIP: Refer to the 3300 R7.0 version of the Technician's Handbook for SX-2000 peripheral cabinet, SUPERSET HUB, and Digital Service Unit component installation instructions.

Install Telephones

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 II/CXi II controllers only 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.

Install Telephones, Consoles and Appliances

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

NOTE: Each IP Phone must be directly connected to an L2 switch port. DO NOT connect them in series (daisy-chaining) using the 2nd LAN port in the phone. If daisy chained, a problem with one phone can affect all the others in the chain. Also, all chained phones share the same bandwidth.

NOTE: If you intend to rely on LLDP VLAN Discovery in the network, you must first upgrade the 3300 ICP to R7.0 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), 5240 IP Appliance, and 5485 IP.

IP phone firmware is automatically downloaded from the 3300 controller to the IP Phones (requires a DHCP server configured with options 128-133). You can also download firmware to the telephone by plugging it directly into an Ethernet port on the 3300 controller. The controller must be running R7.0 or later to provide LLDP-compliant firmware to the telephone.

NOTE: When a resilient hot desk device rehomes to a switch that has newer device firmware, the user (including hot desk ACD agents) is automatically logged out to allow the firmware upgrade to proceed.

Install Line Interface Modules

The Line Interface Module (LIM) provides analog operation to the 5220 IP Phone (Dual Mode), 5224 IP Phone, 5330 IP Phone, 5340 IP Phone, or 5360 IP 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*.

Register IP Devices from the Telephone

Use one of the following procedures to register IP devices with the MiVoice Business database:

- **PIN Registration**
This procedure will program the MiVoice Business database with the MAC address of the IP device.
TIP: Use the System Administration Tool to complete all other set programming (for example, Class of Service, Interconnect Restriction, Set Key Assignments, and Class of Restriction).
- **Registration without a DN**
Use this procedure to register and auto-provision a basic Userless Device (a device with service level “IP Device Only” that allows the user to log in, but does not require a license). With this procedure, a device is registered and brought to service without being pre-configured first and the installer does not need to specify the device's Directory Number (DN) - only the Set Registration Access Code - to initiate the registration.

Before you begin

For PIN Registration, ensure that

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

For Registration without a DN, ensure that

- the local host controller is MiVoice Business 7.0 or later.
- the Set Registration Access Code is configured in the System Options form.
- the following DN range-defining parameters are configured:
 - Set Registration Auto DN Selection - Prefix in the Shared System Options form.
 - Set Registration Auto DN Selection - Begin and Set Registration Auto DN Selection - End parameters in the System Options form.
 - the Set Registration Auto DN Selection - Secondary Element is assigned in the System Options form (optional).

Register an IP Device

1. Connect the IP device to an RJ-45 Ethernet port on the LAN. For the CXi II, connect to a controller Ethernet port.
2. Provide power to the IP device (refer to the 3300 ICP Hardware Technical Reference Manual in the Document Center for power option information).
3. For PIN Registration, type the PIN number at the prompt on the IP device.

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

For Registration without a DN, type the Set Registration Access Code (without the DN) 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**.

4. Complete one of the following:

- 5001, 5005, 5201 and 5205 IP Phones: press **Hold**.
- 5010, 5207, 5215, 5020, 5212, 5220, 5224, 5312, 5324, 5530 and 5340 IP Phones: press **SuperKey/Settings**.
- 5140 and 5240 IP Appliances: press **OK**.

***NOTE:** If you want to clear any PIN number from the memory, press * during power-up.*

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 Elements** form matches the ICP/PBX Number programmed in the **ICP/PBX Networking** form.
- 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.

***NOTE:** If Registration without a DN is used, all added devices are hosted by the same (primary) node. If load-balancing is required, use the PIN Registration method to add new devices.*

Install Music on Hold

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

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

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

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

- Music on Hold connector on the back of a controller with Embedded Analog (MXe III; see for information on adding MOH support to an AX)
- Music on Hold connector on the back of a Universal ASU (see [ASU 25-Pair D-Type Connector Pinout](#))
- Music on Hold connector on a peripheral cabinet E&M trunk card

Digital Music on Hold is provided by an external music source connected to a DNIC Music on Hold/Pager Unit (DMP). A peripheral cabinet is required. The DMP is connected to a DNI line card.

Music on Hold over IP (MiVoice Business 7.0 and later) provides live music from a source on the Internet; see the System Administration Tool Help for provisioning information.

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

TIP: To reduce the risk of hum or other interference, 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 AX, CX II/CXi II, or Mx III/Mx III-L):

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 AX, CX II/CXi II or Mx III/Mx III-L):

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).

TIP: Refer to the 3300 ICP Hardware Technical Reference Manual for connector pinouts.

Program 5485 IP Paging Unit

NOTE: See [Table 8.14](#) for the paging unit pinout and [Figure 8.20](#) for the cross connection wiring.

To program a 5485 IP Paging Unit (this programming procedure provides a burst of ringing prior to the speech broadcast):

1. Launch the System Administration Tool.
2. In the Multiline IP Sets form
 - Program the IP Paging Unit as "5010 IP".
 - Enter the MAC address.
3. In the Feature Access Codes form (optional)
 - Assign a code to Direct Page Paging.
4. Multiline Set Keys form (optional)
 - Program a Paging key.
5. Interconnect Restriction Table
 - Ensure that the station is not restricted from Paging.

To program Group Page with the IP Paging Unit (This programming procedure does not provide a ring burst prior to the speech broadcast):

1. Multiline IP Sets form
 - Program the IP Paging Unit as "5010 IP".
 - Program the MAC address.
2. Page Groups form

- Complete all required fields. Symbol Wireless Phones should not be programmed into paging groups.
- 3. Class of Service Options form
 - Set the Group Page Accept field to "Yes" for the IP Paging Unit.
 - Ensure that each telephone in the paging group has the Group Page Allow field set to "Yes".
- 4. Feature Access Codes form (optional)
 - Assign a Direct Page feature access code.
- 5. Multiline Set Keys form (optional)
 - Program a Paging key.
- 6. Interconnect Restriction Table
 - Ensure that the station is not restricted from Paging.

Appendix-J Upgrade and Deploy VM

Two types of upgrades are supported:

- Upgrade applications on the same VM.
- Upgrading application by deploying a new VM.

Upgrade applications on the same VM

For MiVB applications, use the Server Manager Blades panel to perform an upgrade. For the MarWatch MarProbe installed in the MiVB VM, use the MiVB Server Manager Blades panel to perform an upgrade. For upgrade instruction browse to the Blades panel and select the Help icon.

For Micollab Application Use The Server Manager Install Applications Panel To Perform An Upgrade. For Upgrade Instruction Browse Install Applications Panel And Select The Help Icon.

Upgrading application by deploying a new VM

Follow the steps below to upgrade a new VM:

Backup data from old VM

From the old VM, backup system data to the Azure File Share.

Refer the MSL Backup Configuration section of the MiVoice Business Azure Deployment Guide to backup data to the Azure File Share. Note the backup file name.

The screenshot shows the Mitel MiVoice Business interface. On the left is a navigation menu with 'ServiceLink' (Blades, Status) and 'Administration' (Web services, Backup, Restore, View log files, Event viewer, System information, System monitoring). The 'Backup' option is selected. The main area is titled 'Backup to Network' and shows an 'Operation status report'. It states 'Current system time: Wed 21 Apr 2021 09:33:10 PM UTC' and 'Backup to network completed successfully.' Below this, a red box highlights the text 'Created backup file: mslserver_my-mivb-vm_2021-04-21_21-33.tgz'. At the bottom, it says 'MiVoice Business 9.1.1.60' and '© Mitel Networks Corporation'.

Shutdown old VM

Locate the old VM, select **Stop** to shut it down.

The screenshot shows the Azure portal interface for a virtual machine named 'My-Mivb-Vm'. The left sidebar shows the navigation menu with 'Overview' selected. The top bar has a search box and action buttons: Connect, Start, Restart, Stop (highlighted with a red box), Capture, Delete, Refresh, and Open in mobile. Below the buttons is an advisor message: 'Advisor (1 of 5): Log Analytics agent should be installed on your virtual machine'. The main area shows the 'Essentials' section with details about the VM: Resource group (MY-RESOURCE-GROUP), Status (Running), Location (East US), Subscription (MiVoice Business Flex), Subscription ID (aa1b0fb1-0caa-4ebf-bd2e-3f7f03242184), Tags, Operating system (Linux (redhat 11.0.78.0)), Size (Standard F2s_v2 (2 vcpus, 4 GiB memory)), Public IP address (-), Virtual network/subnet (My-Virtual-Network/default), and DNS name (-).

Deploy a new VM

Deploy a new VM with the same properties as the old VM. It is important that the new VM uses the same IP addresses as the old VM for the following reasons.

1. The Network Element form in MIVB may be referencing other servers by IP addresses.
2. MBG Clustering in 11.0.x uses private IP address.
3. Minet IP Phones may be referencing the MBG Servers using a Public IP as opposed to its FQDN.
4. Any other provisioning referencing servers by IP address.

CREATE A NEW VM

Refer the Create MSL VM for MBG, MiVB, or MiCollab section of the MiVoice Business Azure Deployment Guide to deploy a standard MSL VM. In the Management section, make sure that you are using the same storage account that the old VM uses. In the Advanced section, make sure that you are using the same custom data as the old VM.

STOP AND RESIZE NEW VM

After deployment completes, stop the new VM. Follow the instructions provided in the Resizing VM disk section of the MiVoice Business Azure Deployment Guide to resize the new VM.

The new VM will use the same network interface(s) and associated NSG from the old VM. For MBG upgrade, there is no need to create another network interface, add firewall rules in the NSG associated with the network interface, or add a public IP address for AWV.

Next move the network interface(s) from the old VM to the new VM.

MOVE NETWORK INTERFACE FROM OLD VM TO NEW VM

MiVB VM

The MiVB VM has one network interface. Follow the instruction below to move the network interface from the old VM to the new VM.

1. Locate old VM i.e. My-Mivb-Vm. Select **Networking** to see the attached Network Interface. The snapshot below shows that the old VM is attached to Network Interface my-mivb-vm2912 with private IP address.

Home > My-Mivb-Vm

My-Mivb-Vm | Networking ...

Virtual machine

Search (Ctrl+/) << Attach network interface Detach network interface

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Settings
Networking
Connect
Disks
Size
Security
Advisor recommendations
Extensions

my-mivb-vm2912

IP configuration ⓘ
ipconfig1 (Primary)

Network Interface: my-mivb-vm2912 Effective security rules Troubleshoot VM connection issues Topology

Virtual network/subnet: My-Virtual-Network/default NIC Public IP: - NIC Private IP: Accelerated networking: Disabled

Inbound port rules Outbound port rules Application security groups Load balancing

Network security group My-Mivb-Vm2-nsg (attached to network interface: my-mivb-vm2912)
Impacts 0 subnets, 1 network interfaces

Add inbound port rule

Priority	Name	Port	Protocol	Source	Destination
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any

2. A VM must have at least one NIC assigned. The Azure portal UI will allow you to detach a NIC if the VM has more than one NIC assigned. Hence create a temporary NIC to assign to the old VM. Select **Attach network interface**. This opens the **Attach network interface** blade dialog.

Home > My-Mivb-Vm

My-Mivb-Vm | Networking ...

Virtual machine

Search (Ctrl+/) << Attach network interface Detach network interface

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Settings

Attach network interface

Attach existing network interface

Create and attach network interface

OK Cancel

3. Select **Create and attach new network interface** and then select **OK**. This opens a new page to create a new NIC for the old VM.

Home > My-Mivb-Vm >

Create network interface ...

Project details

Subscription ⓘ

MiVoice Business Flex

Resource group * ⓘ

My-Resource-Group

[Create new](#)

Location ⓘ

(US) East US

Network interface

Name *

my-mivb-vm-temp-nic

Virtual network ⓘ

My-Virtual-Network

Subnet * ⓘ

default

Create

4. Specify the Name for the temporary NIC and select Create. After the NIC is created the old VM has two NICs assigned (my-mivb-vm2912 and my-mivb-vm-temp-nic) and the 'Detach network interface' function is enabled.

Home > My-Mivb-Vm

My-Mivb-Vm | Networking ...

Virtual machine

Search (Ctrl+/)

Attach network interface **Detach network interface**

my-mivb-vm2912 my-mivb-vm-temp-nic

IP configuration ⓘ

ipconfig1 (Primary)

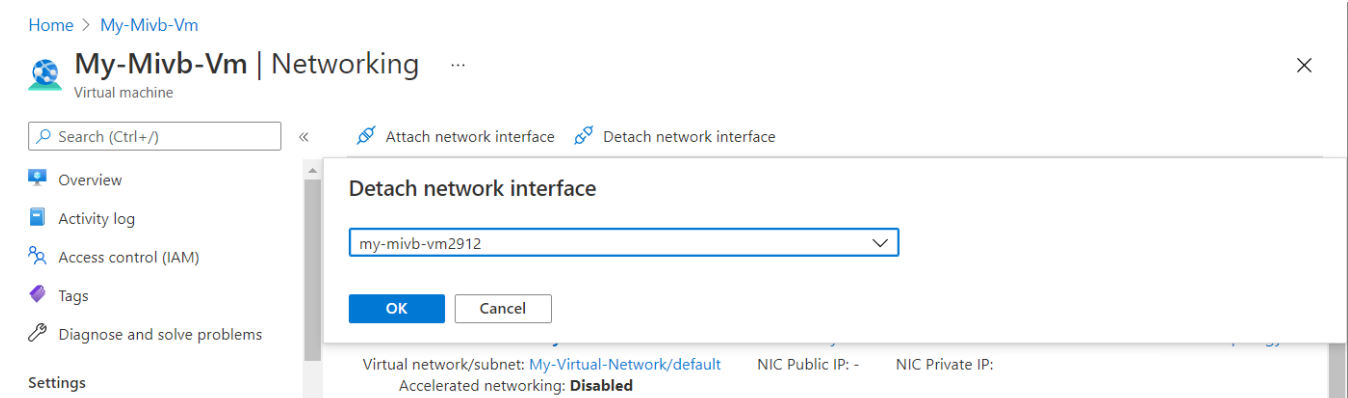
Network Interface: my-mivb-vm2912 [Effective security rules](#) [Troubleshoot VM connection issues](#) [Topology](#)

Virtual network/subnet: My-Virtual-Network/default NIC Public IP: - NIC Private IP: -

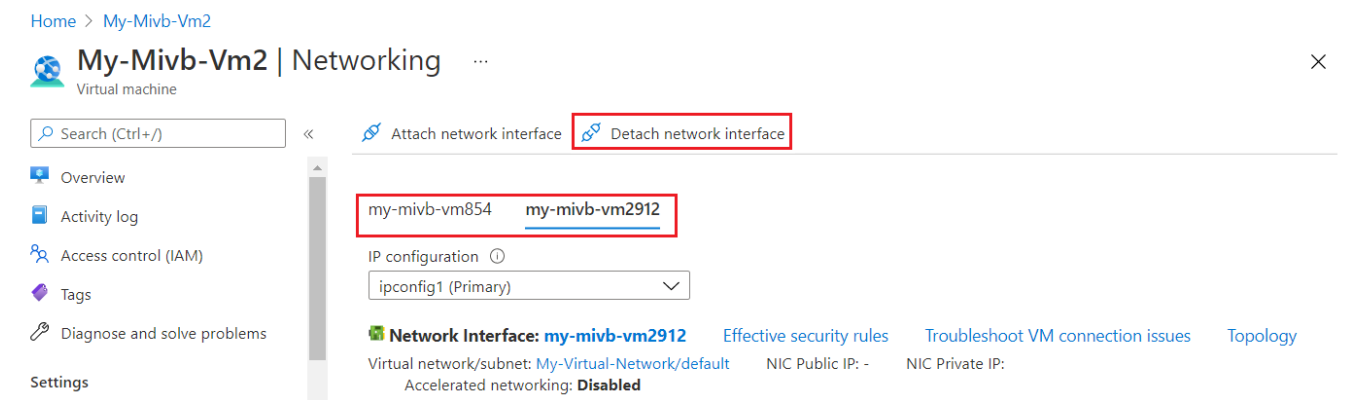
Accelerated networking: **Disabled**

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings

5. Select **Detach network interface** to detach the old VM NIC i.e. my-mivb-vm2912. This opens a **Detach network interface** blade. Make sure the right NIC is selected. Select **OK** to detach it from the old VM.



6. The old VM now has a temporary NIC assigned.
7. Locate the new VM i.e. My-Mivb-Vm2, select **Networking** to see the NIC assigned. The Azure portal UI will not allow you to detach the NIC unless there is more than one NIC assigned.
8. Select **Attach network interface** to open the **Attach network interface** blade. Specify the NIC originally from the old VM i.e. my-mivb-vm2912 and select OK to attach the NIC to the new VM.



START THE NEW VM

Select **Overview** and select **Start** to start the new VM.

Restore data to new VM

For the new VM, log into Server Manager using its FQDN. Refer the MiVoice Business Subscription Azure Deployment Guide to configure the Restore form to access and restore the backup file from the old VM. You can monitor progress of the data restore from the VM Serial Console. The data restore requires a system reset.

After data restore completes, log back into the SM. Navigate to the Status form to verify presence of the ARID restored from the old VM.

Install application SW blade

- From the Status form, verify that the system is licensed to retrieve blade SW from the SWDL.

- From the Blades form, install the application SW blade. When install completes it triggers the application to do a data restore.
- After data restore completes, log into the application to verify that data from the old VM is restored into the new VM.

Cleanup resources after upgrade succeed

If upgrade to the new VM is a success, then delete the old VM and its associated resources. The associated resources include the Network Interfaces, the Network Security Group, and the Disk.

Rollback to old VM if upgrade to new VM fails

If upgrade to the new VM fails you can revert to using the old VM. Stop the new VM. Follow similar instructions to move the network interface(s) from the new VM back to the old VM.

Start the old VM. You can monitor system start up via the serial console. After startup completes, verify that you can access the old VM with its FQDN.

EX Controller Hardware Installation

For EX controller hardware installation, see *EX Controller Installation Guide* in the Document Center.

Program System

Programming Tools

The MiVoice Business system includes a number of programming tools:

- **Server Manager** supports a suite of managed services and applications delivered from the Mitel Applications Management Center (AMC). The Server Manager is used to perform; administration (such as, software upgrade, database backup and restore), security, and platform configuration related tasks. For more information, see **Server Manager > About Server Manager** in the *MiVoice Business System Administration Tool Help*.
- **System Administration Tool** that provides a Web-based interface that trained technicians use to program (partial) the MiVoice Business system (in conjunction with the Server Manager).
- **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.
- **Mitel Integrated Configuration Wizard** assists you in the initial system programming. After you specify the system setup, you can save the configuration data for future use or apply the changes to the 3300 ICP. See the System Administration Tool Help for installation and configuration instructions.
- **MiVoice Business Migration Tool** helps you migrate from an MCD 6.0 SP3 or later to MiVoice Business Release 9.0. For more information, see the MiVoice Business Migration Guidelines document.
- **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 [IP Phone Analyzer](#)).

Log in to the Programming Tools

System Administration Tool

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>, where <hostname> is the name or IP address assigned to the Controller if no DNS is available. Refer to [Establish Communication with Controller](#).
2. The first time you connect, you must install the Mitel Root CA security certificate (see [Secure Sockets Layer \(SSL\) and Security Certificate](#)).
3. To log into the ESM:
 - Type the default **Login ID** (“system”) and **Password** (“password”).
 - Select **Remember Login ID** if you want to save the Login ID on your computer.
 - Click **Log In**.

TIP: To prevent unauthorized use, change the Login ID 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 the System Administration Tool. For the MXe III Server, the PC must use the System IP address.

TIP: The system will allow up to five concurrent System Administration Tool or Group Administration Tool sessions (or any combination of the two) provided that the initial login browser is closed plus ten concurrent Desktop Tool sessions.

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

MiWalkThru

MiWalkThru widget contains the list of guided walkthroughs that helps you perform a configuration task in the MiVB application with step-by-step instructions. It provides you on-screen guidance for completing your configuration tasks successfully.

1. Click the MiWalkThru widget to get the list of available Guided Walkthroughs.
2. Click on the MiWalkThru Guidelines in the footer of the MiWalkThru widget to know more.
3. The following URL s3.walkmeusercontent.com allows Images in WalkMe Solutions hosted by WalkMe’s AWS.

NOTE: If this domain is blocked then the Images in WalkMe Solutions that are hosted by WalkMe’s AWS won’t appear.

4. The following URL d3sbxpiag177w8.cloudfront.net also allows files and images in the walkme solutions that are hosted by Walkme’s AWS.

NOTE: if this domain is blocked and the URL is referenced in any WalkMe content then the image file will not load.

Server Manager

To log in to the Server Manager:

1. Enter the following address in the address bar of a browser, and then press **Enter**: `http://<host-name or IP address of the MiVoice Business system>/server-manager`
2. In the **Username** field, type the default user name `admin`.
3. In the **Password** field, enter the password associated with the *root* user, and then click **Login**.

Mitel Integrated Configuration Wizard

Install the Configuration Wizard on a maintenance PC that meets the following minimum requirements:

- Windows 2000 operating system
- JRE (Java Run-time Environment) 1.6.0_1 or later installed

To install the Configuration Wizard onto the maintenance PC:

- Close all applications running on the PC.
- Download the MICW Setup.exe file from MOL.
- Double-click the Setup.exe file. Follow the prompts to install the program.

IP Phone Analyzer

To install the IP Phone Analyzer

- See [Analyze IP Phone Issues](#).

To launch the IP Phone Analyzer:

- On the **Start** menu, point to **Programs**, and click **Mitel IP Phone Analyzer** (see [Analyze IP Phone Issues](#) for details).

Program LS Trunk Settings via LS Measure Tool

Use the LS Measure tool in the System Administration Tool to program the line settings for Loop Start (LS) trunks that are connected to the AX Controller Card Chassis, Analog Main Board, Analog Option Board, or ASU II. The LS Measure Tool supports the following tests:

- Individual or Batch Line Quality Test
- Individual or Batch Distortion/Echo Test

The Line Quality Test allows you to obtain the optimum Balance Network Setting and Trunk Category for each LS trunk, based on the signals received from the CO. These settings are then programmed into the Analog Trunks form of the LS trunks to reduce the possibility of echo and audio level issues between the trunks and IP phones.

The Distortion/Echo test should only be run at the request of Mitel Technical Support.

Refer to the following book in the System Administration Tool Help for instructions: **Programming -> Programming Trunks -> Using the Line Measure Tool**.

LS Trunk Selection in the UK

Poor audio quality may be experienced if the incorrect subscriber line has been provided by the carrier.

To ensure that the correct lines are provisioned in the UK, the installer or system administrator should request that the Telco (e.g. BT), or carrier, provide trunks that are compatible to System X line type '0' (Subscriber lines) or line type '3' (business PBX/PABX lines).

Both types of lines will work satisfactorily with the 3300 ICP, however line type '3' is the preferred line type for connecting a PBX/PABX.

Configure Analog Music On Hold (MOH)/Paging

The 3300 ICP supports:

- Analog MOH
- Digital MOH (via a DMP)
- Embedded MOH
- MOH over IP

Refer to the System Administration Tool Help for instructions on how to program Digital MOH, Embedded MOH, and MOH over IP.

To program Analog Music on Hold:

1. Launch the System Administration Tool
2. In the System Options form:
 - Set the Music On Hold option to "Yes".
 - (Optional) Class of Service Options form.
3. In the E&M Trunk Circuit Descriptors form:
 - Set the Outgoing Start Type parameter to "Immediate".
 - Set the Transmission Facility parameter to "2 wire".
 - Set the 2 Wire Balanced Network Setting parameter to "600".
 - Set "Perform Seize Test on Out-of-Service Trunks" to "No".
 - All other parameters may be any value.
4. In the E&M Trunk Assignments form:
 - Ensure that the trunk number is unique. The service number, E&M trunk circuit descriptor number, and the interconnect number may be the same as other E&M trunks.
5. In the System Access Points form:
 - Set "Music Source" to "External".
 - In the "Music Source Port - Location ID" field, enter the PLID of the E&M trunk circuit.
***NOTE:** Music on Hold can be assigned to either of the first two ports on a Universal ASU E&M card or to the E&M port on the Analog Main Board (AMB) (on a controller with embedded analog). Only one Music on Hold source is permitted per system.*
6. If you assigned Music on Hold to an E&M port on the AMB (on a controller with embedded analog) reboot the controller to start Music on Hold operation. Or, if you assigned Music on Hold to a port on a Universal ASU E&M card, reload the Analog Services Unit to start Music on Hold operation.

Software Installation

Software installation on 3300 ICP controller

This section describes methods of installing MiVoice Business 9.0 or later software on a supported storage device for your MxIII, CX II, and CXi II controllers (MiVoice Business 9.1 or later for AX and MxIII-L controllers).

If your system is either running a pre-9.0 MiVoice Business software version or you have acquired a supported storage device with a pre-9.0 MiVoice Business software version, and you want to upgrade to 9.0 or later, you can use the MiVB Migration Tool to perform either:

- a full migration (applicable to MxIII, MxIII-L, CX II, CXi II controllers only), or
- Migration with media replacement procedure (applicable to MxIII, MxIII-L, CX II, CXi II and AX controllers), provided you have a supported storage device with a pre-installed MiVoice Business Release 9.1 software version

You can install or re-install MiVoice Business Release 9.0 or later on a supported storage device by performing a manual full install procedure.

NOTE: MiVoice Business Software Installer Tool is not supported in MiVoice Business Release 9.0 and later.

If you have a supported storage device with pre-installed MiVoice Business Release 9.1, you may perform disk/CF replacement procedure.

To navigate and choose the correct method, see [Appendix H: Configuration of Brand-New/Used Controllers and Storage Devices](#).

If you are performing a new installation, see **Ch. 3, Initial Setup >Overview**.

Install System Software using the Migration Tool

Overview

This procedure applies to:

- new installations of MiVoice Business Release 9.1 or later
- systems running a pre-9.0 MiVoice Business software version that you want to migrate to MiVoice Business 9.1 or later

In the case of new installations, the storage device you received has either MiVoice Business 7.2 SP2 or MiVoice Business 9.1 software pre-installed. If you received a new storage device with MiVoice Business 9.1, refer to the [Appendix H: Configure New/Used Controllers and Storage Devices](#) section for the appropriate sub-section and procedure (for example, Hard Disk Replacement). Otherwise, refer to the **Procedure** below.

NOTE: AX Controllers support migration with media replacement only; not a full migration (see [Note in Step 4 of the Procedure](#) below).

Before You Begin

Ensure that you have the following:

- IP address for the 3300 ICP controller

- MiVoice Business user name and password
- MiVoice Business 9.0 or later software (downloaded from the Software Download Centre)
- MiVoice Business Migration Tool (see [Installation of the MiVoice Business Migration Tool](#))

Procedure

The manual migration procedure consists of the following steps, which **must be completed in the listed order**:

NOTE: You can connect directly to the controller through an Ethernet port. You can also connect to the controller through the LAN.

1. Ensure that the initial set up is complete. See **Ch 2, Initial Setup** in the *MiVoice Business Technician's Handbook, Release 7.2* document.
This step is applicable only for new MiVoice Business 9.1 installations; skip this step if you want to migrate a controller with an installed pre-9.0 MiVoice Business software version to 9.1 or later.
2. Start the **MiVoice Business Migration Tool**.
3. Connect to the MiVoice Business system using the MiVoice Business Migration Tool (See **Getting Started > Connecting to the MiVoice Business System** in *MiVoice Business Migration Tool Help*).
4. Perform full migration (see **Performing a Full Migration** in *MiVoice Business Migration Tool Help*).
NOTE: If you are migrating an **AX Controller** to MiVoice Business 9.1 or later, you must perform migration with media replacement only (see **Performing a migration with media replacement** in *MiVoice Business Migration Tool Help*).
5. Log in to the System Administration Tool to verify whether the installation is successful (see [Log in to the Programming Tools](#)).
6. Configure the MiVoice Business System using one of the following methods:
 - By using the Mitel Integrated Configuration Wizard (See the *Mitel Integration Configuration Wizard Help*)
 - By using the MiVoice Business System Administration Tool (See the *MiVoice Business System Administration Tool Help*)

Install MiVB Software on a 3300 ICP Controller (Manually)

Overview

The following section describes the procedure to manually install or re-install the MiVoice Business system software on 3300 ICP controllers. The procedure applies to MiVoice Business Release 9.0 or later (MiVoice Business Release 9.1 or later for AX controllers).

This procedure assumes that your controller features U-Boot as the bootloader. If your controller features Bootrom as the bootloader, and you want to perform a manual full install of MiVoice Business 9.0 or later, you must first [upgrade the bootloader of the controller to U-Boot](#).

NOTE: Before re-installing MiVoice Business Release 9.0 or later on a system that is unable to boot, follow the procedure, **Ch 4, Software > Unable to boot the MiVoice Business System on 3300 ICP Controller** in the *MiVoice Business Troubleshooting Guide* to attempt recovery of the system without a full manual re-install.

NOTE: If MiVB is deployed with an MSL backup or restore and Mitel Performance Analytics (MPA) Probe is running in the same instance as MiVB, then after you have completed the MiVB upgrade, you must

manually deploy the MPA probe. This will ensure that the MPA will get back to its current status after the MiVB upgrade.

For more information about deploying MPA probe, see [Mitel Performance Analytics Probe Installation and Configuration Guide](#).

Before you begin

Ensure that you have the following:

- Access to the controller's Maintenance port.
- Access to a TFTP server. If you do not have a TFTP server, see [Set up a TFTP server and a custom repository](#).
- Access to an HTTP server. If you do not have an HTTP server, see [Set up an HTTP/HTTPS Server and a Custom Repository](#).
- A 3300 ICP controller that features U-Boot as the bootloader.

Procedure

NOTE:

- As a result of executing this procedure, the content of the hard disk/Compact Flash (CF) will be lost.
- You cannot ping the controller while the controller is in U-Boot command prompt. U-Boot can only issue ping requests but cannot respond to ping requests.

Table below lists the U-Boot variables you must configure to initiate a manual full installation:

Table 5.1: U-Boot Variables for a 3300 ICP Controller (Sheet 1 of 3)

U-Boot Variable	Purpose
serverip	IPv4 address (dot-decimal format) of the TFTP server that features the MiVoice Business installation files for the required software release. Default value: 192.168.1.4 .
httpserverip	IPv4 address (dot-decimal format) of the HTTP server that features the MiVoice Business installation files for the required software release. Default value: 192.168.1.4 .
httpserverpath	Base path for the MiVoice Business installation files on the HTTP server. For example: Applications. The default value is not defined.
release	The MiVoice Business software release to be installed. For example: MiVB_ppc_image/9.1/9.1.0.88 Default value: 20.0.0.0 .

Table 5.1: U-Boot Variables for a 3300 ICP Controller (Continued) (Sheet 2 of 3)

U-Boot Variable	Purpose
bootcmd	<p>Boot command that U-Boot uses to boot the controller.</p> <p>Default value: run load_ata</p> <p>For this procedure, the value of the boot command must be set to:</p> <pre>run load_ram</pre>
ipaddr	<p>IPv4 address of the controller in dot-decimal format.</p> <p>Default value: 192.168.1.2.</p> <p>NOTE: There is no need to change the value of the <code>ipaddr</code> variable, if you have already configured the IP setup for the controller.</p>
netmask	<p>IPv4 net mask of the controller in dot-decimal format.</p> <p>Default value: 255.255.255.0.</p> <p>NOTE: There is no need to change the value of the <code>netmask</code> variable, if you have already configured the IP setup for the controller.</p>
netmask_hex	<p>IPv4 net mask of the controller in hexadecimal format.</p> <p>Default value: FFFFFF00.</p> <p>NOTE: There is no need to change the value of the <code>netmask_hex</code> variable, if you have already configured the IP setup for the controller.</p>
gatewayip	<p>IPv4 address (dot-decimal format) of the gateway for the subnet.</p> <p>Default value: 192.168.1.1.</p> <p>NOTE: There is no need to change the value of the <code>gatewayip</code> variable, if you have already configured the IP setup for the controller.</p>
hostname	<p>Host name of the controller (as displayed in the System IP Properties form in the <i>System Administration Tool</i>); used to form the controller's FQDN.</p> <p>Default value: mpc8360-<platform>, where platform is either <code>mxiii</code>, <code>cxii</code>, or <code>ax</code>.</p> <p>NOTE: There is no need to change the value of the <code>hostname</code> variable, if you have already configured the IP setup for the controller.</p>

Table 5.1: U-Boot Variables for a 3300 ICP Controller (Continued) (Sheet 3 of 3)

U-Boot Variable	Purpose
ata_active_part	The disk partition hosting the active MiVoice Business software version. For this procedure, leave the value of the <code>ata_active_part</code> variable unchanged. There is no need to change the value of this variable because the manual full installation reformats the disk, and chooses the default active partition number as the active partition.

NOTE: In the examples below (Step 5), the values chosen for the `release` and `httpserverpath` variables are based on the assumption that the MiVoice Business installation files are installed on your HTTP server and visible at: **`http://<httpserverip>/Applications/MiVB_ppc_image/9.1/9.1.0.88`**, and that the TFTP server's base directory contains the path: **`MiVB_ppc_image/9.1/9.1.0.88`**, and the relevant content under it. If the TFTP server is hosted on the same machine as the HTTP server, then it is assumed that the TFTP server's base directory is the **Applications** folder.

1. Power off the controller.
2. [Access 3300 ICP Controller Through the Maintenance Port](#)
3. Power on the controller.
4. From the communication application, stop the auto-boot sequence by pressing the SPACE key three or more times consecutively within seven seconds at the following prompt:

```
Press <SPACE> key 3 times within 7 seconds to stop autoboot
```

The system displays => prompt.

5. Configure system parameters, using one of the following two methods:

- `run ubootcfg` command (available only for U-Boot 1.0.3.11 or later), or
- `setenv` command

Using the `ubootcfg` command

The `run ubootcfg` command allows for the configuration of individual system parameters, one at a time (see Table above for more information about the system parameters). If you do not want to change the value of a particular system parameter, press ENTER to move on to the next system parameter in the list. If you want to delete the current value of a system parameter, and set it to a blank value, press the `.` key.

For example, if you want to install MiVB PPC image 9.1.0.88 on a brand new CX II controller from TFTP server 10.44.23.34 and HTTP server 10.44.16.126, with controller's intended IP address 10.38.72.37/24 and gateway at 10.38.72.1, host name `mycxii`, then you must modify the entries as follows (new values after the colon) using the `ubootcfg` command:

```
=> run ubootcfg
```

```
.=clear field, <ENTER>= no change;
```

```

Please enter 'ipaddr' [192.168.1.2]: 10.38.72.37
Please enter 'netmask' [255.255.255.0]:
Please enter 'netmask_hex' [ffffff00]:
Please enter 'gatewayip' [192.168.1.1]: 10.38.72.1
Please enter 'hostname' [mpc8260-cxii]: mycxii
Please enter 'ata_active_part' [1]:
Please enter 'serverip' [192.169.1.4]: 10.44.23.34
Please enter 'httpserverip' [192.168.1.4]: 10.44.16.126
Please enter 'httpserverpath' []: Applications
Please enter 'release' [migrateflash]: MiVB_ppc_image/9.1/9.1.0.88
Please enter 'bootcmd' [run load_ata]: run load_ram

```

To save the changes, if any, execute `saveenv`

=>

If the controller has already been in use, with the IP configuration completed, modify the entries as shown below (new values after the colon) for the same example:

=> `run ubootcfg`

`.=clear field, <ENTER>=no change;`

```

Please enter 'ipaddr' [10.38.72.37]:
Please enter 'netmask' [255.255.255.0]:
Please enter 'netmask_hex' [ffffff00]:
Please enter 'gatewayip' [192.38.72.1]:
Please enter 'hostname' [mycxii]:
Please enter 'ata_active_part' [1]:
Please enter 'serverip' [10.35.5.38]: 10.44.23.34
Please enter 'httpserverip' [192.168.1.4]: 10.44.16.126
Please enter 'httpserverpath' []: Applications
Please enter 'release' [migrateflash]: MiVB_ppc_image/9.1/9.1.0.88
Please enter 'bootcmd' [run load_ata]: run load_ram

```

To save the changes, if any, execute `saveenv`

=>

Using the `setenv` command

The `setenv` command allows for configuration of only the required system parameters by typing out the individual parameter's name, followed by its new value (see Table above for more information about the system parameters).

For example, if you want to install MiVB PPC image 9.1.0.88 on a brand new CX II controller from TFTP server 10.44.23.34 and HTTP server 10.44.16.126, with the controller's intended IP address 10.38.72.37/24 and gateway at 10.38.72.1, host name mycxii, then you must modify the entries as follows (new values are typed after the system parameter name) using the `setenv` command:

```

setenv ipaddr 10.38.72.37
setenv netmask 255.255.255.0

```

```
setenv netmask_hex ffffffff00
setenv gatewayip 10.38.72.1
setenv hostname mycxii
setenv serverip 10.44.23.34
setenv release MiVB_ppc_image/9.1/9.1.0.88
setenv httpserverip 10.44.16.126
setenv httpserverpath Applications
setenv bootcmd run load_ram
```

If the controller has already been in use, with the IP configuration completed, modify the entries as shown below for the same example:

```
setenv serverip 10.44.23.34
setenv release MiVB_ppc_image/9.1/9.1.0.88
setenv httpserverip 10.44.16.126
setenv httpserverpath Applications
setenv bootcmd run load_ram
```

6. To confirm if the values you entered in Step 5 are set correctly, run one of the following two commands:

- run `ubootprint` command (available only for U-Boot 1.0.3.11 or later), or
- `print` command

Using the `ubootprint` command

The `ubootprint` command displays the complete list of system parameters and their corresponding values (available only for U-Boot 1.0.3.11 or later):

```
run ubootprint
```

Using the `print` command

The `print` command enables you to check the values of individual system parameters:

```
print <variable>
```

For example:

```
print bootcmd
```

The value of the `bootcmd` variable will be displayed.

If you need to change the value of a parameter, see Step 5.

7. Save the changes to the U-Boot variables by running the following command:

```
saveenv
```

8. Enter the following command to boot the installer and start installing the MiVoice Business software:

```
boot
```

The installation may take up to an hour to complete (assuming that the TFTP and HTTP servers are accessible over the LAN).

9. To monitor the installation progress, at the login prompt, log in as user *root*, and use the default password, and then run the following command:

```
tail -f /tmp/install.log
```

The communication application displays the installation progress. If the installation fails, an error message is displayed.

After successfully installing the software, the system configures the U-Boot's boot command, **bootcmd**, to boot the software from the partition 1 (CX II/MXe III/MXe III-L) and partition 2 (AX) and then reboots the system.

10. After the system boots, an End User License Agreement screen is displayed on the communication application. Read the entire EULA text; if you agree with it, select **Accept** to proceed to the next step (see [Set Network Configuration on 3300 ICP Controller with a New HDD](#)).
11. Log in to the Server Manager and do the following:
 - a. License the system (**ServiceLink > Status**).
 - b. Restore the database (**Administration > Restore**).
12. Log in to the System Administration Tool to verify that the installation is successful.

Install MiVB 9.0 or Later on a 3300 ICP Controller using HDD

Overview

If you acquired a new 3300 ICP controller with U-Boot and a new hard disk with MiVoice Business Release 7.2 SP2, but you want to run MiVoice Business Release 9.0 or later, then you must downgrade the bootloader of the controller to Bootrom before migrating the MiVoice Business application to MiVoice Business Release 9.0 or later.

Procedure

1. See [Disk Drive Installation \(3300 ICP Controller\)](#).
2. [Access 3300 ICP Controller Through the Maintenance Port](#).
3. Power on the controller.

U-Boot automatically discovers the 7.2 SP2 software load on partition 1 of the new hard disk and boots the system from this partition.

NOTE: The U-Boot takes up to 3 minutes to read the RTC8260 image from disk .

4. From the maintenance port, run the following commands to configure the networking parameters for your environment, and then to re-flash Bootrom over U-Boot:

```
bootChange  
Upgrade_Bootrom
```

5. Log in to the System Administration Tool and change the default password for the system user.

The above steps result in a change in bootloader from Bootrom to U-Boot.

6. Migrate the system to MiVoice Business Release 9.0 or later (see [Software installation on 3300 ICP Controller](#)). Use the system user password that you configured in the previous step.

Installation of the MiVoice Business Migration Tool

Overview

The MiVoice Business Migration Tool helps you prepare and migrate (upgrade) your MiVoice Business system to MiVoice Business Release 9.0 or later.

Before proceeding with using the MiVoice Business Migration Tool, see the *MiVoice Business Migration Guidelines* document for details on migration.

Procedure

You can obtain the MiVoice Business Migration Tool from the **Downloads** page on Mitel MiAccess. You can install the MiVoice Business Migration Tool on the Installation/Maintenance PC, or on its own PC (see [PC Requirements](#) for more information).

To install the MiVoice Business Migration Tool:

1. Download the `MiVBMigrationToolSetup_<version>.exe` file from the **Downloads** page on [Mitel MiAccess](#).
2. Double-click the `MiVBMigrationToolSetup_<version>.exe` file. Follow the prompts to install the MiVoice Business Migration Tool.

NOTE: After installing the MiVoice Business Migration Tool, the system might prompt you to reboot your PC/laptop.

DHCP Server Programming

Program the DHCP Server

Refer to **Configuration > DHCP** in the *Server Manager Help* for programming a DHCP server.

Upgrade System Software (3300 ICP Controller)

You can upgrade your MiVoice Business system (3300 ICP controller) from MiVoice Business Release 9.0 to a later release using the Server Manager. For more information, see **System Upgrade** in the *Server Manager Help*.

TIP: To speed up the upgrade, you may want to ask your users to delete voice mail messages that are no longer required.

CAUTION: PC or Layer 2 switch connection must be to Ethernet port 1.

NOTE: During an upgrade from MiVoice Business release 9.0/SP1/SP2 to 9.0 SP3 or later, the system automatically upgrades the root certificate. You can, ignore the error messages related to root certificate as the system automatically resolves the errors after restoring the database.

Upgrading System Software: Notes, Tips, and Cautions

NOTES:

- The browser cache must be cleared whenever the MiVoice Business system is upgraded (or downgraded) to a newer load.
 - In Internet Explorer: press CTRL+SHIFT+DEL, select **Temporary Internet Files and website files** and clear **Preserve Favorites website data**. Leave other check boxes cleared, and then click **Delete**.
 - In Firefox: press CTRL+SHIFT+DEL, select **Everything** next to **Time range to clear** and **Cache**, then click **Clear Now**.
 - In Chrome: press CTRL+SHIFT+DEL, select **beginning of time** next to **Clear the following items from** and **Cached images and files**, then click **Clear Browsing Data**.
 - In Edge: press CTRL+SHIFT+DEL, select **Cached data and files**, and then click **Clear**.
- Users of FireFox 33 and later are required to restart their browser following an upgrade to MiVoice Business 7.1. Otherwise, the browser may not trust the Mitel Root Certificate and refuse to connect to the System Administration Tool.
- A Backup Failure or Audit Failure alarm will prevent a software upgrade from proceeding. For more information on these alarms and how to resolve them, see “Alarm Categories” in the System Administration Tool Help.

Upgrade Firmware of 3300 ICP Controllers

After upgrading the system software (from MiVoice Business 9.0 to later), you must manually upgrade the firmware of the controller.

NOTE: You must perform this procedure each time after you upgrade the software.

For an MXe III/MXe III-L controller with an E2T card, if the **E2T Comms Alarm** exists, you must clear the alarm before upgrading the firmware. See Unable to Boot the E2T Card on how to clear the alarm.

To upgrade the firmware of the controller:

1. Log in to the System Administration Tool.
2. Navigate to the **Maintenance Commands** form, and run the following command:

```
UPGRADEBOOTROM ALL
```

3. Run the following command to reboot the MiVoice Business system:

```
RESET SYSTEM
```

NOTE: If you had an MXe III/MXe III-L controller with the FPGA alarm, you must power down and power up the system, instead of a reboot; this is required because the FPGA gets programmed only after power on reset (see [Power Down the Controller](#)).

Change Number of IP User Licenses

If you need to decrease or increase the number of IP User Licenses during the software installation, perform the following steps to avoid losing data at reboot.

Table 5.2: Changing the Number of IP User Licenses

If you are increasing or decreasing the number of IP User Licenses	You MUST do the following:
AND the Maximum Configurable IP Users and Devices parameter is NOT modified	<ul style="list-style-type: none"> - save the change - perform DBMS Save command
AND the Maximum Configurable IP Users and Devices parameter IS modified	<ul style="list-style-type: none"> - save the change - perform DBMS Save command - perform a backup and restore
NOTE: The Maximum Configurable IP Users and Devices parameter is only modified when you are increasing the number of IP User Licenses over 700 or decreasing from 5600 back to 700.	

Upgrading to more than 65,000 RDN users

To support more than 65,000 RDNs, both flash cards (system and voice mail) in the AX controller must be the 4 GB size. Use the `ataGetDiskSize` RTC shell command without parameters to determine system card size and with the parameter 1 to determine the voice mail card size. For a 2 GB card, the value returned is approximately 2000. A 4 GB card returns approximately 4000.

If both flash cards are 4 GB, upgrade the controller using the existing upgrade procedure (Online Upgrade suggested).

For controllers that need the bigger card(s), do a manual system software install (see [Software installation on 3300 ICP Controller](#)) after installing the card(s). Refer to the Knowledge Base for specific upgrade instructions.

WARNING: AX controllers must be upgraded to 4 GB flash cards BEFORE expanding RDN capacity beyond 65,000. Failure to do so may block login attempts to System Administration Tool and disrupt call processing. The only way to recover is to do a fresh install.

Distributing New Firmware to IP Phones

Use this procedure to distribute IP Phone firmware after you upgrade any controller in a resilient cluster.

1. Wait for all IP devices to return to their primary controller (now upgraded).
2. Use the `LOAD IPDEVICE 1 to 300` maintenance command to force a firmware reload of all devices.

The Load command uses TFTP connections to transfer software to IP devices. Because **MiVoice Business** supports a maximum of 300 TFTP connections at any one time, you must issue the command multiple times to load software to a large number of IP devices. For example to load software to 500 IP devices, you must issue the command twice:

```
LOAD IPDEVICE 1 TO 300
LOAD IPDEVICE 301 TO 500
```

Distributing Firmware to 69xx IP Phones

The 69xx IP Phones have a larger firmware load that takes longer to download. For this reason an external TFTP server must be configured for all 3300 ICP controllers with more than two hundred 69xx phones, and for all MiVoice Business server variants with more than fifteen hundred 69xx phones. For more information on using external TFTP servers, see the MiVoice Business Engineering Guidelines.

NOTE: Upgrading firmware will take significantly longer if a 10 MB/s Ethernet link is used to connect the MiVoice Business system to the IP phones. This can occur when the phones are connected to the MiVoice Business system through an L2 switch that only supports 10MB/s Ethernet links such as the StreamLine Ethernet switches

Load IP Phone Software Remotely

Use the LOAD IPDEVICE maintenance command to transfer IP Phone software to the IP Phones. Because MiVoice Business supports a maximum of 300 TFTP connections at any one time, you must issue the command multiple times to load software to a large number of IP devices. For example to load software to 500 IP devices, you must issue the command twice:

- LOAD IPDEVICE 1 TO 300
- LOAD IPDEVICE 301 TO 500

Use the IPDevice <1>, <2>...<1400> qualifier to load software into an individual IP device.

Use the IPDevice <1 TO 300> qualifier to load software into all IP devices (up to 300 devices at a time)

If IP Phones fail to load software:

1. Verify the network connection.
2. Verify power.
3. Check the wiring.
4. Check LED on the IP telephone for network activity.
5. A green LED on the bottom of the phone indicates a proper connection.
6. A flashing red LED indicates activity (data flow) on the network.
7. Use the PING (Packet Internet Groper) on the IP telephone to determine whether the server's (3300 ICP, DHCP, and/or TFTP) IP address is accessible.
8. Ensure that the DHCP server has been programmed with the correct information. Refer to the System Administration Tool Help for details.
9. If the IP telephone displays "TFTP LOAD FAILURE" verify that the TFTP Firmware, DSP, and Main software loads are available and not corrupted.
10. Ensure that the phone is registered with the system.

Downgrading to a Previous Software Release

See the **Reverse Migration** appendix in the *MiVoice Business Migration Guidelines* document.

Maintenance

This chapter describes the maintenance procedures for the 3300 ICP controller post installation.

Access 3300 ICP Controller Through the Maintenance Port

To access a 3300 ICP controller through its RS-232 port (Maintenance port) from your maintenance PC:

1. Connect an RS-232 straight DTE male to female serial cable between the controller's RS-232 port (Maintenance port) and your PC's serial port.
2. Open a communication application on your PC (for example, PuTTY) and ensure that the connection parameters are as follows:
 - **Port:** Select the COM port to which you have connected the serial cable. Typically, **COM1**.
 - **Bits Per Second:** Set the baud rate to U-Boot's baud rate (For a controller that has Bootrom as its bootloader, the baud rate is 9600).
 - **Data Bits:** 8
 - **Parity:** None
 - **Stop Bits:** 1
 - **Flow Control:** None
 - **Emulation:** VT100

Determine 3300 ICP Controller Bootloader

To determine the bootloader of your 3300 ICP controller:

1. If your controller is powered on, power it off.
2. After the controller is powered off, [Access 3300 ICP Controller Through the Maintenance Port](#).
3. Power on the controller.
4. The communication program instructs you to Press the SPACE key three times to stop auto-boot after the count-down starts.
5. After you press the SPACE key three times, the prompt displayed determines the bootloader of the controller:
 - If the prompt is **[VxWorks Boot]:**, then the bootloader is **Bootrom**.
 - If the prompt is **=>**, then the bootloader is **U-Boot**.

Determine Last Known Active Partition using U-Boot

Overview

This section describes the procedure to determine the current active partition number on a disk featuring MiVoice Business software, that is, the disk partition number associated with the last known active MiVoice Business software on the disk; in the process, you will also determine the MiVoice Business software version and the completion status (success or failure) of the MiVoice Business application startup the last time it was run.

It is important to boot 3300 ICP controllers from the active partition to prevent potential corruption of the MiVoice Business database.

The following table shows the valid bootable disk partition numbers that depend on the MiVoice Business software version and 3300 ICP controller type:

MiVoice Business Release	Platform	Partitions
Pre-9.0	All	1 or 4
9.0 or later	CX II, Mx III/Mx III-L	1 or 2
	AX	2 or 3

If you do not know which of the two valid bootable disk partition numbers feature the active MiVoice Business software, it is recommended that you run the procedure below to determine the last known active partition number on a disk before you proceed with booting the MiVoice Business software from the disk. For example, this procedure can be used in the following scenarios:

- **Controller Replacement:** If you have the disk from your old controller, and know the active MiVoice Business software version on the disk, but you do not know which disk partition features the active MiVoice Business software version.
- **Disk Replacement:** If you acquired a spare disk that was used previously, but you do not know the active or inactive MiVoice Business software version installed on the disk.

NOTES:

1. Brand-new factory disks featuring pre-9.0 MiVoice Business software are pre-installed with the MiVoice Business software only on partition 1. Partition 4 is always empty. Hence, the system can boot software only from partition 1 of these disks.
2. Brand-new factory disks featuring MiVoice Business 9.0 or later are pre-installed with the same MiVoice Business software on both bootable partitions: 1 and 2 for CX II and Mx III/Mx III-L controllers, or 2 and 3 for the AX controller. Hence, either of the two bootable partitions could become the active partition.
3. Once you discover the disk partition number with the active MiVoice Business software (active partition), you must configure 3300 ICP bootloader to boot the software from the active partition.
4. The procedure described here is applicable to all disks regardless of the MiVoice Business version installed on it; the procedure as such modifies neither the disk content nor the U-Boot configuration.

Before you Begin

Ensure that you have:

1. A 3300 ICP controller with U-Boot
2. A hard disk (for which you want to determine the active partition number)

Procedure

1. Before powering on the 3300 ICP controller (with U-Boot), remove any hard disk installed on this controller.
2. [Access 3300 ICP Controller Through the Maintenance Port.](#)
3. Power on the controller (if controller is already powered on, reboot the controller) and stop the auto-boot sequence by pressing the SPACE key three or more times consecutively within seven seconds at the following prompt:

```
Press <SPACE> key 3 times within 7 seconds to stop autoboot
```

If you observe the U-Boot command prompt (=>) after stopping the auto-boot sequence, then your communication application was configured correctly. Proceed to Step 4.

If you do not observe readable content on the console, the baudrate configuration set on your communication application may be different from the baudrate configuration of your controller. Restart your communication application, and ensure that you set the correct baudrate configuration so that you are able to stop the auto-boot sequence (see Step 2).

If you observe readable output on the console but are unable to stop the auto-boot sequence, it is possible that **some** of the configuration parameters for your communication application are not set properly. Restart your communication application and set all the parameters correctly so that you are able to stop the auto-boot sequence (see Step 2).

4. After you confirm that you are able to stop the auto-boot sequence, power off the system and install the disk (for which you want to determine the active partition number) into the controller (see [Disk Drive Installation \(3300 ICP Controller\)](#)).
5. Power the controller on and stop the auto-boot sequence by pressing the SPACE key three or more times consecutively within seven seconds at the following prompt:

```
Press <SPACE> key 3 times within 7 seconds to stop autoboot
```

6. Determine if the software version installed on the disk is a pre-9.0 or 9.0 (or later) MiVoice Business release by running the following command:

For CX II and Mx III/Mx III-L controllers:

```
ls sata 0:1
```

For AX controllers:

```
ls ide 0:2
```

If the `ls` command displays the Linux file system structure as shown below, then your controller has MiVoice Business Release 9.0 or later software:

```
=> ls sata 0:1
<DIR> 4096 .
<DIR> 4096 ..
<DIR> 16384 lost+found
<DIR> 4096 usr
<DIR> 4096 etc
<DIR> 4096 var
<DIR> 4096 lib
<DIR> 4096 sbin
<DIR> 4096 bin
<DIR> 4096 home
<DIR> 4096 boot
<DIR> 4096 dev
<DIR> 4096 media
<DIR> 4096 mnt
<DIR> 4096 proc
<DIR> 4096 root
<DIR> 4096 run
<DIR> 4096 sys
<DIR> 4096 tmp
<DIR> 4096 service
<DIR> 4096 e2tfs
<DIR> 4096 srv
<DIR> 4096 sysro
<DIR> 4096 db
<DIR> 4096 vmail
<DIR> 4096 inactive
=>
```

If the `ls` command displays the content of the `/sysro` folder as shown below, then your controller has a pre-9.0 MiVoice Business software:

```
=> ls sata 0:1
4301 3300sw_toc.txt
1436960 bootrom.s3
0 helpfiles.tar.gz.txt
65896436 rtc8260
0 rtc8260.gz.txt
dspconfig/
globalization/
lmttestsignals/
script/
esm_browsedlg_applet/
esm_ftp_applet/
esm_ftp_client/
esm_ftp_display/
install/
symbol/
30 _swrevs
```

```
5 _swvariant
6 ftpproxyport.txt
27 spcversions.txt
17806 taskmonitor.txt
104 wdmmonitor.txt
webs/
0 sysro_common.tar.gz.txt
0 active
61931 post.hex
1022699 dsp_ii_fpga.hexout
0 sysro_common_hw_loads.tar.gz.txt
234535 3xxx_fpga.bit
234535 3xxx_fpga_n12.bit
303284 bcm_cfe.bin
13457525 cxii_fpga.xsvf
567 cxii_fpga.txt
31220 heavy_fpga.bit
41411 kts_fpga.bit
41417 lite_fpga.bit
135198 msp430.s1
651 msp430.txt
135198 msp430n12.s1
653 msp430n12.txt
223064 mxe_bcm_cfe.bin
615412 mxe_fpga.bin
221827 mxe_fpga.bz2
632 mxe_fpga.txt
135204 mxe_msp430.s1
656 mxe_msp430.txt
1947290 mxe_testrom.s3
282472 mxe_testrom_cfe.bin
615412 mxeiii_fpga.bin
228583 mxeiii_fpga.bz2
632 mxeiii_fpga.txt
0 sysro_hd.tar.gz.txt
6129587 dig_largesysal_link.out
1951611 dim_module_link.out
15914228 sip_sdk_link.out
40582163 javalayer_link.out
80294 prowlerppc.out
2190369 prowlerobserverppc.out
0 sysro_ppc.tar.gz.txt
tftp/
0 tftp_analog_amb.tar.txt
0 tftp_analog_asu.tar.txt
0 tftp_analog_coeff.tar.txt
0 tftp_ip.tar.txt
0 tftp_ip_move.tar.txt
0 tftp_ip_move2.tar.txt
0 tftp_mip_bin.tar.txt
```



```

0 tftp_old_ip.tar.txt
0 webs.tar.gz.txt
0 webset.tar.gz.txt
zoneinfo/
0 zone_info.tar.txt
71098 enumfielddata.dat59 file(s), 13 dir(s)
=>

```

7. Run the following commands to determine which MiVoice Business software version is installed on the two bootable partitions by displaying the content of the product_version and/or _swrevs files:

MiVB Release	Platform	Commands (to be run one line at a time)
Pre-9.0	CX II, MXe III/MXe III-L	mw.b 1000000 0 1000 fatload sata 0:1 1000000 _swrevs md.b 1000000 10 mw.b 1000000 0 1000 fatload sata 0:4 1000000 _swrevs md.b 1000000 10
	AX	mw.b 1000000 0 1000 fatload ide 0:1 1000000 _swrevs md.b 1000000 10 mw.b 1000000 0 1000 fatload ide 0:4 1000000 _swrevs md.b 1000000 10
9.0 or later	CX II, MXe III/MXe III-L	md.b 1000000 10 ext4load sata 0:1 1000000 /usr/libexec/mitel-3300icp/sysro/product_version md.b 1000000 9 mw.b 1000000 0 1000 ext4load sata 0:2 1000000 /usr/libexec/mitel-3300icp/sysro/product_version md.b 1000000 9
	AX	mw.b 1000000 0 1000 ext4load ide 0:2 1000000 /usr/libexec/mitel-3300icp/sysro/product_version md.b 1000000 9 mw.b 1000000 0 1000 ext4load ide 0:3 1000000 /usr/libexec/mitel-3300icp/sysro/product_version md.b 1000000 9

In the above tables, the first command (mw.b) clears out 0x1000 bytes in RAM starting at the location 0x1000000 to create space for reading in the product_version file.

The second command (fatload or ext4load) reads the product_version file into RAM at 0x1000000.

NOTE: If the disk features a pre-9.0 MiVoice Business software release that was never upgraded, then partition 4 is empty. In this case, the system's response is: **** Invalid partition 4 ****, and the active partition number is 1.

The third command (md.b) displays the read content both in hex and ASCII.

Then, these commands are repeated for the other partition.

For example, if you have a CX II or MxIII/MxIII-L controller with MiVoice Business Release 9.0 or later, then an example of a system response to the appropriate command taken from the table above is as follows:

```
=> mw.b 1000000 0 1000
=> ext4load sata 0:1 1000000 /usr/libexec/mitel-3300icp/sysro/product_version
9 bytes read in 408 ms (0 Bytes/s)
=> md.b 1000000 9
01000000: 39 2e 31 2e 30 2e 34 38 0a 9.1.0.48.
=> mw.b 1000000 0 1000
=> ext4load sata 0:2 1000000 /usr/libexec/mitel-3300icp/sysro/product_version
9 bytes read in 199 ms (0 Bytes/s)
=> md.b 1000000 9
01000000: 39 2e 30 2e 32 2e 31 36 0a 9.0.2.16.
=>
```

In the above example, the system response indicates that partition 1 features MiVoice Business Release 9.1.0.48 and partition 2 features MiVoice Business Release 9.0.2.16; now, if you know that the active MiVoice Business software version on the disk is say, 9.1.0.48, then you can conclude that the partition with that MiVoice Business software version (partition 1) is the active partition on your disk, and you can configure the system's bootloader to boot the MiVoice Business application from partition 1.

However if you recently acquired the disk, and do not know the active or inactive MiVoice Business software version on this disk, see [Step 8](#).

8. The date and time of creation of files within the **/db/spyLog/resource** folder on a partition are recorded in the filename. The more recent the time of creation of **/db/spyLog/resource** files on a certain partition, the more likely that this is the active partition. Run the following commands to list the files within the **/db/spyLog/resource** folder on both partitions of the disk:

MiVB Release	Platform	Commands (to be run one line at a time)
Pre-9.0	CX II, MxIII/MxIII-L	For the bootable partition 1: ls sata 0:2 spyLog/resource For the bootable partition 4: ls sata 0:5 spyLog/resource
	AX	For the bootable partition 1: ls ide 0:2 spyLog/resource For the bootable partition 4: ls ide 0:5 spyLog/resource
9.0 or later	CXII, MxIII/MxIII-L	ls sata 0:1 /var/mivb/active/db/spyLog/resource ls sata 0:2 /var/mivb/active/db/spyLog/resource
	AX	ls ide 0:2 /var/mivb/active/db/spyLog/resource ls ide 0:3 /var/mivb/active/db/spyLog/resource

For example, if you have a CX II or MxIII/MxIII-L controller with MiVoice Business Release 9.0 or later, the following is an example of a system response to the appropriate command:

```
=> ls sata 0:1 /var/mivb/active/db/spyLog/resource
<DIR> 4096 .
<DIR> 4096 ..
32294 resmon.log
28130 procmon.procmon.log
8091764 resmoncpu.rrd
8091764 resmonmem.rrd
<DIR> 4096 procmon
3 miso_time.txt
247105 resmoncpu_20190823_101047_8h.csv
230161 resmonmem_20190823_101050_8h.csv
1392 availInfo.bin
245859 resmoncpu_20190823_020827_8h.csv
231374 resmonmem_20190823_020830_8h.csv
740871 resmoncpu_20190822_180627_1d.csv
712374 resmonmem_20190822_180634_1d.csv
30962 resmoncpu_20190823_181547_1h.csv
31312 resmonmem_20190823_181548_1h.csv
632078 resmoncpu_20190821_175827_1d.csv
630687 resmonmem_20190821_175833_1d.csv
31021 resmoncpu_20190823_141217_1h.csv
28886 resmonmem_20190823_141218_1h.csv
12715 resmoncpu_20190823_154402_1h.csv
12263 resmonmem_20190823_154404_1h.csv
716065 resmoncpu_20190823_161522_1d.csv
670836 resmonmem_20190823_161541_1d.csv
12156 resmoncpu_20190823_161046_1h.csv
12933 resmonmem_20190823_161047_1h.csv
12456 resmoncpu_20190823_154838_1h.csv
12425 resmonmem_20190823_154842_1h.csv
31315 resmoncpu_20190823_131147_1h.csv
28424 resmonmem_20190823_131148_1h.csv
30455 resmoncpu_20190823_171537_1h.csv
31345 resmonmem_20190823_171538_1h.csv
=> ls sata 0:2 /var/mivb/active/db/spyLog/resource
<DIR> 4096 .
<DIR> 4096 ..
223286 resmon.log
109270 procmon.procmon.log
8091764 resmoncpu.rrd
8091764 resmonmem.rrd
<DIR> 4096 procmon
4 miso_time.txt
8939 resmoncpu_20190718_175756_1h.csv
9327 resmonmem_20190718_175800_1h.csv
1392 availInfo.bin
7275 resmoncpu_20190722_142751_1h.csv
```

```
7300 resmonmem_20190722_142753_1h.csv
736593 resmoncpu_20190715_151256_1d.csv
679902 resmonmem_20190715_151304_1d.csv
7275 resmoncpu_20190727_185448_1h.csv
7300 resmonmem_20190727_185450_1h.csv
9076 resmoncpu_20190727_185919_1h.csv
9170 resmonmem_20190727_185923_1h.csv
736485 resmoncpu_20190714_150356_1d.csv
677734 resmonmem_20190714_150403_1d.csv
59148 resmoncpu_20190820_213526_8h.csv
59630 resmonmem_20190820_213529_8h.csv
736406 resmoncpu_20190717_143210_1d.csv
712672 resmonmem_20190717_143217_1d.csv
736916 resmoncpu_20190716_142230_1d.csv
738044 resmonmem_20190716_142237_1d.csv
245282 resmoncpu_20190717_062910_8h.csv
237672 resmonmem_20190717_062912_8h.csv
7275 resmoncpu_20190820_213053_1h.csv
525 resmonmem_20190820_213055_1h.csv
8885 resmoncpu_20190722_143225_1h.csv
9160 resmonmem_20190722_143229_1h.csv
7275 resmoncpu_20190718_175324_1h.csv
7300 resmonmem_20190718_175325_1h.csv
738850 resmoncpu_20190711_143456_1d.csv
711696 resmonmem_20190711_143503_1d.csv
737609 resmoncpu_20190712_144416_1d.csv
691701 resmonmem_20190712_144423_1d.csv
736695 resmoncpu_20190713_145356_1d.csv
677831 resmonmem_20190713_145403_1d.csv
=>
```

In the above example, the system response indicates that the newer set of resmon files (dates in the range of 21/08 to 23/08) are on partition 1; hence, partition 1 is the last known active partition.

9. To verify whether the MiVoice Business application in the last known active partition booted and completed the startup the last time it was run, check whether the text **s10startup done** is present at the end of the **/db/log/appStartup.log** file; run the following commands to display the content of this file:

MiVB Release	Platform	Commands (to be run one line at a time)
Pre-9.0	CX II, MXe III/MXe III-L	For the bootable partition 1: mw.b 1000000 0 1000 ext4load sata 0:2 1000000 log/appStartup.log md.b 1000000 800 For the bootable partition 4: mw.b 1000000 0 1000 ext4load sata 0:5 1000000 log/appStartup.log md.b 1000000 800
	AX	For the bootable partition 1: mw.b 1000000 0 1000 ext4load ide 0:2 1000000 log/appStartup.log md.b 1000000 800 For the bootable partition 4: mw.b 1000000 0 1000 ext4load ide 0:5 1000000 log/appStartup.log md.b 1000000 800
9.0 or later	CX II, MXe III/MXe III-L	mw.b 1000000 0 1000 ext4load sata 0:1 1000000 /var/mivb/active/db/log/appStartup.log md.b 1000000 800 ext4load sata 0:2 1000000 /var/mivb/active/db/log/appStartup.log md.b 1000000 800
	AX	mw.b 1000000 0 1000 ext4load ide 0:2 1000000 /var/mivb/active/db/log/appStartup.log md.b 1000000 800 ext4load ide 0:3 1000000 /var/mivb/active/db/log/appStartup.log md.b 1000000 800

NOTE: The text **s10startup done** may be split at random places in the ASCII part of the displayed content.

Upgrade 3300 ICP Controller's Bootloader Without Using a Hard Disk

Overview

This section describes how to upgrade the bootloader of a 3300 ICP controller without using its hard disk. The bootloader can be upgraded from Bootrom to U-Boot, or downgraded from U-Boot to Bootrom; to execute either of these procedures, your system does not require a disk drive to be installed. The procedures are applicable to MXe III, CXi II or AX controller types.

To upgrade the Bootrom to U-Boot without using a hard disk drive, you must configure the Bootrom to boot the **RTC_Migrate_FLASH** image from your FTP server.

To downgrade the U-Boot to Bootrom, you must configure the U-Boot to boot the **RTC_Upgrade_FLASH** image from your TFTP server.

The procedure takes approximately two minutes to execute, excluding the time required to set up FTP and TFTP servers.

Before you Begin

Ensure that you have:

- Downloaded the **migrateflash.zip** archive from the *Mitel Software Download Center* --> *Navigate by categories* --> *MiVoice Business* --> *Migrate Flash Utility for 3300 ICP Controllers* on the *MiAccess* site.
- Configured an external FTP server (for example, <http://filezilla-project.org>) as specified in the [Setup](#) section.

NOTE: The above prerequisites are common to the procedures for both, upgrading and downgrading the bootloader of a 3300 ICP Controller.

Prerequisites for the Upgrade Procedures

Ensure that you have:

- Acquired and installed a 1 GiB RAM module (applicable only to MxIII and CXi II controllers); otherwise **RTC_Migrate_FLASH** rejects the request to upgrade the bootloader.

Prerequisites for the Downgrade Procedure

Ensure that you have:

- Configured an external TFTP server (for example, **Tftpd64** from <http://tftpd64.jounin.net>) as specified in the [Setup](#) section.
- Configured the Maintenance port of your controller for the default baud rate of 9600 bps; for verification, run the following command:

```
print baudrate
```

The value of the `baudrate` variable is displayed. If the `baudrate` variable is not set to **9600**, then run the following command:

```
setenv baudrate 9600
```

The following system response is displayed:

```
"##Switch baudrate to 9600 bps and press ENTER..."
```

Modify your terminal emulator application's baudrate to 9600 bps and then, press the ENTER key at least once to verify that you get the U-Boot prompt. Save the change using the `saveenv` command.

Contents of the Migrateflash.zip archive

Table 6.1: Contents of the **migrateflash.zip** archive

File Name	Comment
RTC_Migrate_FLASH	VxWorks-based image that flashes in platform-specific U-Boot and a subset of other firmware components.
RTC_Upgrade_FLASH	VxWorks-based image that flashes in Bootrom and a subset of other firmware components.
flash-mxeiii.tar.gz	MXe III U-Boot 1.0.3.11 packaged as bootrom.s3 and FPGA binaries.
flash-cxeii.tar.gz	CXi II U-Boot 1.0.3.11 packaged as bootrom.s3.
flash-ax.tar.gz	AX U-Boot 1.0.3.11 packaged as bootrom.s3 and FPGA binaries.
flash.tar.gz	14.0.3.51 version of Bootrom, FPGA, CFE, MSP430, AX line card CPLD.

Setup

As part of the initial setup process, you must complete the following steps before executing the procedure:

1. On the FTP server, create a user and extract the contents of the **migrateflash.zip** archive to the user's home directory. For example, assume that the FTP user name is **migrateflash**, the user's password is **passwd** and the user's home directory is **D:\FTP\migration**.
2. For downgrading U-Boot to Bootrom, you also must set up a TFTP Server. On the TFTP server, you must either:
 - Make **D:\FTP** home directory of the TFTP Server (applicable only if the TFTP server is on the same machine as the FTP server), or
 - Create a new directory named migration in the TFTP server's home directory and copy the **RTC_Upgrade_FLASH** file here
3. Set up access to the controller's Maintenance port (serial port). Set up the terminal emulator application (for example, PuTTY) with the following default parameters:
 - **Baud Rate:** 9600
 - **Data Bits:** 8
 - **Stop Bits:** 1
 - **Parity:** None
 - **Flow Control:** None

NOTE: Controllers with Bootrom support a baud rate value of 9600 only. Controllers with U-Boot use 9600 as the default baud rate value, but also support a range of other values. If you modified the de-

*fault baud rate for U-Boot (that is, U-Boot variable **baudrate**), you must change it back to 9600 (see [commands](#)) and save the change before you can perform a downgrade to Bootrom.*

Procedures

Upgrade Bootloader from Bootrom to U-Boot (MXe III and CXi II)

To upgrade the bootloader of a 3300 ICP Controller from Bootrom to U-Boot:

1. Power on the controller.
2. Stop the auto-boot sequence by pressing the SPACE key three or more times consecutively within seven seconds at the following prompt:

Press <SPACE><SPACE><SPACE> to stop auto-boot AFTER countdown starts...

3. Run the following command to boot the **RTC_Migrate_FLASH** over the network from the external FTP server that you configured:

c

For example, the parameters for an FTP server with IP address: 10.35.5.38 and FTP username/password: migrateflash/passwd (configured as described in step 1 of [Setup](#)) can be changed as displayed below. The value of a parameter is changed by entering its new value after the current value (text in bold in the example below):

```
boot device : ata=00 qefcc
processor number : 0
host name :
file name : /partition1/RTC8260 RTC_Migrate_FLASH
inet on ethernet (e) : 10.38.72.57:ffffff00
inet on backplane (b) :
host inet (h) : 192.168.1.4 10.35.5.38
gateway inethist (g) : 10.38.72.1
user (u) : ftp migrateflash
ftp password (pw) (blank = use rsh) : @ passwd
flags (f) : 0x0
target name (tn) : swecxii-1
startup script (s) :
other (o) : qefcc
```

4. Run the following command to boot the **RTC_Migrate_FLASH** image:

@

If you have configured both the FTP server and the bootline properly in Step 3, the Bootrom downloads the **RTC_Migrate_FLASH** image and transfers control to it. This file then determines the platform type (MXe III, CXi II or AX), and verifies that 1 GiB RAM module is installed on the controller (for MXe III and CXi II controllers only). If 1 GiB RAM module is not installed on the controller, then the system informs you that the 1 GiB RAM module is required and aborts the upgrade. If the RAM requirements are satisfied, the **RTC_Migrate_FLASH** file downloads the platform-specific flash.tar file, and checks the bootrom.s3 file to confirm that it features platform-specific U-Boot content. **RTC_Mi-**

grate_FLASH then flashes this content to the bootloader partition of the system FLASH. If the platform is MxIII or AX, **RTC_Migrate_FLASH** also attempts to upgrade content of the FPGA system FLASH partition. On successful completion, the **RTC_Migrate_FLASH** indicates success, and initiates system reboot after 10s.

The U-Boot starts running.

5. Stop the auto-boot sequence by pressing the SPACE key three or more times consecutively within seven seconds at the following prompt:

```
Press <SPACE> key 3 times within 7 seconds to stop autoboot
```

6. Power off the system.

The system is now ready for the installation of a hard disk/CF (if present).

NOTE: Hard disks with MiVoice Business Release 9.0 or later are platform specific (MxIII, CXi II or AX). A CXi II disk with MiVoice Business 9.0 or later cannot be used on an MxIII controller or vice versa.

NOTE: If you do not know the active partition of the new disk, see [Determine Last Known Active Partition using U-Boot](#).

Upgrade Bootloader from Bootrom to U-Boot (AX)

The procedure for the AX controller is the same as [Upgrade Bootloader from Bootrom to U-Boot \(MxIII and CXi II\)](#), with the following difference:

- In Step 3, enter **motfcc**, and not **qefcc**, as the value of the `boot device` parameter.

Downgrade Bootloader from U-Boot to Bootrom

To downgrade the bootloader of a 3300 ICP controller from U-Boot to Bootrom:

1. Power on the controller.
2. Stop the auto-boot sequence by pressing the SPACE key three or more times consecutively within seven seconds at the following prompt:

```
Press <SPACE> key 3 times with 7 seconds to stop autoboot
```

3. Configure U-Boot to TFTP VxWorks-based image **RTC_Upgrade_FLASH** from the external TFTP server, and input the location of the external FTP server that **RTC_Upgrade_FLASH** uses to download `flash.tar.gz`, using one of the following two methods:

- The `run vxbootcfg` command (available only for U-Boot 1.0.3.11 or later)
- The `setenv` command

Using the `vxbootcfg` command

The `run vxbootcfg` command allows for the configuration of individual system parameters, one at a time. If you do not want to change the value of a particular system parameter, press ENTER to move on to the next system parameter in the list. If you want to delete the current value of a system parameter, and set it to a blank value, press the `.` key.

For example, for a TFTP and FTP server both with IP address 10.35.5.38, modify the fields as below. The value of a parameter is changed by entering its new value after the colon:

```
run vxbootcfg
```

```
. = clear field, <ENTER> = no change
```


The U-Boot will download the **RTC_Upgrade_FLASH** file and transfer control to it. This file then downloads flash.tar file, extracts its content, and flashes Bootrom to the bootloader partition of the system FLASH. On successful completion, the system indicates that it is rebooting; after 10 seconds, it transfers control to Bootrom.

5. Stop the auto-boot sequence by pressing the SPACE key three or more times consecutively within seven seconds at the following prompt:

```
Press <SPACE><SPACE><SPACE> to stop auto-boot AFTER countdown starts...
```

6. Power off the system.

The system is now ready for the installation of a hard disk/CF (if present).

NOTE: A 3300 ICP controller with Bootrom is unable to boot MiVoice Business 9.0 or later.

Upgrade 3300 ICP Controller's Bootloader using the Migration Tool

Overview

This section describes the procedure to upgrade the bootloader of a 3300 ICP Controller from Bootrom to U-Boot, given the availability of a hard disk with a pre-9.0 MiVoice Business software version installed on it.

Use this procedure if you are required to replace your controller (or RTC card for an MxIII controller) running MiVoice Business Release 9.0 or later, and the new controller/RTC card ordered from Mitel features Bootrom as the bootloader (to determine the bootloader, see [Determine 3300 ICP Controller Bootloader](#)). Since Bootrom cannot boot MiVoice Business Release 9.0 or later, the use of a hard disk with a pre-9.0 MiVoice Business software version is required to allow Bootrom to boot a pre-9.0 MiVB release, which in turn, enables the system to connect to the Migration Tool for migration of the bootloader from Bootrom to U-Boot.

The alternative procedure for upgrading a 3300 ICP Controller's Bootloader is [Upgrade 3300 ICP Controller's Bootloader Without Using a Hard Disk](#).

Before you Begin

Ensure that:

- You have a new or used 3300 ICP hard disk drive with a pre-9.0 MiVoice Business software version installed on it.

Procedure

1. Install the hard disk with a pre-9.0 MiVoice Business software version on a controller with Bootrom (see **New Disk Drive Installation (3300 ICP Controller)** in the *MiVoice Business Technician's Handbook, Release 9.0 SP3*).
Do not power on the controller yet.
2. [Access 3300 ICP Controller Through the Maintenance Port](#).

3. Power on the controller and observe the output on the Maintenance Port.
4. After the count-down starts, press SPACE three times to stop auto-boot.
5. When the prompt **[VxWorks Boot]:** gets displayed, run the following command and change bootline parameter values to configure the networking parameters and the partition number.
6. Run the following command to reboot the controller:

```
@
```
7. After the new controller boots up, follow the steps below to migrate the controller's bootloader from Bootrom to U-Boot using the Migration Tool:
 - a. Launch the Migration Tool.
 - b. Connect the migration tool to the controller by entering the controller's **IP Address or FQDN** and the System Administration Tool's login credentials.
 - c. Select the **Migration with Media Replacement** option under **Step 1**. Select the sub-option **Bootloader Upgrade only**.
 - d. Enter the location of the **External Repository** or **Internal Repository** that contains the bootloader software. Click **Next**.
 - e. Select the **Use current network configuration** option. Click **Next**.
 - f. Click **Start**.

The bootloader migration process begins.

8. After the migration of the bootloader completes successfully, close the Migration Tool session and the Migration Tool. From the Maintenance port (communication application), run the following command:

```
appShutdown 3
```

Observe the output and power off the system when the system says it is safe to do so.

9. Remove the hard disk with a pre-9.0 MiVoice Business software version from the controller.

Configuring the Server using Server Console

Overview

Server Console provides a console version of the Server Manager. The following sections help you access and perform tasks on a 3300 ICP controller:

- [Accessing Server Console](#)
- [Checking the server status](#)
- [Configuring the server](#)
- [Reboot or shut down the server](#)
- [Managing trusted networks](#)
- [Backing up the database](#)
- [Restoring a database](#)

NOTES:

- The **Register for ServiceLink** option is currently is not supported for 3300 ICP based MiVoice Business systems.
- The following procedures also apply to x86-based controllers. However, the options presented during the configuration may slightly vary.

Accessing Server Console

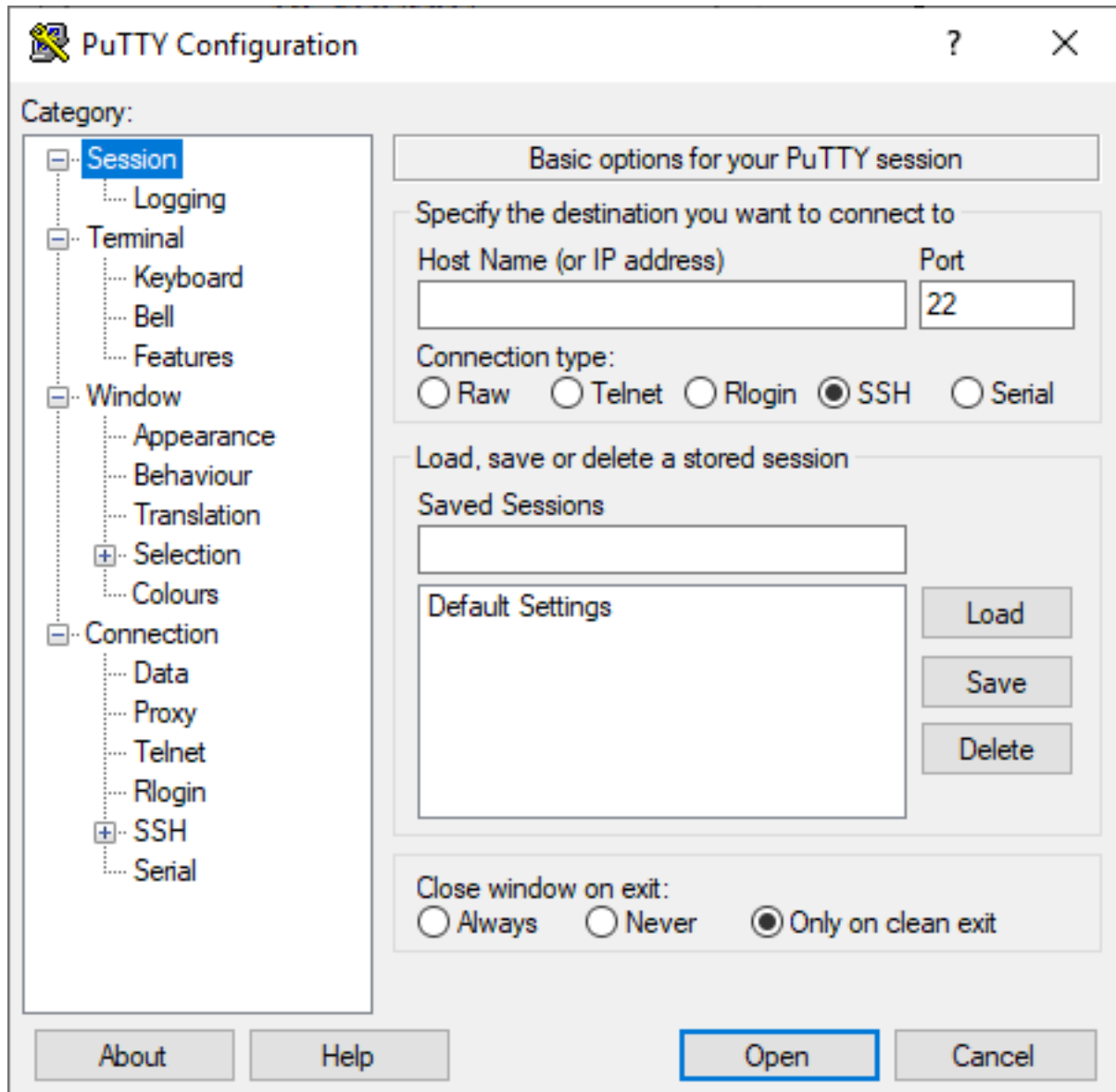
This section describes the two procedures to access the Server Console program. You can perform either of the two procedures for accessing the Server Console.

Do one of the following:

- Method 1 (on premise) - See [Access 3300 ICP Controller Through the Maintenance Port](#).
- Method 2 (Remote) - Connect to the MiVoice Business system using a terminal emulator application (for example, PuTTY).

NOTE: Before you begin, ensure that you have enabled SSH access through the Server Manager (**Security > Remote Access**).

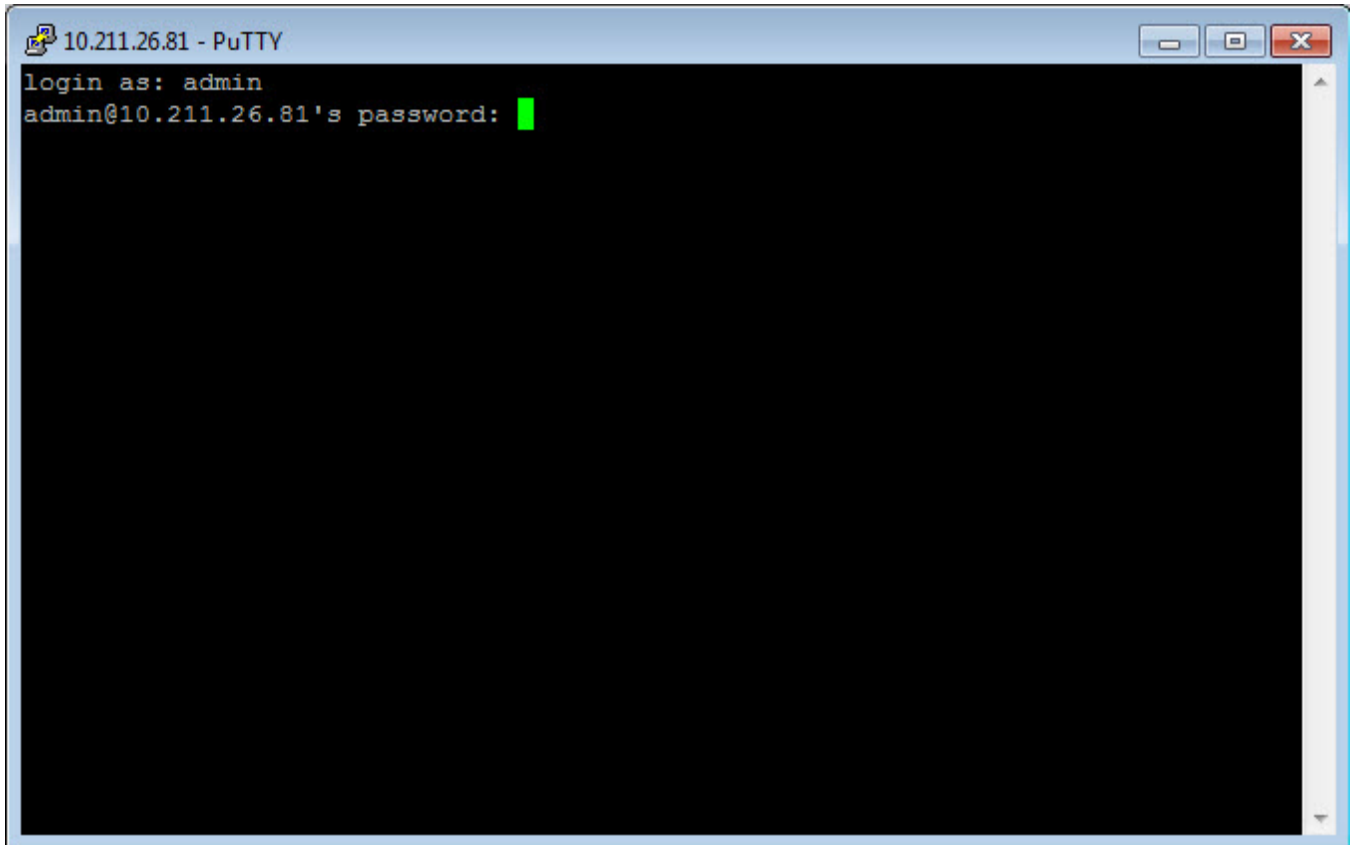
- a. Launch a terminal emulator application.
- b. In the **Host Name (or IP address)** field, type the IP address of the MiVoice Business system.



c. Select **SSH** under **Connection** type, and then click **Open**.

The login prompt is displayed.

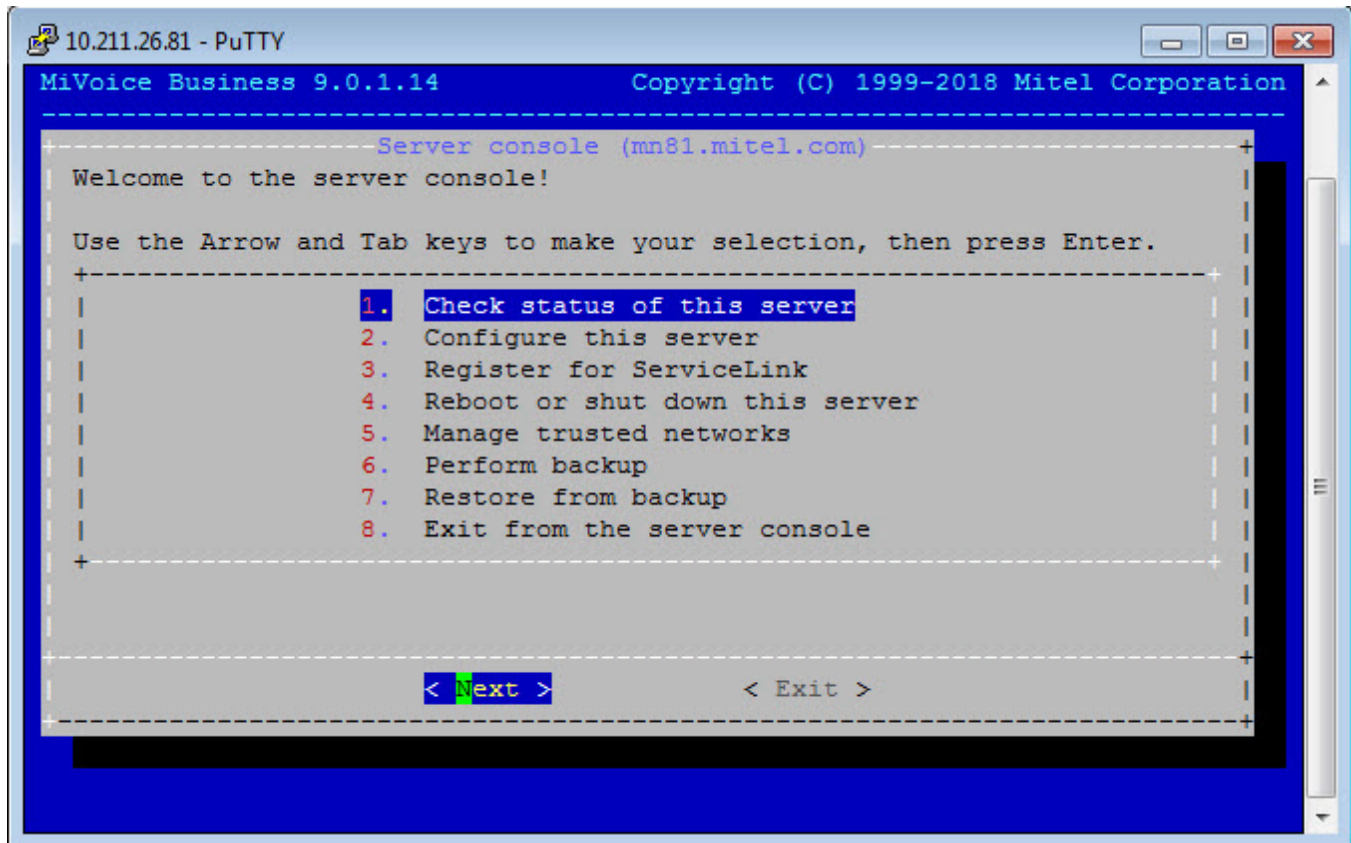
d. At the login prompt (**login as:**), type **admin** (user *admin*) and press the ENTER key.



NOTE: You can also log in as the root user and type **su admin** to switch to the admin user.

- e. At the password prompt, type the administrator password, and press the ENTER key.

NOTE: If the following error message is displayed: *ADMIN LOGIN IS BLOCKED UNTIL MIVOICE BUSINESS IS STARTED*, the MiVoice Business application has not completed the startup. Wait for the system to boot fully, and the MiVoice Business application to complete the startup; this usually takes less than 15 minutes from the moment the system starts booting. If the application does not complete its startup even after 20 minutes (for example, 3300 ICP controller and/or RTC Card replacement scenarios), see **Ch 4, Software > System Software** in the MiVoice Business Troubleshooting Guide, Release 9.1.



NOTE: The following procedures, except Restore a Database, can be performed using either Method 1 or Method 2. The procedure Restore a Database can be performed using Method 1 or from **Administration > Restore** in Server Manager.

Checking the server status

This section describes the procedure to check the status of the server from the Server Console.

1. In the server console main menu, click **1. Check status of this server**, and then click **Next**.
The system displays the duration for which the server was running in days, hours, and minutes.
2. Click **OK** to return the main menu.

Configuring the server

This section describes the procedure to perform network configuration changes to the server from the Server Console.

1. In the server console main menu, click **2. Configure this server**, and then click **Next**.
2. In the configuration screens, enter the following settings:

Screen	Action
Primary domain name	Enter the domain name (for example, mitel.com).
Enter system name	Enter a system name (for example, your company name)
Select local network adapters.	Select one or more network adapters. NOTES: <ul style="list-style-type: none"> This screen is displayed only for an EX controller. If you have restored a database from the MiVoice Business Virtual system in an EX controller, then after the restore, select eth1 virtio_net - <IP address of the adapter> [eth1: UP].
Local networking parameters	Enter an available IP address (without leading zeros) that is used to access both the Server Manager and the MiVoice Business system.
Enter local subnet mask	Enter the IP address of the subnet mask.
Enter gateway IP address	Enter the gateway IP address.
DNS server addresses	Enter one or more corporate DNS server IP addresses, separated by a comma.

3. Do one of the following:

- If you have modified only **DNS server addresses** configuration setting, click **Finish** to save the configuration changes.
The configuration settings are applied without rebooting the system.
- If you have modified any other configuration setting, click **Reboot**.
The configuration settings are applied upon system reboot.

Reboot or shut down the server

This section describes the procedure to reboot or shut down the server from the Server Console.

1. In the server console main menu, click **4. Reboot or shut down this server**, and then click **Next**.
2. In the configuration screens, select the following settings:

Screen	Action
Reboot or shutdown this server	Click one of the following, and then click OK . <ul style="list-style-type: none"> Reboot this sever Shutdown this server

3. Click **Yes** to proceed.

Managing trusted networks

This section describes the procedure to display, add and delete trusted networks from the Server Console.

1. In the server console main menu, click **5. Manage trusted networks**, and then click **Next**.
2. In the configuration screens, select the following settings:

Screen	Action
Trusted Networks Operations	<ul style="list-style-type: none"> • Click 1. Show trusted networks, and then click Next. The system displays the trusted IPv4 networks. • To add IPv4 trusted networks, click 2. Add IPv4 trusted network, and then click Next. <ol style="list-style-type: none"> a. Enter the IP address, and then click Next. b. Enter the subnet mask, and then click Next. c. Enter the gateway IP address, and then click Next. • To delete the trusted IPv4 networks added, click 3. Delete IPv4 trusted network, and then click Next. <ul style="list-style-type: none"> – Click to select the network you want to delete, and then click Next.

Backing up the database

This section describes the procedure to perform a backup of the MiVoice Business system configuration, server configuration, and the user data to a network file share server. Two file-sharing protocols are supported:

- Samba (SMB)/Common Internet File System (CIFS)
- Secure File Transfer Protocol (SFTP) To back up the database:

1. In the server console main menu, click **6. Perform backup**, and then click **Next**.
2. In the configuration screens, select the following settings:

Screen	Action
Backup server IP address	Enter the IP address of the network file share server where you want to store the database backup file.

Screen	Action
Backup server domain or workgroup name	Enter the Domain or workgroup name. Applies only to SMB/CIFS. Leave the field blank for SFTP. Sets the SMB domain of the user name. If the domain specified is the same as the server's NetBIOS name, then the server's local Security Account Manager (SAM) is used for authentication, instead of the domain SAM. This field is required only for the SMB/CIFS protocol.
Backup share name	Enter the file-share name. Applies only to SMB/CIFS. Leave the field blank for SFTP. The restore utility will try to connect to the server/shared folder as an SMB/CIFS resource. The shared folder must have permissions set to Full Control .
Optional Directory Path	Enter the name of the sub-folder where you have stored the database backup file. For SMB/CIFS, the sub-directory is relative to the share. For SFTP, the sub-directory is relative to the root of the file system accessed through the SFTP protocol.
Backup username	Enter the user name to use when connecting to the network file share server.
Backup password	Enter the password to use when connecting to the network file share server.
Proceed with Backup to network	Click Proceed .

The system creates a database backup file in the specified directory on the file server.

Restoring a database

This section describes the procedure to restore a server backup file stored on a network file share. Two file-sharing protocols are supported:

- Samba (SMB)/Common Internet File System (CIFS)
- Secure File Transfer Protocol (SFTP) To back up the database:

WARNING: Restoring a database deletes your current application configuration and user data.

NOTE: You can also restore the database using Server Manager. Log in to Server Manager, and click **Restore** under **Administration**.

1. In the Server Console main menu, click **7. Restore from a backup**, and then click **Next**.
2. In the configuration screens, select the following settings:

Screen	Action
Restore after Reboot	Click Reboot Now . The system reboots the server.
Local networking parameters	Enter an available IP address that is used to access both the Server Manager and the MiVoice Business system.
Select local subnet mask	Enter the IP address of the subnet mask.
Select backup/restore server IP address	Enter the IP address of the network file server where you have stored the database backup.
Backup server domain or workgroup name	Enter the Domain or workgroup name. Applies only to SMB/CIFS. Leave the field blank for SFTP. Sets the SMB domain of the user name. If the domain specified is the same as the server's NetBIOS name, then the server's local Security Account Manager (SAM) is used for authentication, instead of the domain SAM. This field is required only for the SMB/CIFS protocol.
Backup share name	Enter the file-share name. Applies only to SMB/CIFS. Leave the field blank for SFTP. The restore utility will try to connect to the server/shared folder as an SMB/CIFS resource. The shared folder must have permissions set to Full Control .
Optional Directory Path	Enter the name of the sub-folder where you have stored the database backup file. For SMB/CIFS, the sub-directory is relative to the share. For SFTP, the sub-directory is relative to the root of the file system accessed through the SFTP protocol.
Backup username	Enter the user name to use for connecting to the network file share server.
Backup password	Enter the password to use for connecting to the network file share server.
Choose backfile to restore from	Select the database backup file you want to restore, and click Next .
Start restore from backup	Click Yes .

Screen	Action
Restoring from network share	Displays the progress of the restore. NOTE: <ul style="list-style-type: none"> The screen displays only the last restore status of the server. The screen page does not display the restore status of the applications installed on the server. You must check the restore status of an application through the application for example, by logging in to the application. If the restore fails, see the MiVoice Business Software logs for more information.
Restore successful	Click Reboot .

Access the E2T Card console on MXe III/MXe III-L Controller

Connect to the E2T Card console

To connect to the E2T card console on an MXe III/MXe III-L controller, you can use either of the following methods:

- [Connect through an SSH session of the RTC Card](#)
- [Connect through the Controller Printer Port](#)

NOTE: The default baud rate for the E2T card console is 9600. For information about modifying the default baud rate, see [Modify Default Baud Rate of the System console \(3300 ICP Controller\)](#).

Connect through an SSH session of the RTC Card

1. Log in to the Server Manager and go to the **Security > Remote Access** page. In the **Secure shell access** drop-down list, select **Allow access only from trusted and remote management networks** and click **Save**.
2. Log in to the RTC card through SSH as *root*.
3. Run the following command to connect the E2T card's serial port to this terminal:

```
e2tCardConsoleStart
```

NOTE: If the system response is that **Device/dev/ttyQE1** is locked, then there is already an active connection with either the E2T card or MIPS processor through this device. However, the device can be connected to only one source at a time. To terminate the existing minicom session, run the *e2tCard-ConsoleStart* command with the *-f* option.

The usage format of the *e2tCardConsoleStart* command is presented when you run this command with the *-h* option:

```
e2tCardConsoleStart -h
```

e2tCardConsoleStart connects E2T card's serial port to this terminal.

```
Usage: e2tCardConsoleStart [-f] [ -b {9600|19200|38400|57600|115200} ]  
-<baudrate>: sets supported baud rate; default is 9600  
-f: force terminate pre-existing minicom session first  
-h|-help|--help : displays this usage info
```

4. Press the ENTER key.
5. If the login prompt is displayed, log in as *root*.

NOTE: If the login prompt is not displayed, check whether the E2T card is connected to the RTC card. To do this, log in to the System Administration Tool and go to the **Hardware Compute Cards** form; here, check the status of the card in **Slot ID 2**. If the status is **Not Responding**, then see *Unable to Boot the E2T Card on an MXe III/MXe III-L Controller*.

When you have finished working with the E2T card, [Disconnect from the E2T Card Console](#).

Connect through the Controller's Printer Port

The E2T card's serial port is, by default, connected to the printer port after system startup with 9600 as the default baud rate.

1. Connect an RS-232 serial cable from a COM port (for example COM1) on your PC to the **Printer** port on the controller; the **Printer** port is internally connected to the serial port of the E2T card.
NOTE: The MXe III/MXe III-L controller has two DB-9 ports at the front labeled, **Printer** and **RS-232** (Maintenance port). The Printer port is used for accessing the E2T card's serial port and the **RS-232** port is used for accessing the RTC card's serial port. For more information, see the **Chapter 1 3300 ICP Controllers > 3300 ICP Controller Units > MXe Controller** in the MiVoice Business Hardware Technical Reference Manual document.
2. Open a communication application (for example, PuTTY) on your PC and set the connection parameters as follows:
 - **Connection type:** Serial
 - **Port:** Select any COM port; for example, COM1.
 - **Bits Per Second:** 9600
 - **Data Bits:** 8
 - **Parity:** None
 - **Stop Bits:** 1
 - **Flow Control:** None
3. Click the communication application window and press the ENTER key a few times, and observe the output in the communication application.

If there is no output, check the following and repeat the step.
 - Ensure that there is only one active connection with the E2T card console by accessing the RTC card's Linux shell either through the maintenance port or an SSH session and executing the `e2tCardConsoleStop` command.
4. If the login prompt is displayed, log in as *root*.

NOTE: If the login prompt is not displayed, check whether the E2T card is up and connected to the RTC card. To do this, log in to the System Administration Tool and go to the **Hardware Compute Cards** form; here, check the status of the card in **Slot ID 2**. If the status is **Not Responding**, then see *Unable to Boot the E2T Card on an MXe III/MXe III-L Controller*.

5. To verify that you are connected to the E2T card's shell, run the following command:

```
fw_printenv slot
```

System Response:

```
slot = 1
```

If the system response is `slot=0`, then you are connected to the RTC card's shell and not to the E2T card's shell. Repeat step 1 and ensure that the serial cable is connected to the **Printer** port. When you have finished working with the E2T card, [Disconnect from the E2T Card Console](#).

Disconnect from the E2T Card Console

Disconnect from the E2T Card Console (RTC Card SSH Session)

If the E2T card console session is connected to the RTC card through an SSH session, then you must disconnect and redirect the E2T card to the **Printer** port after you are done using the console.

1. Log out from the E2T card console by running the following command: **logout**
2. After you are logged out, press CTRL + A followed by the X key.
3. At the **Leave Minicom** prompt, press the ENTER key to select the Yes option. If the **Yes** option is not highlighted, then use the TAB key to highlight the **Yes** option and then press ENTER key to select the Yes option.

System Response:

Hanging up

The system disconnects the E2T card console session from the RTC card SSH session.

4. Redirect the E2T card serial port to the **Printer** port of the controller by running the following command:

```
e2tCardConsoleStop
```

Disconnect from the E2T Card Console (Printer port)

1. Run the following command in the communication application to log out of the E2T card console:

```
logout
```

2. If you are disconnecting the RS-232 serial cable from the PC, ensure that you also disconnect the other end of the cable from the **Printer** port of the controller.

Modify Default Baud Rate of the System Console (3300 ICP Controller)

NOTE: A system reboot will be required to activate the new baud rate setting.

The default baud rate of both the system console (Maintenance port) and the MxIII/MxIII-L E2T card console (**Printer** port) is 9600. To modify the baud rate:

1. If you want to modify the baud rate of the system console, connect to the Maintenance port (through an RS-232 cable or SSH). If you want to modify the baud rate of the E2T card console, connect to the E2T card console (see [Access the E2T Card Console on MxIII/MxIII-L Controller](#)).
2. Run the following command to set a new baud rate value (select a value only from the supported values below):

```
fw_setenv baudrate <9600, 19200, 38400, 57600 or 115200>
```

3. To activate the new baud rate, reboot the system from the Server Manager (**Administration > Shut-down or reboot**).

Determine Bootloader of the E2T card

To determine the issue, you must first determine the bootloader of the E2T card:

1. [Connect to the E2T Card Console](#)
2. Connect to the RTC card shell either through SSH or the serial port asroot.
3. In the RTC card shell, run the following commands to reset the E2T card, and observe the output in the E2T card's serial port.

```
mcdDebug CpuOff 1  
mcdDebug CpuOn 1
```

4. In the E2T card shell, press the SPACE key three or more times at the following prompt to stop the autoboot:

```
Press <SPACE> key 3 times within 7 seconds to stop autoboot
```

5. If the prompt is[VxWorks Boot]:, then the E2T card's bootloader is bootrom. Proceed with [Manually Upgrade E2T Card Bootloader from Bootrom to U-Boot](#). After you are done using the console, [disconnect from the E2T Card Console](#).
6. If the prompt is=>, then the E2T card's bootloader is U-Boot. Proceed with [Configure U-Boot Networking Parameters of the E2T Card](#). After you are done using the console, [disconnect from the E2T Card Console](#).

Configure U-Boot Networking Parameters of the E2T Card

DHCP

To configure the E2T card to use DHCP:

1. Provision the E2T card on your DHCP server. See Configuring External DHCP Settings for the E2T Card.
2. Stop the E2T card's autoboot, and from the U-Boot's command line, set the `bootcmd` parameter in one of the following two methods:

Run the `ubootcfg` command (available only for U-Boot 1.0.3.11 or later):

```
run ubootcfg
```

Press the ENTER key until the `bootcmd` parameter is displayed. You do not need to type out the parameter name. Enter the value of the `bootcmd` parameter as `run loadet2_dhcp`.

Or

Run the `setenv` command, and enter the value of the `bootcmd` parameter. Using this method, you must type out the parameter name:

```
setenv bootcmd run loadet2_dhcp
```

3. Ensure that the VLAN ID of the E2T card is the same as the VLAN ID of the RTC card by verifying the value of the `vlan` parameter for the E2T card:

```
print vlan
```

If the two VLAN IDs are different, change the VLAN ID of the E2T card to the same value as the VLAN ID of the RTC card:

```
setenv vlan x (where x is the VLAN ID of the RTC card)
```

4. Run the following commands to save your changes and boot the E2T card:

```
saveenv  
boot
```

5. Log in to the System Administration Tool.
6. Verify the status of the card in **Slot ID 2** in the **Hardware Compute Cards** form. If the E2T card is connected and you can make an IP - TDM call, then the configuration is successful.

Static IP

To configure the E2T card with static IP configuration, you must set the following U-Boot variables for the E2T card from the U-Boot command line:

Table 6.2: U-Boot Variables for E2T Card

U-Boot Variable	Purpose
ipaddr	IPv4 address of the E2T card in dot-decimal format. For example, 10.10.10.11.
netmask	IPv4 net mask of the E2T card in dot-decimal format. For example, 255.255.255.0.
netmask_hex	IPv4 net mask of the E2T card in hexadecimal format. For example, FFFFFFF0.
gatewayip	IPv4 address of the gateway (must be same as the RTC card). For example, 10.10.10.1.
serverip	IPv4 address of the RTC card in dot-decimal format (IPv4 address of the TFTP server from which the E2T card is to be booted). For example, 10.10.10.10.
vlan	VLAN ID for the E2T card (must be same as the RTC card).
bootcmd	Boot command to boot the E2T card using static IP; for this procedure, it must be set to: <code>run loadet2t_static</code>

1. The system parameters for a static IP address can be configured using one of the following two commands:

- `ubootcfg` command (available only for U-Boot 1.0.3.11 or later)
- `setenv` command

Using the `ubootcfg` command

The `ubootcfg` command prompts you to enter values for all the variables (available only for U-Boot 1.0.3.11 or later).

Using the `ubootcfg` command, you can modify the required parameters and skip the other parameters by pressing the ENTER key. See Table 6.2 for the list of all system parameters.

Using the `setenv` command

The `setenv` command allows you to set values for only the required variables individually.

Stop the E2T card's autoboot, and from the U-Boot's command line, run the `setenv` command to set values for the required system parameters by typing out the individual parameter names (see Table 6.2):

```
setenv bootcmd run loadet2t_static
setenv ipaddr <new value>
setenv gatewayip <new value>
setenv netmask <new value>
setenv serverip <new value>
```

2. Verify the values specified in the previous step, in the E2T card's shell by using one of the following two commands:

- `ubootprint` command (available only for U-Boot 1.0.3.11 or later)
- `print` command

Using the `ubootprint` command

The `ubootprint` command displays the list of system parameters and their corresponding values (available only for U-Boot 1.0.3.11 or later).

Using the `print` command

The `print` command enables you to check the values of individual system parameters:

```
print <variable>
```

For example, `print ipaddr`

If you want to change the value of a parameter, then repeat Step 1 for that parameter.

3. Ensure that the VLAN ID of the E2T card is the same as the VLAN ID of the RTC card by verifying the value of the `vlan` parameter for the E2T card:

```
print vlan
```

If the two VLAN IDs are different, change the VLAN ID of the E2T card to the same value as the VLAN ID of the RTC card:

```
setenv vlan x (where x is the VLAN ID of the RTC card)
```

4. In the E2T card's shell, run the following commands:

```
saveenv  
boot
```

The E2T card boots and connects to the RTC card.

5. Log in to the System Administration Tool.
6. Verify the status of the card in **Slot ID 2** in the **Hardware Compute Cards** form. If the E2T card is connected, then the configuration is successful.
7. Verify that you can make an IP - TDM call; if yes, the configuration is successful.

NOTE: If you cannot make a successful IP - TDM call and the E2T card displays *connected* in the **Hardware Compute Cards** form, then verify that you have configured the E2T card's gateway IP address (`gatewayip` U-Boot variable).

Manually Upgrade E2T Card Bootloader from Bootrom to U-Boot

NOTE: The following procedure exposes the password for the root user both on the screen and in the system's flash memory. You may consider changing the password of the root user to a temporary value

(through the Server Manager) at the beginning of the procedure, and then changing it back to the preferred value after the procedure is completed. You can delete the password of the root user from the system's flash memory using the `bootChange` command (see Step 12 of procedure).

1. Use a terminal emulator application (for example, PuTTY) to access a 3300 ICP controller's RTC card's shell through SSH, and log in as the *root* user.
2. From the RTC card's shell, run the following command to ensure that the MiVoice Business application does not reset the system while you are upgrading the E2T card:

```
mcdDebug ResetOff
```

3. Start the FTP server on the RTC card:

```
e2tCardVxBootEnable
```

4. Redirect the connection to the E2T card's serial port:

```
e2tCardConsoleStart
```

5. The terminal emulator session is connected to the E2T card's serial port. Observe the output. The E2T card should be in a constant reboot cycle. At the following prompt, press the SPACE key three or more times to stop the auto-boot sequence and access the E2T card's Bootrom command prompt:

```
Press <SPACE><SPACE><SPACE> to stop auto-boot AFTER countdown starts...
```

The Bootrom prompt is displayed: `[VxWorks Boot]`

6. Change the network parameters of the E2T card to the values that allow the E2T card to be configured for either static IP or DHCP:

```
c
```

The command `c` is interactive; to change the value of a parameter (for example, **gateway inet (g)**), you must type in the new value (for example, **10.38.72.1**) before pressing the ENTER key. If you press ENTER without typing in a new value, then the current value is retained (see [Example](#) in this step). Ensure that you set the following network parameters as listed below (see [Example](#) in this step):

user (u)- root (mandatory)

ftp password (pw) - Password for the *root* user

e - IP address and network mask of the E2T card

h - IP address of the RTC card

g - IP address of the gateway server

Example:

The following example shows how to change the DHCP configuration of a brand-new E2T card into a static IP configuration (where password for the root user is **default**).

```
[VxWorks Boot]: c
```

You will observe the following interactive system response:

```
'.' = clear field; '-' = go to previous field; ^D = quit
boot device : qefcc0
processor number : 0
```

```
host name : bootHost
file name : /sysro/E2T8260
inet on ethernet (e) : 10.38.72.54:ffffff00
inet on backplane (b):
host inet (h) : 10.38.72.53
gateway inet (g) : 10.38.72.1
user (u) : ftp root
ftp password (pw) (blank = use rsh): @ default
f flags (f) : 0x40
target name (tn) :
startup script (s) :
other (o) : qefcc
[VxWorks Boot]:
```

In the above example, the values in bold (typed in after the original values) are examples of new values for the parameters: **inet on ethernet (e)**, **host inet (h)**, **gateway inet (g)** and **ftp password (pw)**. Note that the **user(u)** parameter must be set to *root*.

7. To verify that the changes you made in **step 7** are saved correctly, run the following command:

p

You will observe the following system response:

```
boot device : qefcc
unit number : 0
processor number : 0
host name : bootHost
file name : /sysro/E2T8260
inet on ethernet (e) : 10.38.72.54:ffffff00
host inet (h) : 10.38.72.53
gateway inet (g) : 10.38.72.1
user (u) : root
ftp password (pw) : default
flags (f) : 0x0
other (o) : qefcc
[VxWorks Boot]:
```

8. Boot the E2T card:

@

The E2T card will boot its pre-9.0 software release image. The following system response (containing the new network parameters from Step 6) confirms that the pre-9.0 software release image is fully loaded:

```
boot device : qefcc
unit number : 0
processor number : 0
host name : bootHost
file name : /sysro/E2T8260
```

```
inet on ethernet (e) : 10.38.72.54:ffffff00
host inet (h) : 10.38.72.53
gateway inet (g) : 10.38.72.1
user (u) : root
ftp password (pw) : default
flags (f) : 0x0
other (o) : qefcc
Attached TCP/IP interface to qefcc0.
Attaching network interface lo0... done.
Loading... 10130112
Starting at 0x10000...
Attached TCP/IP interface to qefcc unit 0
Attaching interface 100...done
Unable to add route to 10.38.72.0; errno = 0xffffffff.
Adding 27323 symbols for standalone.
Last reset cause was (0x1103) SOFTWARE_RESET
->
VxWorks
Copyright 1984-2002 Wind River Systems, Inc.
CPU: Mitel MMC-C PPC83XX F2500
Runtime Name: VxWorks
Runtime Version: 5.5.2
BSP version: 3.1/17
Created: Nov 26 2018, 17:15:07
WDB Comm Type: WDB_COMM_END
WDB: Ready.
```

9. Press the ENTER key several times to get the following prompt:

->
If the E2T card fails to boot, you will see an error number:

```
Attached TCP/IP interface to qefcc0.
Attaching network interface lo0... done.
Loading...
Error loading file: errno = 0x3d.
```

In the above example, 0x3d is the error number. In the case of an E2T card boot error, perform the required corrective actions as listed in the following table.

Table 6.3: Corrective Actions for E2T Card Boot Errors (Sheet 1 of 2)

Error No.	Corrective Action
0x880212	Using the command <code>p</code> , verify the bootline parameters of the E2T card: <code>user (u)</code> must be set to root . <code>ftp password (pw)</code> must be set to the password of the <i>root</i> user. If this is not the case, use the command <code>c</code> to modify the incorrect values.

Table 6.3: Corrective Actions for E2T Card Boot Errors (Continued) (Sheet 2 of 2)

Error No.	Corrective Action
0x880226	Using the command <code>p</code> , verify the bootline parameters of the E2T card: <code>host</code> name must be set to bootHost . <code>file</code> name must be set to /sysro/E2T8260 . If this is not the case, use the command <code>c</code> to modify the incorrect values.
0x3d0001	Log in to the RTC card of the controller through SSH as user <i>root</i> and verify that the FTP server is active: <code>systemctl status vsftpd</code> If the FTP server is active, then stop and start FTP server: <code>e2tCardVxBootDisable</code> <code>e2tCardVxBootEnable</code>
0x3d	SSH as user <i>root</i> to the RTC card of the controller and verify that the FTP server is active: <code>systemctl status vsftpd</code> If the FTP server is inactive, then start the FTP server: <code>e2tCardVxBootEnable</code>

10. At the `->` prompt, upgrade the bootloader of the E2T card from Bootrom to U-Boot:

```
Upgrade_Bootrom
```

You will observe the following system response:

```
_Upgrade_Bootrom: loading bootrom S-records - please wait...
_UUpgrade_Bootrom: comparing 983040 bytes in bootrom images...
_UUpgrade_Bootrom: bootrom images different - upgrade required
_UUpgrade_Bootrom: programming flash - do NOT power off or reset...
_UUpgrade_Bootrom: verifying 983040 bytes in bootrom image...passed
_UUpgrade_Bootrom: programming completed with OK status value = 0 = 0x0
->
```

11. After the upgrade of the bootloader completes successfully, remove the password of the root user from the system's flash memory by changing the ftp credentials (that is, **user (u)** and **ftp password (pw)**) back to the default values (**ftp** and **@** respectively):

```
bootChange
```

12. Reboot the E2T card:

```
reboot
```

The new bootloader, U-Boot, boots the E2T card with MiVoice Business Release 9.0 or later. The E2T card login prompt is displayed.

13. Log in to the System Administration tool, go to the **Hardware Compute Cards** form, and verify that the E2T card is in the **Connected** state.
14. To verify that the E2T card is fully functional, make an ONS to IP call on the system and check the incoming and outgoing voice quality.
15. After you confirm that the E2T card is functional, redirect the connection from the E2T card's shell to the RTC card's shell by pressing and releasing each of the following keys in the sequence listed below:
 - a. CTRL+A
 - b. X
 - c. ENTER
16. From the RTC card's shell, run the following command to disable access to the E2T card's serial port:

```
e2tCardConsoleStop
```
17. Stop the FTP server on the RTC card:

```
e2tCardVxBootDisable
```
18. Allow the MiVoice Business application to initiate system reboots:

```
mcdDebug ResetOn
```

Access the MIPS Console on MXe III Controllers

Connect to the MIPS Console

To connect to the MIPS console on an MXe III controller, follow the steps below:

1. Log in to the Server Manager and go to the **Security > Remote Access** page. In the **Secure shell access** drop-down list, select **Allow access only from trusted and remote management networks** and click **Save**.
2. Log in to the RTC card through SSH from a terminal emulator application (for example, PuTTY) as *root*.
3. Run the following command to connect the MIPS' serial port to this terminal:

```
mipsConsoleStart
```

NOTE: If the system response is that **Device/dev/ttyQE1** is locked, then there is already an active connection with either the E2T card or MIPS processor through this device. However, the device can be connected to only one source at a time. To terminate the existing minicom session, run the `e2tCard-ConsoleStart` command with the `-f` option.

The usage format of the `mipsConsoleStart` command is presented when you run this command with the `-h` option:

```
mipsConsoleStart -h
```


`mipsConsoleStart` connects MIPS' serial port to this terminal.

```
Usage: mipsConsoleStart [-f]
-f: force terminate pre-existing minicom session first
-h|-help|--help: displays this usage info
```

Disconnect from the MIPS Console

To disconnect from the MIPS console on an MXe III controller, follow the steps below:

1. On a connected MIPS serial port, the `mipsConsoleStop` command disconnects the MIPS serial port from the minicom session, and terminates the session. For MXe III controllers, this command also connects the E2T card's serial port to the printer port:

```
mipsConsoleStop
```

The usage for the `mipsConsoleStop` command is as follows:

`mipsConsoleStop [Options]`, where the Options are:

- `-f`: force terminate any existing minicom session(s) first
- `-h|-help|--help`: displays this usage info

Change IP Settings on 3300 ICP Controller

Change IP Settings Of MiVoice Business System

To change IP settings of a MiVoice Business System, see [Configuring the server](#).

The system's networking configuration includes the VLAN ID parameter. The VLAN ID cannot be changed from the Server Console. To change the VLAN ID of a 3300 ICP controller, see [Change VLAN ID for a 3300 ICP Controller](#). For more information about the VLAN ID, see [Determine VLAN ID on Separate Subsystems](#).

Change IP Settings of an Out-of-Service E2T Card

An out-of-service E2T card is an E2T card that has not booted, and cannot boot because its IP configuration is incorrect (for example, in your in-service MXe III/MXe III-L system, you have replaced the existing E2T card with a brand-new E2T card, or you have performed a first-time installation of a brand-new or used E2T card).

To change the IP settings of an out-of-service E2T card, see [Unable to Boot the E2T Card on an MXe III/MXe III-L Controller](#).

See [Configure U-Boot Networking Parameters of the E2T Card](#).

Change IP Settings of an In-Service E2T Card

An in-service E2T card is an E2T card in the operational state, that is, the E2T card has booted, and connected to the RTC card; the E2T card is fully functional.

Static IP to DHCP Configuration

To change the static IP address to DHCP, follow the steps below:

1. Provision the E2T card from the DHCP server (see Configuring External DHCP Settings for the E2T Card).
2. [Connect to the E2T Card Console.](#)
3. From the Linux shell, run the following command:

```
fw_setenv bootcmd run loadet_dhcp
```

4. Initiate system reboot from the Server Manager Help (Administration > Shutdown or reboot) for the change to take effect.

NOTE: The system will auto-correct the E2T card's VLAN ID if it was changed in the **System IP Properties** form prior to the reboot.

5. After the system reboot, log in to the System Administration Tool, navigate to the **Hardware Compute Cards** form, and verify that the E2T card is in the **Connected** state.
6. To verify that the E2T card is fully functional, make an ONS to IP call on the system, and check the incoming and outgoing voice quality.

DHCP to Static IP Configuration

If you want to change the DHCP to static IP configuration, follow the steps below:

1. [Connect to the E2T Card Console.](#)
2. From the Linux shell, run the `setenv` command to configure the required variables as listed in the table below:

U-Boot Variable	Purpose
ipaddr	IPv4 address of the E2T card in dot-decimal format. For example, 10.10.10.11.
netmask	IPv4 net mask of the E2T card in dot-decimal format. For example, 255.255.255.0.
netmask_hex	IPv4 net mask of the E2T card in hexadecimal format. For example, FFFFFFF0.
gatewayip	IPv4 address of the gateway (same as the RTC card). For example, 10.10.10.1.
serverip	IPv4 address of the RTC card in dot-decimal format (IPv4 address of the TFTP server from which the E2T card is to be booted). For example, 10.10.10.10.
vlan	VLAN ID for the E2T card (should be the same as the RTC card).

U-Boot Variable	Purpose
bootcmd	<p>Boot command to boot the E2T card using static IP.</p> <ol style="list-style-type: none"> Run the following command: <pre>fw_setenv bootcmd run loade2t_static</pre> Run the following command to verify the change: <pre>fw_printenv bootcmd</pre> Reboot the system from the Server Manager Help (Administration > Shut-down or reboot) for the change to take effect. After the system reboot, log in to the System Administration Tool, navigate to the Hardware Compute Cards form, and verify that the E2T card is in the Connected state. To verify that the E2T card is fully functional, make an ONS to IP call on the system, and check the incoming and outgoing voice quality.

Static IP Configuration Modification

If you want to modify the existing static IP configuration, follow the steps from the [DHCP to Static IP Configuration](#) section with the following exception: You do not have to modify the `bootcmd` variable.

Determine VLAN ID on Separate Subsystems

The system's networking configuration includes the VLAN ID parameter.

The VLAN ID of a 3300 ICP controller gets recorded in the following subsystems:

- MiVoice Business database
- U-Boot environment
- Linux kernel (passed by U-Boot)
- IP networking components
- MIPS FLASH for systems with MIPS processors

To get access to the MiVoice Business system over the network, all these records must be in sync.

The following table shows how to verify the VLAN ID value for each subsystem from the Linux command prompt:

Subsystem	Command to determine VLAN ID	Comments
U-Boot	<code>fw_printenv vlan</code>	
Linux kernel	<code>cat /proc/cmdline</code>	
MiVoice Business database	<code>mcdDebug disp_berk_db 13</code>	
IP Network database	<code>mcdDebug icp_vlan</code>	
MIPS FLASH	<code>mcdDebug mipsEnvShow</code>	This command resets both the MIPS processor and the internal L2 switch; as a result, network connectivity is lost for approximately 2 seconds.

Change VLAN ID for a 3300 ICP Controller

To access your ICP 3300 controller over the network, VLAN ID must be configured properly.

By default, the system is configured for a VLAN ID of 1.

If the system's VLAN ID is 1, the controller can be connected to an external L2 switch port with VLAN value different from 1 as untagged, or VLAN ID 1 as tagged.

If the system's VLAN ID is not 1, the external L2 switch port to which the system is connected must be configured with the same VLAN ID as the system's and as tagged.

You can modify ICP 3300 Controller's VLAN ID from **System IP Properties** form in the System Administration Tool.

To change VLAN ID of the ICP 3300 controller, you must be able to access the controller over the network.

If you can access the system over the network, to change the VLAN ID of the controller:

1. Ensure that you can [access 3300 ICP controller through the maintenance port](#) to help recover the system's network access in case something goes wrong in the following steps.
2. Log in to the System Administration Tool, and navigate to the **System IP Properties** form.
3. Change the VLAN ID to the value corresponding to the new network's VLAN.
4. Initiate system reboot for the change to take effect: in the Maintenance Commands page, run the RESET SYSTEM command. A confirmation message is displayed. Click OK to reset the system.

NOTE: For MXe III/MXe III-L systems with an E2T card in service, this procedure updates the E2T card's vlan configuration as well.

NOTE: If you are moving your controller to a new physical location with a different VLAN, instead of rebooting the system you must shut it down. Log in to the Server Manager, navigate to the **Shutdown or reboot** panel, select **Shutdown** and click **Perform**. Observe the output on the Maintenance port, and power the system down when you see the message that it is safe to do so. Move the controller to its new location. Power the controller up and wait for the MiVoice Business application to complete

its startup. If the user does not know the new VLAN ID on the new physical location, set the VLAN ID to 1, or alternatively at the new location use the `vlan_off` command (see [Disable VLAN Tagging](#)).

5. Configure the port on the external L2 switch.
6. Once the system comes up fully, verify that you can log in to the Server Manager and the System Administration Tool; if you are unable to log in, see [Recover the VLAN ID of a 3300 ICP Controller](#).

Recover the VLAN ID of a 3300 ICP Controller

To access a 3300 ICP controller over the network, the VLAN ID must be configured properly.

If you cannot access your controller over the network even after you have confirmed that your system's IP configuration is correct (using the [Server Console](#)), then it is possible that the VLAN configuration of the system is wrong.

First, check the system's VLAN configuration and confirm that all its subsystems are in sync (see [Determine VLAN ID on Separate Subsystems](#)), and have the expected VLAN ID value. If all the subsystems are configured for the same VLAN ID, verify that this VLAN configuration is in sync with the VLAN configuration of the L2 port on the external L2 switch to which the system is connected.

There are two methods to modify the system's VLAN configuration in order to recover the system's network access:

- Disable VLAN Tagging
- Reset VLAN ID to the Default Value

Each of the above methods use a different `mcdDebug` command: `vlan_off` and `vlan_reset`, respectively (both commands require a system with a running MiVoice Business software).

Disable VLAN Tagging

1. [Access 3300 ICP Controller Through the Maintenance Port](#).
2. Run the following command to disable the VLAN tagging temporarily:

```
mcdDebug vlan_off
```

3. Disable VLAN tagging on the port where your system is connected to the external L2 switch.
4. Verify that you can ping the controller from the PC on which you want to log in to the System Administration Tool.
5. Log in to the System Administration Tool, and navigate to the **System IP Properties** form.
6. In the **System IP Properties** form, change the VLAN ID to the value corresponding to the network.
7. In the **Maintenance Commands** page, run the `RESET SYSTEM` command. A confirmation message is displayed.
8. Click **OK** to reset the system.
9. If the new VLAN is a non-default VLAN, re-enable VLAN tagging on the port where your system is connected to the external L2 switch.

Reset VLAN ID to the Default Value

The default value for the VLAN ID is 1. To reset VLAN ID to the default value:

1. [Access 3300 ICP Controller Through the Maintenance Port.](#)
2. Run the following command to reset the VLAN ID to the default value (1):

```
mcdDebug vlan_reset
```

3. Reboot the system:

```
reboot
```

4. If tagging is enabled on the external L2 switch to which the system is connected, disable tagging on the port where your system is connected.
5. After the reboot, verify that you can ping the controller from the PC on which you want to log in to the System Administration Tool.

Change IP Address of Internal L2 Switch (CXi II and MXe III Controller)

To change IP address of the internal L2 switch of a CXi II or an MXe III controller:

1. Log in to the System Administration Tool (See [System Administration Tool](#)).
2. In the **System IP Properties** form, click **Change**.
3. To change the IP address of the L2 switch, in the **Layer 2 (L2) Switch IPv4 Address** field, enter the new IP address.
4. Click **Save**. A confirmation message is displayed.
5. Click **OK**.
6. To apply the changes, reset the system from the System Administration Tool. (See [System Administration Tool](#) for logging in to the System Administration Tool).
7. In the **Maintenance Commands** form, run the **RESET SYSTEM** command. A confirmation message is displayed.
8. Click **OK** to reset the system.

Check System

Check Alarm State

Alarms indicate the functional state of the system. You can check the alarm status on the front panel of the controller (see [Appendix D - Status LEDs](#)), on the attendant console, or through the system administration tool.

- **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.

To view alarms through the system administration tool:

1. Go to the **Alarms Details** form in **Maintenance and Diagnostics**.
2. Enter the **show fault <alarm category>** maintenance command to view alarm information.

Check System Health

1. Click **Maintenance Commands** in the System Administration Tool.
2. Enter the following commands:
 - **SHOW STATUS RESOURCE:** Provides diagnostic information for use in troubleshooting a system that is running slow or overloaded. You can also refer to the **Administration > System Information** page in Server Manager for information on system resource usage.
 - **SHOW 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 three backups.

Check Controller Hardware Profile

1. Click **Hardware Modules** in the System Administration Tool.
2. Click **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.
 - Verify the value of the **Core Speed** field:
 - For a 133 MHz system, the value is 132000000.
 - For a 266 MHz system, the value is 264000000.
 - For a 300 MHz system, the value is 297000000.
 - For a 450 MHz system, the value is 450000000.

Maintain 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 Help.

Secure Sockets Layer (SSL) and Security Certificate

Chrome and Edge

To install the Mitel security certificate:

1. Start a System Administration Tool session by connecting to the MiVoice Business system.
2. On the login page, click **Install the Mitel Root Certificate** and follow the instructions provided to install the certificate.

Firefox

To install the Mitel security certificate:

1. Start a System Administration Tool session by connecting to the MiVoice Business system.
2. Click **I Understand the Risks** followed by **Add Exception...**
3. Clear the **Permanently store this exception** check box, and then click **Confirm Security Exception**.
4. Once you confirm the exception, the System Administration Tool Login page will be displayed.

NOTE: For instructions on installing the certificate, click **Install the Mitel Root Certificate**.

Once you confirm the exception, the System Administration Tool Login page will be displayed.

Click **Install the Mitel Root Certificate** and follow instructions provided to install the certificate. After the certificate is installed, exit the browser, and then restart it. You can now log in to MiVoice Business and not receive the security certificate warnings.

Securing Telnet Connections

There are various ports on MiVoice Business used for telnet services (see [Table 6.5](#) for the list of those services and their default security settings). By default, all Call Control (CC) telnet and log services are open. By accessing the controller (using a communication application, such as PuTTY) as user *root*, you can:

- close all ports;
- close or open specific services by assigning the appropriate security level for the selected service;
- add a trusted IP address for log ports (type L).

The following security levels are available:

- 0 (Clear text) - security disabled, data is not encrypted
- 1 (Explicit) - client and controller can use encryption, but if the client does not respond to encryption request, clear text mode is possible

NOTES:

1. For tShell telnet clients, explicit (1) or implicit (2) are the only two security options. The tShell configuration applies to ALL telnet ports 2002 - 2007.
2. For the log ports (type L), level 0 (open) or 3 (closed) are the only available options.
3. If explicit, implicit, or port closed security is configured, nothing is sent to the client and the appropriate maintenance logs indicate the connection failures.
4. If all three of CC telnet sessions are set to port closed, the next time the system starts up, the listening sockets will not be created. An attempt to connect to a port that does not have a listening socket will fail.

To ensure the security of your system, it is recommended that you close all telnet ports that are not needed for external applications and selectively open only those that are required.

Call Control Telnet Ports

The Call Control telnet ports are either open (Clear text) or blocked (closed) across all ports of the system. The port numbers and the services are listed in the following table:

Table 6.4: Call Control Telnet Ports

Service	Port
SMDR Report	1752
Hotel/Motel Logs	1753
Line Printer 1	1754
ACD Real Time Events	15373
Property Management Systems	15374

Trusted Networks Functionality

The security configuration of the telnet ports is managed using the Server Manager's Trusted Networks functionality. The Server Manager manages the opening of all ports to the specific devices based on their IP addresses. All IP addresses except the local IP are blocked by default.

The telnet ports allow client connections from specific address or a range of IP addresses (IPV4 or IPV6) based on Server Manager Trusted Networks configuration.

Opening Specific Ports

If there are external applications and you need to keep specific ports open, complete the following step:

1. For each required service, set the appropriate security level. Enter:

```
setServiceSecurity [s smdr_logs|hotel_logs|lpr_output|acd_logs|pms] [0|1 ]
```

Example:

```
setServiceSecurity acd_logs 1
```

You will observe the following system response:

```
Service "acd_logs" security set to 1.
```

WARNING: All security setting changes take affect the next time a client connects and they remain after a reboot or an upgrade. However, the settings have to be re-entered after a full installations. For server-based systems, security settings must also be re-entered after the upgrade.

Table 6.5: MiVoice Business Telnet Services

Service	Service Name	Port	Service Type	Encryption
SMDR logs	smdr_logs	1752	Log (L)	None
PMS/Hotel Logs	hotel_logs	1753	Log (L)	None
LPR output (printer port)	lpr_output	1754	Log (L)	None
ACD real-time events	acd_logs	15373	Log (L)	None
IP PMS	pms	15374	Telnet (T)	None

Collect system Logs

View Maintenance or Software Logs

View maintenance and software logs from the System Administration Tool.

Table 6.6: System Reset Causes (Sheet 1 of 2)

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(s).
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.
0x103	Programmed reset	The system software intentionally restarted the system.
0x203	Push-button reset	The front panel reset button was pressed.

Table 6.6: System Reset Causes (Continued) (Sheet 2 of 2)

Reset Cause	Interpretation	Root Cause
0x100 SOFTWARE_RESET	Abnormal reset (applies to 3300 ICP Controllers only)	Programmed reboot causes abnormal reset of the system. NOTE: The programmed reboot on an x86 platform defaults to the reset cause 0x3.

Collect System Logs

Product Support may request logs in the event of a system failure (see [Table 6.7](#)).

Collecting System Logs and Diagnostics Data

You can download the system log and diagnostics data to your computer from Server Manager (**Administration > View log files**).

View Logs Remotely, TCP/IP Socket Numbers

You can direct logs and 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; 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 6.7](#)).
3. Enter the IP address of the controller RTC (*rtc_ip*).

Table 6.7: TCP/IP Output Streaming Settings (Sheet 1 of 2)

Log Output	Socket Number
Software Logs	1750
Maintenance Logs	1751
NOTE: The ports 1750 and 1751 can only be accessed locally.	
SMDR Logs	1752
Hotel/Motel Logs	1753
LPR1 Telnet Port	1754
ACD Real Time Event	15373
IP PMS (3300 R6.0)	15374

Table 6.7: TCP/IP Output Streaming Settings (Continued) (Sheet 2 of 2)

Log Output	Socket Number
PMS Voice Mail Integration	6830

View Login and Logout Audit Logs

You can view login and logout audit logs from the System Administration Tool. Refer to the Help for instructions.

Detect Device Moves for E911

Device move detection, in support of E911 Emergency Calling Services, is critical to maintaining the accuracy of Customer Emergency Services ID (CESID) information. With 3300 R5.2 and later, 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, CITELink telephones, and Hot Desk Users.

Automatic CESID has the following requirements and restrictions:

- All Layer 2 switches must report to CDP or STP, or both of them (use one or all 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

Monitor Device Moves

1. Log into the System Administration Tool.
2. Click **Device Connectivity - Moved**, or **Device Connectivity - All**. You can print or export the form (see [Export Configuration Data](#)).

Table 6.8: Device Connectivity Form Fields (Sheet 1 of 3)

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.

Table 6.8: Device Connectivity Form Fields (Continued) (Sheet 2 of 3)

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.
Previous LLDP L2 Chassis ID	Chassis ID of the LLDP Layer 2 switch where the IP device was connected before being moved.
Previous LLDP Port Identifier	Port number on the LLDP Layer 2 switch where the IP device was connected before being moved.
Last Known STP L2 Port MAC	<p>MAC address of the STP Layer 2 switch where the IP device was connected on first registration or registration after a move.</p> <ul style="list-style-type: none"> • “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	<p>Port number on the STP Layer 2 switch where the IP device was connected on first registration or registration after a move.</p> <ul style="list-style-type: none"> • 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.

Table 6.8: Device Connectivity Form Fields (Continued) (Sheet 3 of 3)

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. <ul style="list-style-type: none"> “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.
Last Known LLDP L2 Chassis ID	Chassis ID of the LLDP Layer 2 switch where the IP device was connected on first registration or registration after a move.
Last Known LLDP Port Identifier	Port number of the LLDP 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.

TIP: Refer to the System Administration Tool Help for Device - Move examples and explanation of field information.

Detecting Device Moves

- 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 Desk ing 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 R5.0 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 3300 R5.0 or later and the secondary is 3300 R4.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 3300 R5.0 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.

Analyze IP Phone Issues

Use the Mitel 3300 ICP IP Phone Analyzer to collect performance information from the IP devices on the network.

TIP: The PC must be connected to the network via a Layer 2 switch port on the controller.

Install the IP Phone Analyzer

Install the IP Phone Analyzer on a PC running at least Windows NT or Windows 2000.

1. In the System Administration Tool, program the IP address of the PC to Option 131 for pre-3300 R7.0 systems or to the ipa_srv tag in Option 43 for R7.0 and later systems.
2. MCD 5.0 and later: Obtain the IPAnalyserSetup_<version>.exe from MOL. MCD 4.x and earlier: Insert the MCD software CD-ROM in the PC's CD drive. Open the CD's **Tools** folder, then the **Phone Analyzer** folder.
3. Double-click **Setup.exe**. Follow the IP Phone Analyzer install prompts.

Launch the IP Phone Analyzer

1. Open **Mitel IP Phone Analyzer (Start/ Programs)**.
2. For instructions on how to interpret IP Phone information, refer to IP Phone Analyzer Help.

Enable Tool Analysis

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, issue the **LOAD IPDEVICE ALL** maintenance command to monitor all IP telephones. There will be a service outage while the telephones reset.

Disable 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 3300 R7.0 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 IPDE-VICE 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 Voice Encryption:

1. From the System Administration tool, access the System Options form.
2. The Voice Encryption Enabled field is set to “Yes” by default.
3. Click **Change**.
4. To disable voice encryption, select **No**.

Power Down the Controller

To power down AX/MXe III/MXe III-L/CX II/CXi II controllers:

1. Ensure that you can [access 3300 ICP controller through the Maintenance port](#).
2. Log in to the Server Manager.

3. Navigate to the **Shutdown or reboot** panel under **Administration**.
4. Select **Shutdown** and click **Perform**.
5. Click **Yes** on the confirmation screen.
6. Observe the output on the Maintenance port. Wait until you see the message that it is safe to power down the system. Then, set the power switch(es) to OFF.

WARNING: Keep the system powered down for at least 30 seconds before powering it back on.

Perform a System Reset

To reset the system:

1. Log in to the Server Manager.
2. Navigate to the **Shutdown or reboot** panel under **Administration**.
3. Select **Reboot** and click **Perform**.
4. Click **Yes** on the confirmation screen.

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.

TIP: Voice mail messages cannot be backed up on the AX.

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

- Installation/Maintenance PC (see [PC Requirements](#))
- IP address of the Controller
- System Administration Tool username and password

During the first minute of the backup process, 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.

NOTE: You can also back up the database from the Server Manager. The database backup file will include both the MiVoice Business system data and the Server Manager data. For more information, see **Backup Server Data** in the *Server Manager Help*.

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`
- `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).

Database Verification and Backup Failure Notification

During the backup process, the system verifies the following system databases to prevent a backup with incomplete or corrupted data: Management Layer (ML) System, ISDN, Applications, IP Networking, and Voicemail (excluding the EMEM (Embedded Mitel Express Manager) data).

NOTE: Call Control database is not verified.

If a corrupted file is found, the process continues until all databases are verified. Then, a list of all corrupted files is generated, an Audit Failure alarm is raised, and the backup process fails.

When, for any reason, a backup fails, a Backup Failure alarm is raised and an SNMP trap event is sent to all applications registered with the MCD. The most common reasons for a backup failure are:

- An Audit Failure alarm already exists.
- Database verification fails during the backup.
- There is not enough disk space.
- Failure to copy files during the backup.
- Failure to create a .tar file during the backup

The Backup Failure alarm will not be generated for failures associated with the client PC's browsers or applications. For example, if for a manual backup, the "Local hard drive" is selected as the location of the backup file and the ftp process fails, the alarm will not be generated. Similarly, if the client application fails to download the .tar file, the alarm will not be generated.

Both alarms persist after a system reboot and a successful backup cannot be completed until both alarms are cleared. To clear the alarms, [Restore a Database](#), ensuring that you are restoring an uncorrupted data. Otherwise, the alarms will not clear, and they will be regenerated during system start up.

If the Audit Failure alarm is not present and the Backup Failure alarm was generated for other reason(s), resolve the issue(s) and run the backup process again.

For more information, see "Backing up a Database" in the System Administration Tool Help.

NOTE: A Backup Failure alarm is generated only when a failure occurs within the local MiVoice Business node; it will not be generated for failures that occur on a remote node. However, you can use the Admin Group Alarm Summary form to view possible Backup Failure alarms on the remote nodes.

To back up the database:

- Click **Backup** in the **Maintenance and Diagnostics** menu. Refer to the Help for more information on how to perform database restore.

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 xxxxxx 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

If the database backup originated from a different MiVoice Business system, or from an older software release, see **Restore Database** in the *System Administration Tool Help* for more information.

Ensure that the database that you attempt to restore does not contain any corrupted files. Otherwise, an Audit Failure alarm will be generated.

Logging in

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.

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

- Installer PC (see [Connect PC to Controller](#))
- IP address of the Controller
- System Administration Tool username and password

Database Restore Procedure

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.

TIME: Restoring an AX database may take longer than 90 minutes.

NOTE: When restoring an AX database, the voice mail messages are not restored because they are not saved when doing a backup.

- Click **Restore** in the **Maintenance and Diagnostics** menu. Refer to the Help for more information on how to perform database restore.

Verify the Restore

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

CAUTION: Do not restore a database from a virtually installed MiVoice Business application (vMiVB) to a Container-based MiVoice Business application (cMiVB). The cMiVB application requires a base configuration different from that of other installations. Mitel recommends using the Initial Configuration Wizard for setting the initial configuration for all components of the MiCloud Flex solution.

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

1. Log in to System Administration Tool (using the customer's username and password), then click **System Administration Tool** and select **Maintenance Commands**.
2. Issue the **dbms stat** maintenance command to check if the DBMS_Initialized flag is ON. If it is, you'll see `DBMS info: DBMS_Initialized is ON`

3. 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.

Export Configuration Data

You can export data from most forms in the System Administration Tool into comma separated files (.csv) files. You can then use the Mitel Integrated Configuration Wizard to import the data from the .csv files into another system. If you want to view or edit the exported data, Microsoft Excel must be installed on your client station.

To export form data

1. Launch the System Administration Tool and navigate to the form.
NOTE: Not all forms support the exporting of data and not all forms support all the export options. If options are not supported for a form, they will be disabled ("grayed out") in the export dialog window.
2. If you want to export the data for a single record, click the record. To export a selection of records, click the first record that you want your selection to start with.
3. Click **Export**.
4. Choose the export range.
5. Choose **Comma Delimited (Spreadsheet)** as the file type.
6. Click **Export**.
CAUTION: Depending on the amount and type of data being exported, there could be a significant delay before the Save As dialog box is displayed. While data is being retrieved from the system database, other users cannot access or use the Desktop Tool, the Group Administration Tool, or the System Administration Tool.
7. After the File Download dialog box appears, click **Save**. Do not click Open. After the system retrieves the data, the Save As dialog box appears.
8. Navigate to a folder on your computer or the network.
9. If desired, change the filename. By default, files are given filenames in the following format:

Filename={Form Name (max 6 letters)}_{Switch Name (max 4 letters)}_{date followed by 24-hour time (YYYYMMDDHHMM)}
Example: TelDir_Mn98_28031205.csv
10. Ensure that the file extension is .csv.
11. Click **Save**.
12. Click **Open** to view the exported data.

Import Configuration Data

You can export the form data from an existing system into .csv files and then use the Mitel Integrated Configuration Wizard to import the form data into a new system.

To import configuration data using the Configuration Wizard:

1. Export the desired form data from the existing system into .csv files (see [Export Configuration Data](#)).
2. Launch the Configuration Wizard and select **Create a New Configuration**.
3. Select the type of configuration that you want to create.
4. Click Next to advance through the wizard. Enter the information requested on the screens.
5. When you reach the 3300 ICP - Advanced Configuration screen, select the **Import additional forms from csv files** check box. If the check box is cleared, all field entries are ignored.
6. To add a .csv file to the import list, click **Add**, select the .csv file, and click **Open**.

NOTE: The list order is irrelevant.

7. To remove a .csv file from the list, select the file and click **Delete**.
8. Click **Next** to view a summary.
9. Save and implement the new configuration.

CAUTION: If you import a .csv file associated with a form that is modified by the Configuration Wizard, you will overwrite your wizard selections.

Assign Static IP Addresses to IP Phones

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.

Setting Static IP Addresses on Dual Mode Sets

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 and modifying the static IP address](#).

Method C: Using hotkeys, at power up, press and hold the following key combinations:

Table 6.9: Accessing the Configuration Menu: Method C (Sheet 1 of 2)

Key Sequence	Function
* and 6 (M)	Change mode to MiNet

Table 6.9: Accessing the Configuration Menu: Method C (Continued) (Sheet 2 of 2)

Key Sequence	Function
* 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 and modifying the static IP address:

1. Access the Configuration (Debug) Menu on the IP Phone. Refer to the *3300 ICP Troubleshooting Guide* for instructions.
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 the **Phone IP address (static)**, 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**.

Setting Static IP Addresses on Non-Dual Mode 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 (for example, 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 (for example, 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:

- 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**.

At the **USE PRESENT SETTINGS** screen, select * - **DISABLE** to revert back to DHCP from static parameters.

Providing Power Over Ethernet to Devices (CXi II)

The CXi II controller's Layer 2 switch can provide 100 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 100 Watts is being consumed.

TIP: See the **Mitel IP Sets Engineering Guidelines** in the Document Center for IP Phone power requirements.

Disabling the VLAN on Remote 53xx IP Phones

In some network scenarios, VLAN tagged frames from remote 53xx IP phones are not supported over VPN connections. Disabling the VLAN on the phone will allow the IP phone to ignore any VLAN policy offered from LLDP, CDP and/or DHCP while maintaining the local VLAN policy.

Prior to MCD 5.0, to achieve the effect of disabling the VLAN on 53xx phone, the user can statically set VLAN to 1 (Native VLAN) with a priority in the Configuration/Debug menu of the 53xx phone. Once the VLAN ID and priority are statically set on the phone, the 53xx phone will no longer accept any other VLAN ID from LLDP, CDP and/or DHCP. Although this solution appears to work, the underlying network protocol behavior is incorrect due to asymmetrical tagged and untagged frames.

In MCD 5.0 SP2, Mitel has taken the original behavior into account and introduced a new, supported, way to disable the VLAN on 53xx IP phones to achieve the following behavior:

- When the VLAN is disabled on the IP phone, the IP phone will not accept or honor VLAN ID from LLDP, CDP and/or DHCP; and
- Only untagged frames are received and transmitted (see KB 12-5191-00261 for additional information).

How to disable the VLAN on the 53xx Phone

In the Configuration/Debug menu of the phone-->NETWORK PARAMETERS-->STATIC L2 QOS-->MODIFY L2QOS PARAMS, the VLAN ID parameter can be statically disabled by entering 0.

Potential Effect/Impact on Upgrade to MCD 5.0 SP2

1. Upon detection of a static VLAN ID setting of 1 on the 53xx IP phone, the VLAN setting on the 53xx phone will be defaulted to "disable" (see the table below for summary).
2. For any other VLAN ID, the firmware upgrade will maintain the same VLAN ID.

Table 6.10:Summary of VLAN Settings on Upgrade

Prior to MCD 5.0	Between MCD 5.0 and MCD 5.0 SP1	After MCD 5.0 SP2 upgrade
VLAN 1 and Priority are statically set on 53xx phone.	Not Supported. See KB 12-5191-00261	VLAN ID for the corresponding 53xx phone is defaulted to Disable.
VLAN 2 or higher (other than Native VLAN 1) and Priority are statically set on 53xx phone.	No change in behavior.. VLAN ID and Priority left unchanged	No change in behavior.. VLAN ID and Priority left unchanged.
VLAN 1 (Native VLAN ID) and Priority offered by DHCP/LLDP/CDP.	Require to remove VLAN 1 from DHCP/LLDP/CDP. See KB 12-5191-00261 for detail	Require to remove VLAN 1 from DHCP/LLDP/ CDP. See KB 12-5191-00261 for detail
VLAN 2 or higher other than native VLAN) and Priority offered by DHCP/LLDP/CDP.	No change in behavior.	No change in behavior

Troubleshooting Tips

1. In the Configuration/Debug menu of the phone, Network Parameters-->VIEW CURRENT VALUES-->VIEW CURRENT NETWRK, navigate to VLAN ID field to view.
2. In the unlikely event that you need to downgrade 53xx firmware from MCD 5.0 SP2 to the previous firmware, VLAN ID would be statically converted to 0 for the condition of VLAN Disable, causing IP phone to be stuck at DHCP discovery at 0.0.0.0 after firmware downgrade. To resolve this issue, remove VLAN 0 from the configuration/debug menu of the phone.
3. As a general rule, when statically configuring VLAN on the phone menu, please make sure both VLAN and Priority field are set.

Install and Replace Units

3300 ICP Controller Replacement

The following section describes procedures for replacement of a 3300 ICP Controller running MiVoice Business 9.0 or later with a new or used controller.

In the following procedures, the controller being replaced is referred to as the **old controller**, and the replacement controller is referred to as the **new controller** or just **controller**. It is assumed that you will move the disk from your old controller into your new controller.

If you are unable to continue using your controller with MiVoice Business 9.0 or later (for example, due to a hardware failure), then you must replace your controller. You can keep the hard disk from your old controller for use in the replacement controller.

A new controller ordered from Mitel may ship with either Bootrom or U-Boot as the bootloader; you can determine the bootloader only after you physically receive the controller component (see [Determine 3300 ICP Controller Bootloader](#)).

NOTE: MXe III-L controllers support MiVoice Business 9.1 or later releases .

NOTE: If you are moving your hard disk from the old controller to a new MXe III-L controller, then you must upgrade the MiVoice Business software version on the disk to 9.1; an update of the MiVoice Business 9.0 software is required before the upgrade is performed. Download the MXe III-L migration update from the Mitel Online website. Follow the instructions in KMS article S05142 for more information.

AX Controller Replacement

For replacement of the AX controller, see [Controller Card \(AX\)](#) and [Compact Flash Cards \(AX\)](#).

Replacing a CX II/CXi II or MXe III/MXe III-L Controller

Overview

This section describes procedures for replacing a CX II/CXi II/MXe III/MXe III-L controller with a new or used CX II/CXi II/MXe III/MXe III-L controller, respectively.

Before you Begin

Ensure that you:

- Acquire a new or used replacement CX II/CXi II/MXe III/MXe III-L controller from Mitel
- Remove the iButton from the old controller
- Remove the MMC Cards from the old controller
- Remove the E2T card, if installed
- Remove the hard disk(s) from the old controller
 - NOTE:** If you have a RAID system, note down the slot from which the hard disk was removed
- Remove the RAID from the old controller, if installed
- If your replacement controller features Bootrom:

- Download the **migrateflash.zip** archive from the *Mitel Software Download Center* --> *Navigate by categories* --> *MiVoice Business* --> *Migrate Flash Utility for 3300 ICP Controllers* on the *MiAccess* site
- Configure an external FTP server (for example, <http://filezilla-project.org>) as specified in the *Setup* section of *Upgrade 3300 ICP Controller's Bootloader Without Using a Hard Disk*

Procedure

1. Remove the controller cover from the new controller. For more information, see *Remove Controller Cover*.
2. Remove the iButton from the new controller. Install the iButton from the old controller into the new controller.
3. Install the MMC Cards from the old controller into the new controller.
4. Install the E2T Card from the old controller into the new controller, if applicable.
5. Install the RAID from the old controller into the new controller, if applicable.
6. Install the disk from the old controller into the new controller. If your controller is an MXe III/MXe III-L controller with the RAID configuration, install the disk drives ensuring that the drive is installed into the slot from which it was removed.
7. Follow all the steps in the *Procedure* section of *Configuration of RTC Card*.

Component Replacement Notes

See *Table 4.2* for controller component options.

Required Tools

To install or replace components, you require the following tools:

- anti-static strap
- #1 Phillips screwdriver
- #2 Phillips screwdriver
- 3/16 inch socket driver (hex nut)

Required Procedures

Whenever installing or replacing components, you must

1. *Power Down the Controller*.
2. Remove all cables from controller.
3. Attach an anti-static strap.
4. *Remove Controller Cover*. For the AX controller, remove the controller card (see *Controller Card (AX)*).
5. After replacing or installing the component, replace cover or controller card.
6. Reconnect cables.

7. Power the controller back up (see [Power Up the Controller](#)).

CAUTION: Use proper ESD precautions in all operations described in this chapter.

CAUTION: Use extreme care when handling cards and modules to avoid damaging components.

CAUTION: Remove and install blanking plates as necessary to provide access to slots. Ensure that no openings remain in the controller cabinet after installation. Blanking plates are required for safety, EMC protection, and thermal performance.

CAUTION: To prevent ESD damage to the equipment:

- a. Ensure that the system is grounded before you install a card.
- b. Whenever you handle cards, wear an anti-static strap (attached to the cabinet).
- c. When removing cards from the cabinet, immediately place them in an anti-static bag.

MXe III/MXe III-L

Accessing the MXe III/MXe III-L Carrier Board

[Figure 7.1](#), below, shows the MXe III controller without a SATA RAID controller installed. The MMC slots, numbering 1 to 6, start at the left side of the front of the controller and proceed in a counter-clockwise direction.

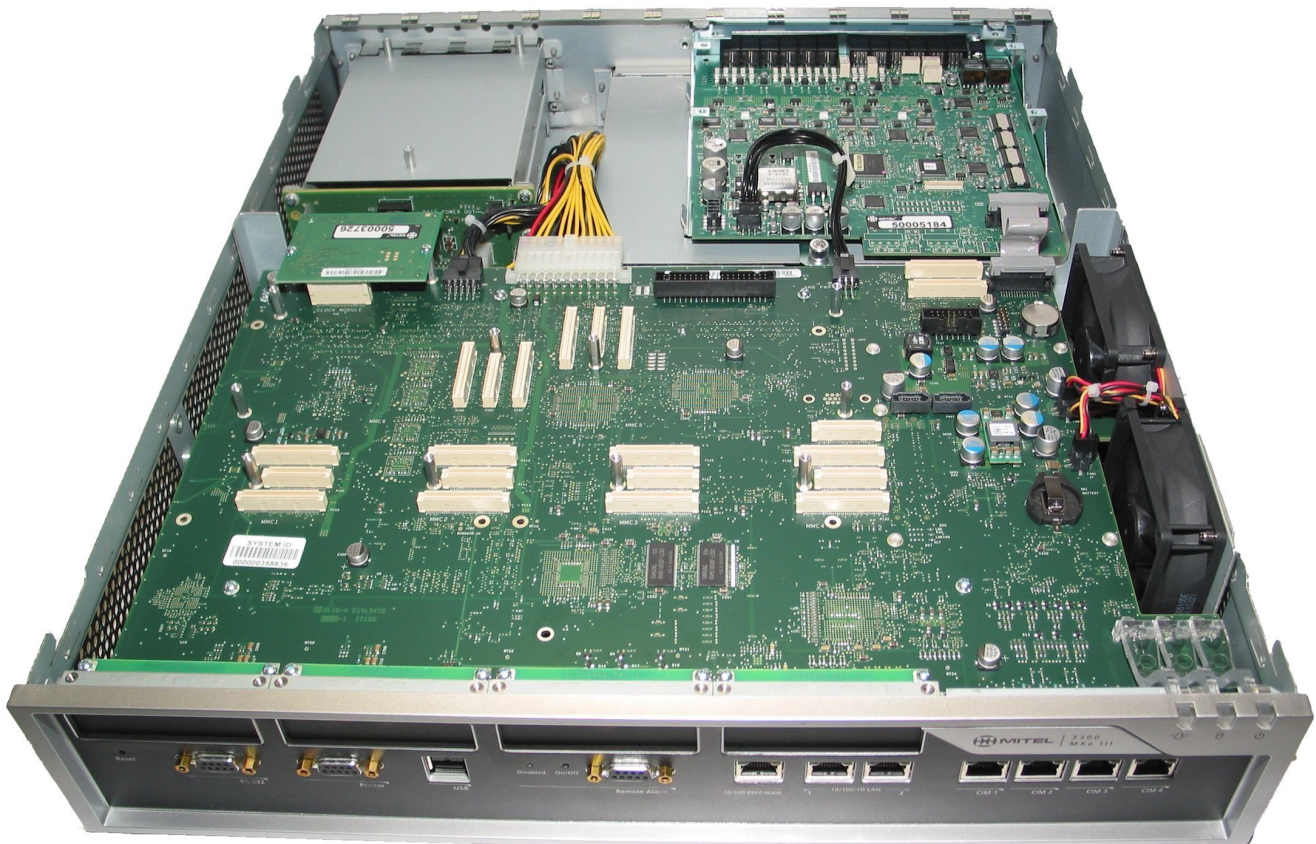


Figure 7.1: MXe III Controller with Top Cover Removed

NOTE: The MXe III-L controller looks similar to the MXe III controller, but it does not have a WAN port.

Before you can add or replace an E2T/RTC compute card, you must first access the MXe III/MXe III-L carrier board.

1. Power down the controller and remove the controller cover (see [Remove Controller Cover](#)).
2. Remove the Stratum 3 clock module and keep the screws.
3. Attach the anti-static strap to your wrist and connect the clip to the controller chassis.
4. If an Analog Main Board (AMB) is present, disconnect the power cable and ribbon cable that connects the AMB to the MXe III/MXe III-L carrier board (see the following figure).

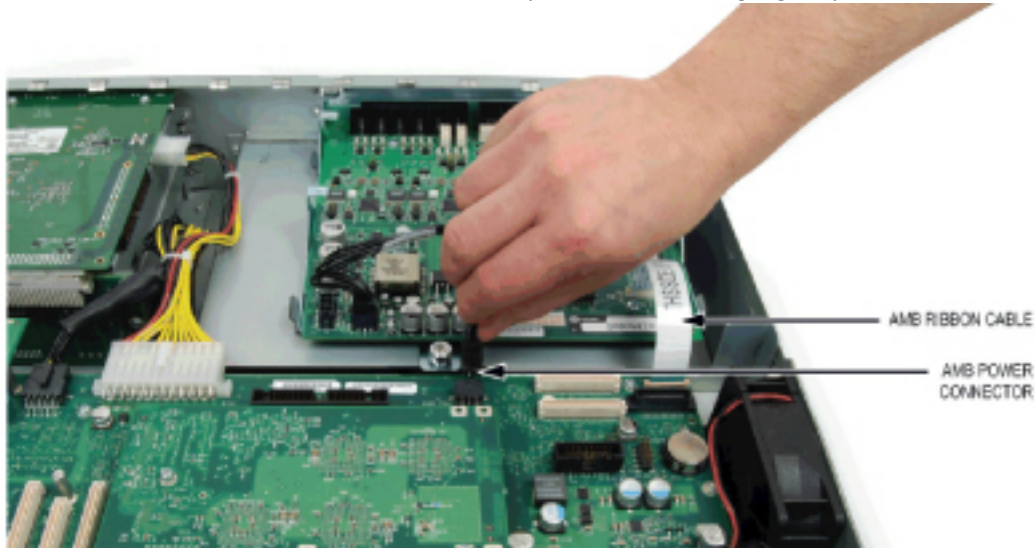


Figure 7.2: Disconnecting the AMB Power Connector

NOTE: Your MXe III/MXe III-L controller may not look exactly as pictured above.

5. Disconnect the power cables from the MXe III/MXe III-L carrier board (see the following figure).



Figure 7.3: Removing the Power Cable

NOTE: Your MXe III/MXe III-L controller may not look exactly as pictured above.

6. Remove the Stratum 3 clock module and keep the screws.
7. Unfasten the MXe III/MXe III-L carrier chassis retaining screw (see the following figure).

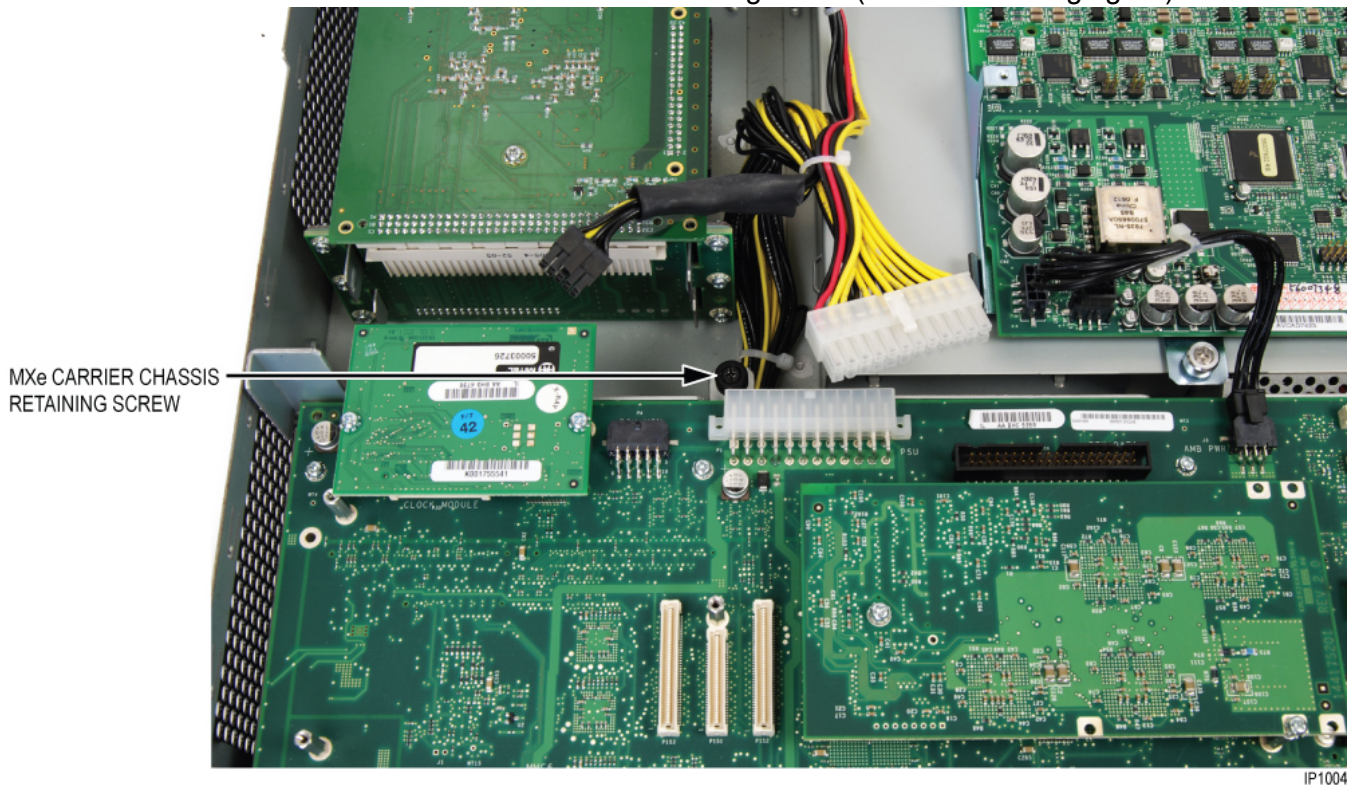
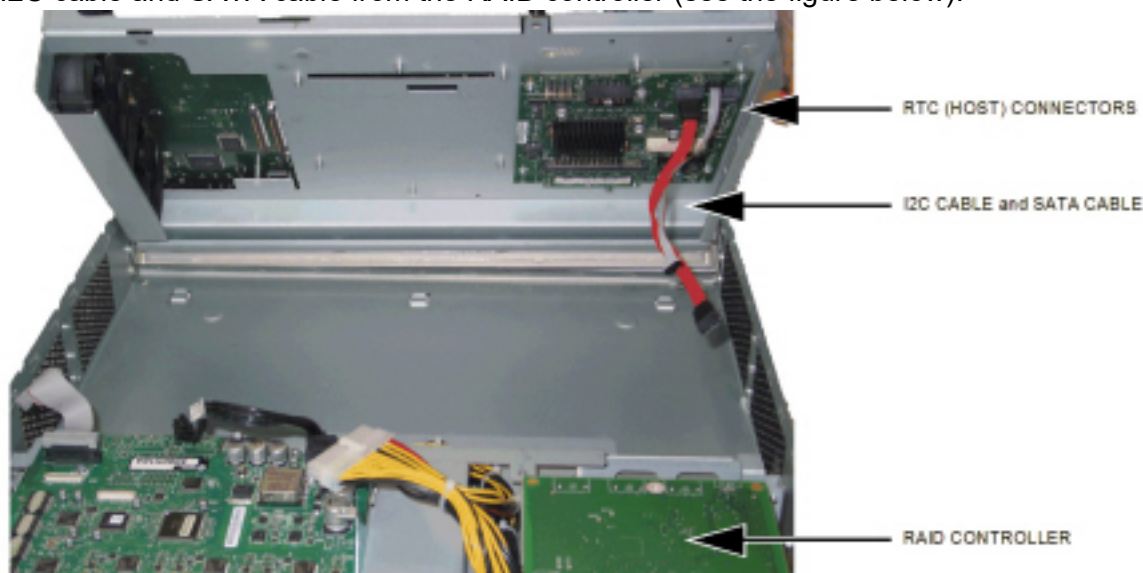


Figure 7.4: Carrier Chassis Retaining Screw

8. Facing the front of the controller, wiggle the chassis back towards yourself until the chassis is free of the controller cabinet.

9. Tilt the back of the chassis up several inches, reach underneath the Mx_e III/Mx_e III-L carrier board and disconnect SATA cable from the hard drive backplane. If a RAID controller is installed, disconnect the I2C cable and SATA cable from the RAID controller (see the figure below).



Add or Replace Controller FRUs

See [Appendix E: FRU Part Numbers](#) (p. 236) for part numbers.

Table 7.1: Field Replaceable Units (Sheet 1 of 2)

Component	Mx _e III/Mx _e III-L	CX II/ CXi II	AX
DSP Module	See DSP Module		
Echo Canceller	See Echo Canceller		
Framers	See Framers		
Dual T1/E1	See Dual T1/E1 Framer		
T1/E1 Combo	See T1/E1 Combo		
Quad BRI	See Quad BRI Framer		
Dual FIM	See Dual Fiber Interface Module (FIM)		
Quad CIM	See Quad CIM MMC		
Stratum 3 Clock Module	See Stratum 3 Clock Module		
System i-Button	See System i-Button/System ID Module		
Analog Main Board	See Mx_e III/Mx_e III-L	See CX II/CXi II	-
Analog Option Board	-	See CX II/CXi II	-

Table 7.1: Field Replaceable Units (Continued) (Sheet 2 of 2)

Component	MXe III/MXe III-L	CX II/ CXi II	AX
Processor	See RTC Processor , E2T Processor	-	-
One Drive (Non-redundant)			
Replace Hard Drive	See Replace Hard Drive	See Solid State Drive	-
Replace SSD	See Replace Hard Drive	See Solid State Drive	-
Two Drives (Redundant)			
Replace One Drive	See Replace one disk drive in an MXe III/MXe III-L	-	-
Replace Both Drives	See Replace both disk drives in an MXe III/MXe III-L	-	-
Fan Complex	-	See CX II/CXi II	-
Power Supply Unit	See Power Supply Unit	-	See Power Supply Unit
Redundant Power Supplies	See Power Supply Unit	-	See Redundant Power Supply
RAID Controller	See MXe III/MXe III-L	-	-
Controller Card	-	-	See Controller Card (AX)
Line Cards	-	-	See Line Cards
Flash Cards	-	-	See Compact Flash Cards (AX)
Memory Module	See Memory Module (AX, CX II, CXi II, MXe III)		

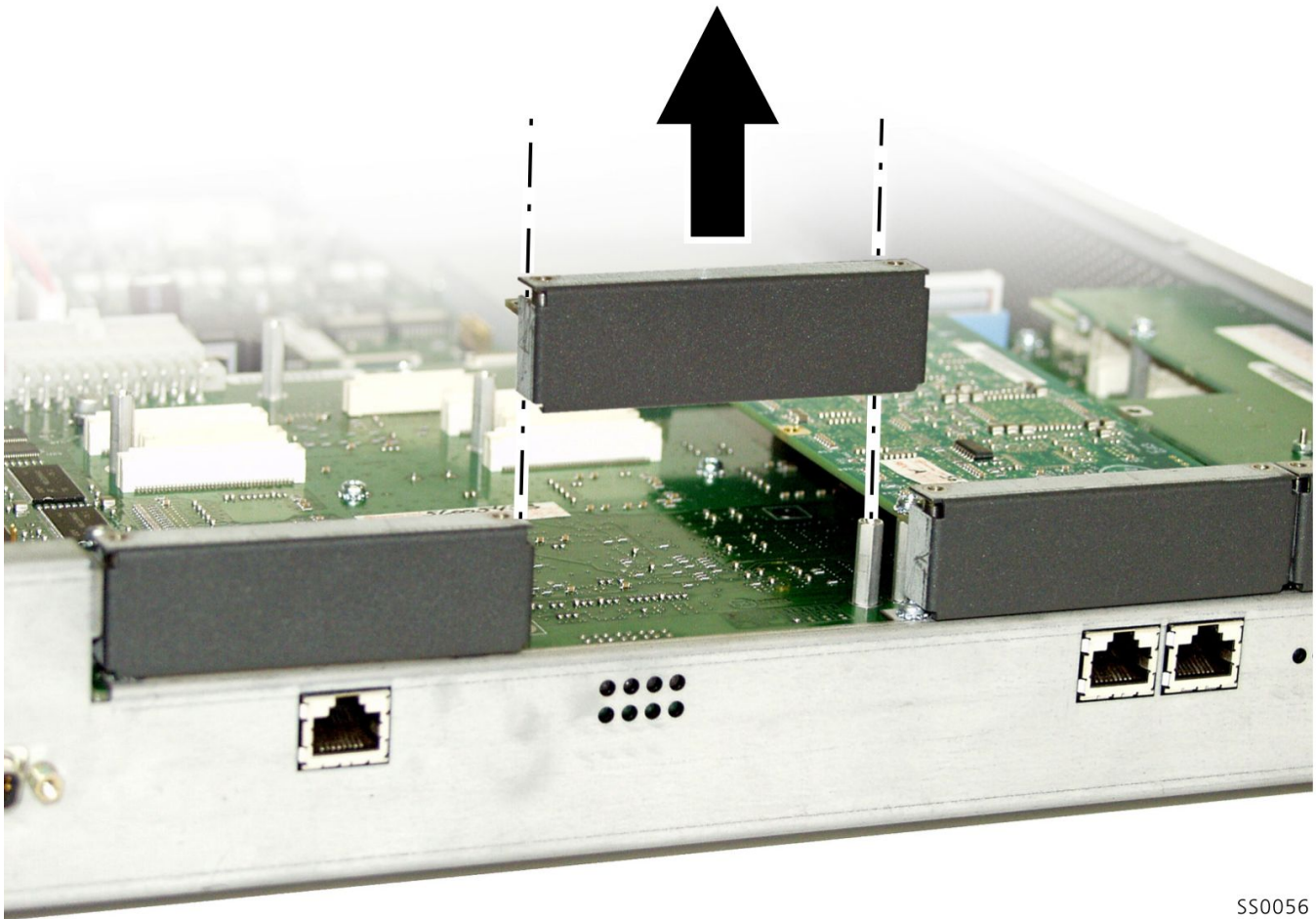
Controller Modules

Adding or replacing controller modules

To add or replace controller modules:

1. Read the notes in this section that apply to the type of module that you are adding or installing before proceeding.
2. Refer to [Determine Controller Module Configuration](#) for appropriate slot location.

3. Remove screws and lock washers and pull up on module to remove it.
4. Remove existing module and replace
 - If adding or replacing a module in an AX front panel, see additional steps below.
 - If a cover plate is attached to the module (for example, DSP module) remove it and install it on the replacement module (see the figure below).
 - Insert module connector into the module slot connector and seat it firmly into the main chassis board. Secure with screws and lock washers.



SS0056

Figure 7.5: Attaching Cover Plate to the DSP Module

AX Controller

To add or replace controller modules in AX front panel:

1. Remove the blanking plate (or the old MMC) from the controller by removing the screws that hold the standoffs to the controller (the screws are on the back side of the controller card).
2. Back off the controller faceplate screw nearest the MMC slot a couple of turns (because the screw interferes with the removal/insertion of T1/E1, Quad BRI, or Dual FIM modules).
3. Slide the blanking plate out of the opening from the back of the controller faceplate.

4. Remove the two standoffs (closest to the face plate) from the blanking plate (or old MMC). Retain the standoffs and screws.
5. Fasten the standoffs to the front of the new MMC.
6. Carefully slide the MMC face plate under the lip of the controller face plate. See [Figure 7.6](#). Do not push the MMC past the controller face plate as shown in [Figure 7.7](#).
7. Re-install and/or retighten screws.
8. Continue with procedure as described in the specific FRU instructions

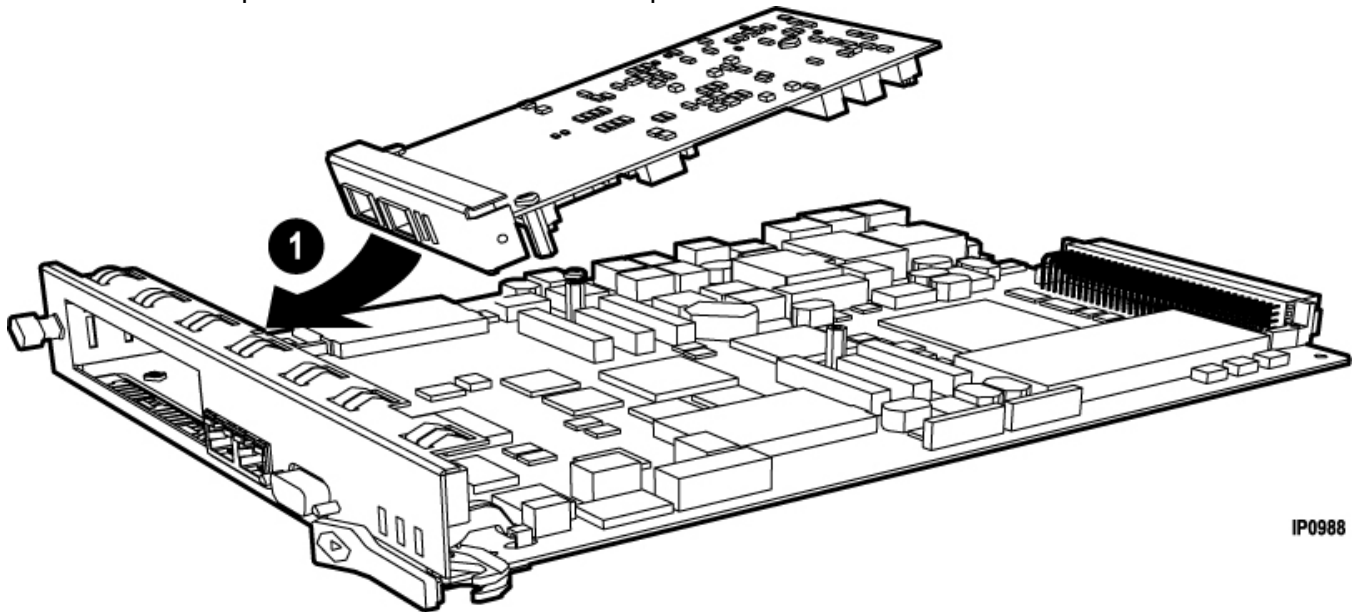


Figure 7.6: Position module at an angle (AX)

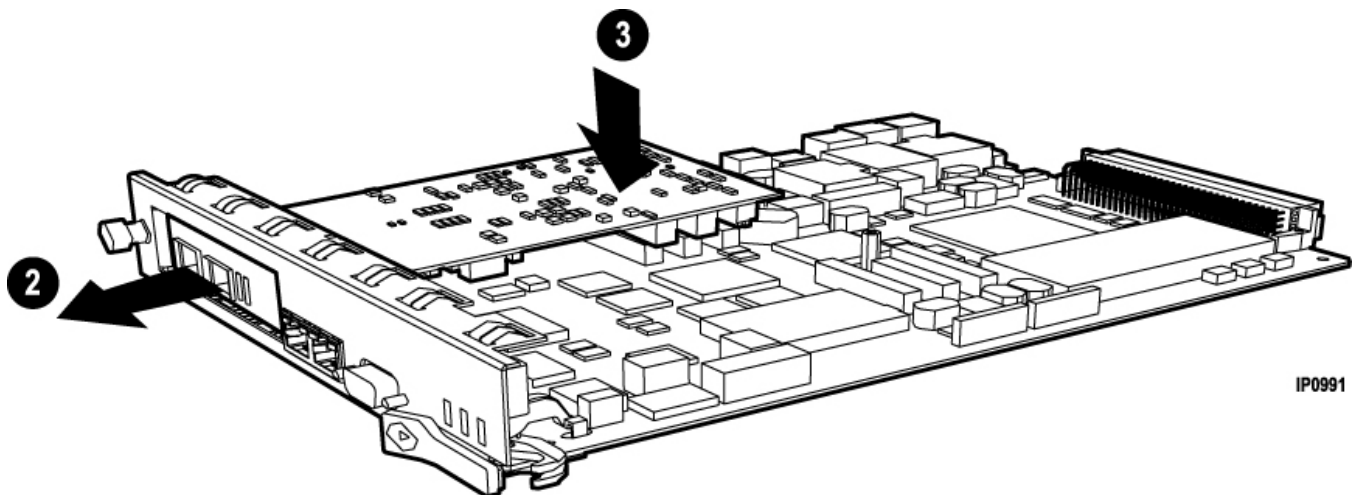


Figure 7.7: Slide in and seat module

Controller Module Installation Notes

DSP Module

- Refer to [Increasing DSP Resources](#).
- Make sure that you have sufficient compression licenses before installing DSP modules for compression.

Dual Fiber Interface Module (FIM)

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

Echo Canceller

- The CX, CXi, CX II, CXi II, Mx III/Mx III-L, Mx III Server, and AX contain echo cancellers on the main board that are sufficient to handle normal traffic conditions.

Framers

Embedded T1/E1 (for PRI, 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, T1/E1 Combo, or Quad BRI). (See [Appendix E: FRU Part Numbers](#) for the part number of the Framer Modules).
- Upgrading to embedded PRI, T1/D4, MSDN/DPNSS, or BRI requires a minimum 300 MHz controller. To determine the speed of your processor, see [Check Controller Hardware Profile](#).
- 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), HKIDAP, and QSIG protocols.

T1/E1 Combo

- The T1/E1 combo module, available only for the CX/CXi and CX II/CXi II controllers at 3300 R6.0, combines trunking (T1D4 and PRI ISDN/QSIG) and DSP functionality in a single card. The R6.0 version of the combo contained a single T1/E1 framer. The module also includes 32-channel Echo Cancellation.
- Supported on the Mx III/Mx III-L controller.
- 3300 R7.0 included a resilient connection for the combo. 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 Links form. Refer to the Resilience Guidelines in the [Document Center](#) for instructions on how to configure T1/E1 resiliency.
- Resilient operation requires that both the primary and secondary controllers are running R7.0 or later 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 [Quad BRI Framer](#) (p. 176)).
- The Quad BRI Framer is not supported in North America.
- When you remove the Quad BRI Framer module from its packaging. DO NOT move LT/NT jumpers.
- 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 8.1](#) for connector pinouts.
- 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.

Quad CIM MMC

- Support for the Quad CIM requires that the 3300 ICP is running software 3300 R7.1 or later.
- The Quad CIM MMC cannot be installed in an AX or Mx III Server.
- The CX, CXi, CX II, and CXi II can accept one Quad CIM MMC.
- All other controllers can accept two Quad CIM MMCs.
- When the Quad CIM MMC is used in a CX, CXi, CX II, or CXi II, only the first three ports are operational.

Stratum 3 Clock Module

To replace the clock module in the CX/CXi, or Mx III/Mx III-L:

NOTE: The other controllers use the Stratum 3 Clock, but in each case, the clock is embedded and is not field replaceable. The Mx III Server does not use a Stratum 3 Clock.

1. Remove the screws from the clock module.
2. Remove the clock module.
3. Seat the new clock module onto the main board.
4. Replace the screws that you removed from the clock module.

System i-Button/System ID Module

To replace the System i-Button (Mx III/Mx III-L, CX/CXi, CX II/CXi II, AX):

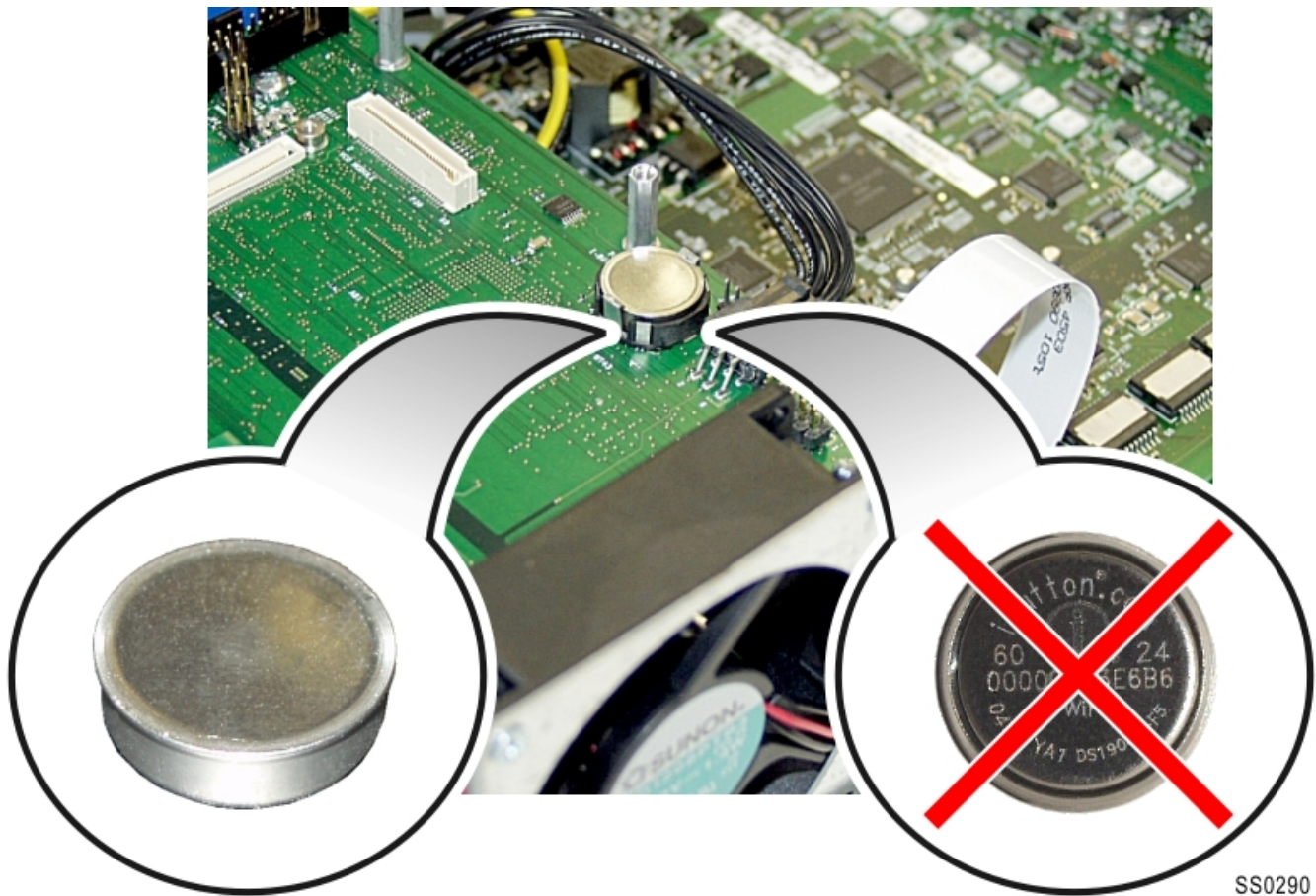
1. Remove the old system i-Button from the main board. Lift slightly the metal clips that hold the i-Button in place.
2. Insert the system i-Button in the twin tab connector located on the main board (see [Figure 7.8](#)) or on the controller card, for the AX, CX II and CXi II directly behind the external MMC slot position (see [Figure 4.2](#), [Figure 4.3](#), and [Figure 4.4](#)).

NOTE: If you observe system reboot issues after you replace the System i-Button, then connect a serial cable from the PC to the controller’s maintenance port. If you observe the following prompt on the serial console: “Welcome to emergGive root password for maintenance (or press Control-D to continue)”, then refer to the troubleshooting steps in **Chapter 3 “Hardware” > “Controllers”** of the *MiVoice Business 9.0 Troubleshooting Guide*.

To replace the System ID Module:

1. Remove the old System ID module from the main board. The module is located between slots 1 and 8 on **LX** controller.
2. Remove the cover from the new System ID module's connector.
3. Install the new System ID module and secure with the screw provided.

NOTE: If you replace the System I-button, you must program the options (see [Enable Licenses and Options](#)) and then restore the database (see [Restore a Database](#)).



SS0290

Figure 7.8: Installing the System i-Button

Analog Main Board

MXe III/MXe III-L

To replace the analog main board (AMB) in an MXe III/MXe III-L:

1. Remove the narrow flex cable on the AMB (J4) by flipping up the clip on the connectors at each end of the cable (prior to 3300 R7.1 version) or remove the ribbon cable on the AMB (J8) (see [Figure 7.9](#)).
TIP: A replacement AMB ships with a connector-less flex cable that you will discard for the MXe III/MXe III-L controller.

2. Loosen the captive screw on the AMB.
3. Remove the AMB.
4. If you are replacing the AMB with an AMBv3, the replacement kit will include a new label that identifies the protected ports.
 - If your MxIII/MxIII-L still has the old AMB label, apply the new label over the existing one.
 - If your MxIII/MxIII-L has the new AMB label, discard the label.
5. Place the new AMB on the power supply carrier and slide the port interfaces through the slots at the rear of the controller.
6. Secure the AMB to the carrier with the captive screw provided.
7. **AMB 2:** Attach the ribbon cable to the controller and the AMB.
8. **AMB 3:** Attach the connector-less flex 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.

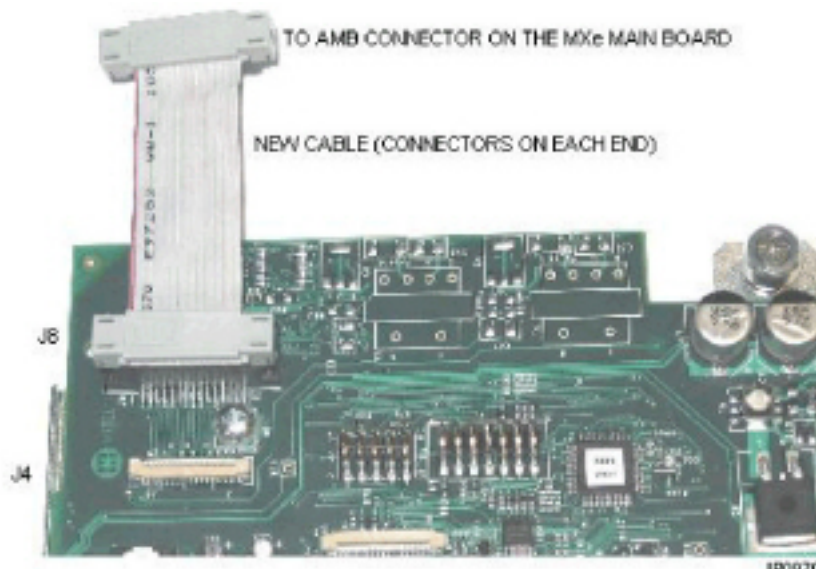


Figure 7.9: AMB with new cable for MxIII/MxIII-L Controller

CX II/CXi II

To replace the AMB in a CX II/CXi II:

1. Power down the controller and remove the controller cover; see [Power Down the Controller](#) for the procedure.
2. Remove the Analog Option Board, if one has been installed. Remove by reversing the steps on [Analog Option Board](#) of this document.
3. Remove the AMB as follows referring to [Figure 7.10](#):
 - Disconnect the power supply cable on the AMB.
 - Disconnect the ribbon cable on the AMB (not from the main board).
 - Unfasten the four screws holding the AMB to the controller chassis.

- Remove the AMB by pushing it toward the front on the controller, and then tipping it upwards.
 - Insert the new AMB and secure it to the chassis using the supplied screws.
4. Reconnect ribbon cable.
 5. Reconnect the power cable to the new AMB.
 6. Replace the Analog Option Board (if previously removed).
 7. Configure the board. See [Configure Embedded Analog Boards](#).

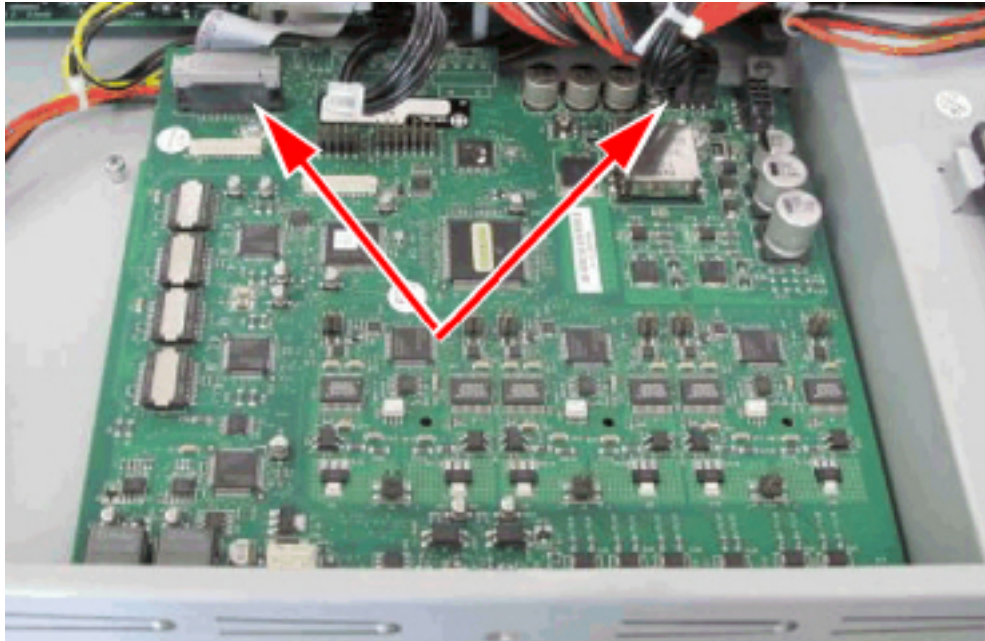


Figure 7.10: AMB - Disconnect Cables

Analog Option Board

CX II/CXi II

Add an AOB to a CX II or CXi II controller to increase LS CLASS circuits from 6 to 12 and ONS CLASS circuits from 4 to 8 (see [Analog Board \(CX II/CXi II and MxIII/MxIII-L Controllers\)](#) (p. 176)).

NOTE: [Figure 7.14](#) shows an older version (57010212A) of the AOB mounting bracket. To support the flex ribbon cable shown, you must replace this older version with the new RD MTKW CX II AOB MNTG BRACKET 2 (57010212B). The installation procedure is otherwise as documented.

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

1. Power down the controller and remove the controller cover; see [Remove Controller Cover](#) and [Power Down the Controller](#).
2. If adding the AOB, remove the blanking panel from the back of the controller.



Figure 7.11: Removing Blanking Panel

3. Remove the four screws that secure the Analog Main Board (AMB) to the bottom of the chassis.
4. Replace the screws removed above with the standoffs included with the AOB.
5. Attach the flex and power cables supplied with the AOB to the AMB.
 - To attach the flex cable, lift up on the tabs at the end of the connector to loosen it, insert the cable label side up, and then press down on the tabs to tighten the connector.

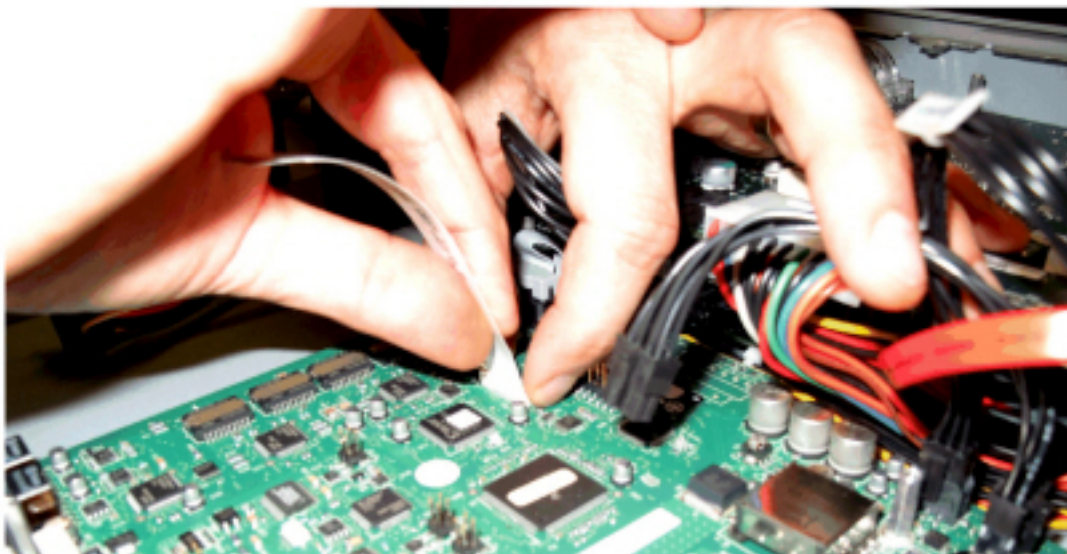


Figure 7.12: Attach Flex cable to AMB

6. Connect the power cable to the connector on the AMB closest to the edge of the board.

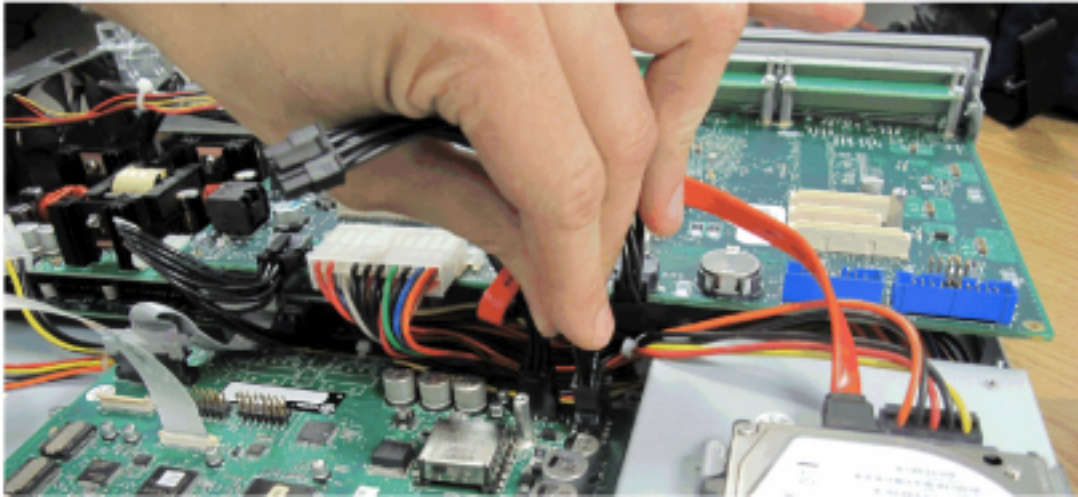


Figure 7.13: Attach Power Cable to AMB

7. Attach the mounting plate to the standoffs and the back panel of the controller using the supplied screws.



Figure 7.14: AOB Mounting Plate in Position

8. Lower the AOB on to the mounting plate and secure it with the four smaller screws supplied with the AOB.
9. Connect the other ends of the flex cable and power cable where indicated in the following figure . To attach the flex cable, lift up on the tabs at the end of the connector to loosen it, insert the cable label side up, and then press down on the tabs to tighten the connector.

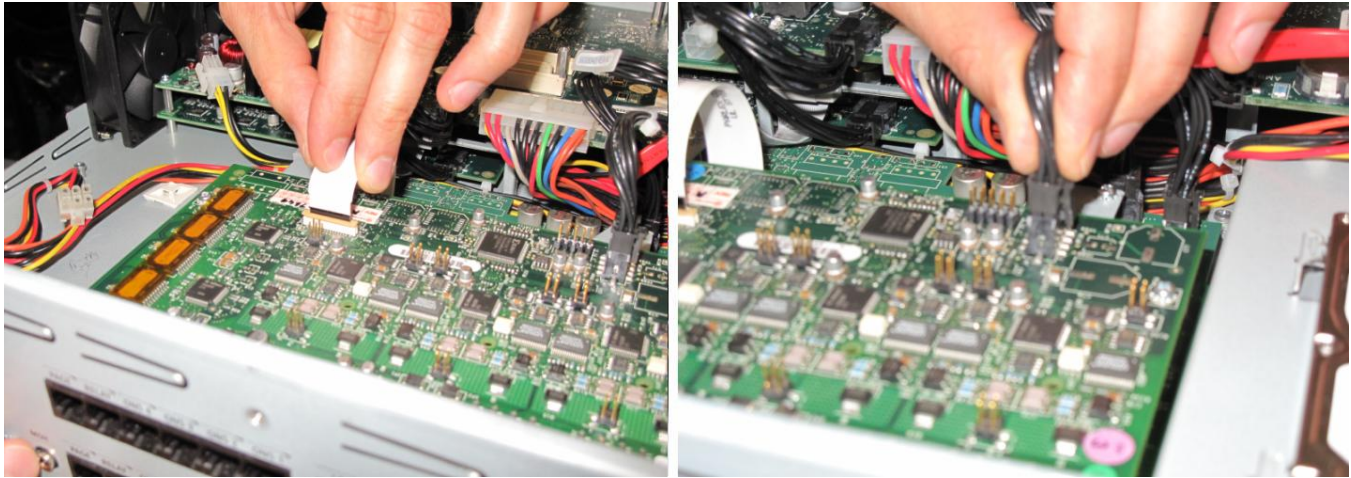


Figure 7.15: Attach Flex Cable and Power Cable to AOB

10. Replace the top cover and power up the controller.
11. In the System Administration Tool, go the **Analog Services Units** form.
12. Select Unit 4 and click **Modify**.
13. Select **3300 Expanded Analog** and click **Save**.
14. Configure the board. See [Configure Embedded Analog Boards](#).

Configure Embedded Analog Boards

To configure controllers with embedded analog boards:

1. Complete telephony cabling for embedded analog (see [Table 8.4](#)).
2. Complete the Music on Hold and Paging cabling if required (see [Table 8.12](#) and [Table 8.4](#)).
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 analog 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 Units form.

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

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 (refer to the System Administration Tool Help).

RTC Processor Card (MXe III/MXe III-L Controller)

Overview

This section describes how to install/replace and configure an MXe III/MXe III-L processor card in the RTC card slot (that is, RTC card) of your MXe III/MXe III-L controller running MiVoice Business Release 9.1.

The first part describes the physical installation/replacement of a new RTC card. The second part describes the configuration of the new RTC card for MiVoice Business Release 9.1.

For the RTC Card replacement, you may choose to install either a brand-new or a used RTC card.

A new RTC Card component ordered from Mitel may ship with either Bootrom or U-Boot as the boot-loader; you can determine the bootloader only after you physically receive the RTC Card component (see [Determine 3300 ICP Controller Bootloader](#) to determine the bootloader).

Before you begin

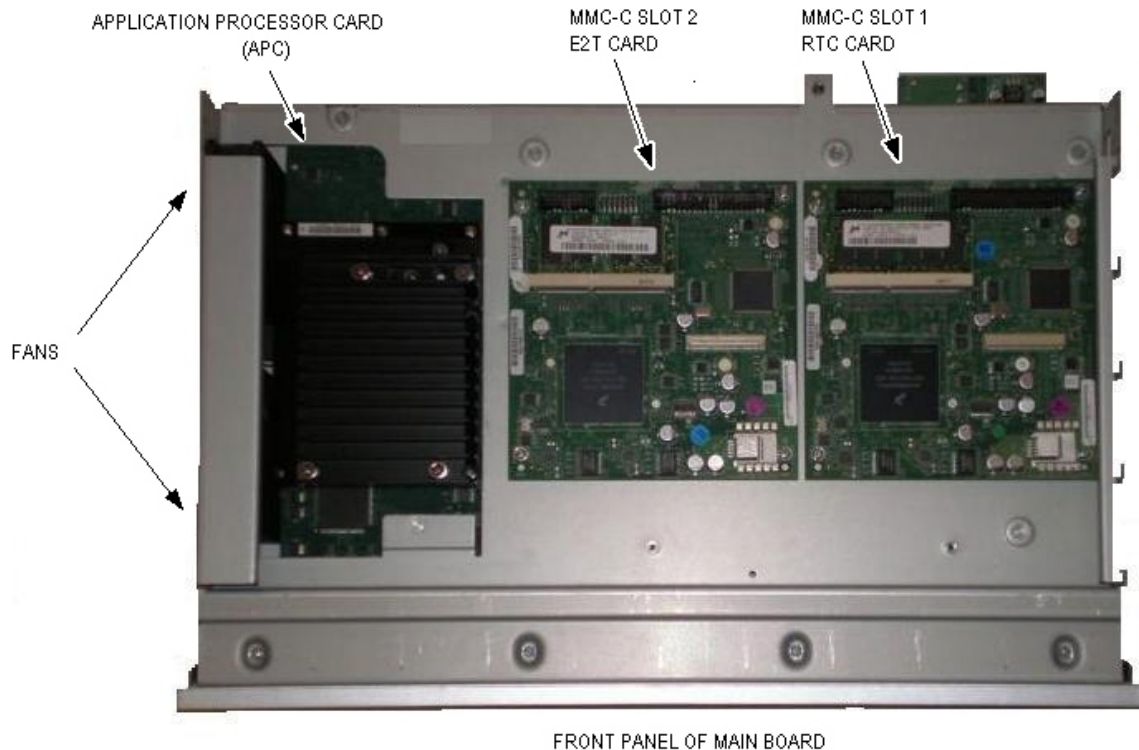
Ensure that:

- You acquire an RTC card (brand-new or used)
- The RTC card has SATA connectors and 1GB of RAM
- You know the active partition number of your current 9.1 disk (see [Determine Last Known Active Partition using U-Boot](#))
- If your replacement RTC card features Bootrom, you do the following:
 - Download the **migrateflash.zip** archive from *Mitel Software Download Center* --> *Navigate by categories* --> *MiVoice Business* --> *Migrate Flash Utility for 3300 ICP Controllers* on the MiAccess site.
 - Configure an external FTP server (for example, <http://filezilla-project.org>) as specified in the [Setup](#) section of [Upgrade 3300 ICP Controller's Bootloader Without Using a Hard Disk](#).

Procedures

Physical Installation of RTC Card in MXe III/MXe III-L Controller

1. Access the main board; see [Accessing the MXe III/MXe III-L Carrier Board](#).
2. Set the main board on a flat surface with the underside facing up. Observe the physical position of the RTC card in the figure below:



3. Remove the four screws and lift the RTC card from the main board.
4. Seat the new card onto the main board and secure with four screws.
5. Perform the steps listed in [Accessing the MXe III/MXe III-L Carrier Board](#) in the reverse order to reassemble the controller.

Configuration of the RTC Card

Overview

To boot MiVoice Business Release 9.1 from the correct disk partition of your MXe III/MXe III-L controller, the RTC card must feature U-Boot as the bootloader, and the U-Boot's variable `ata_active_part` must be configured with the correct partition number. Once you boot the system, you must log in as the *admin* user to configure the RTC card's networking parameters through the Server Console program.

Before you Begin

Ensure that:

- The RTC card features U-Boot as the bootloader (see [Determine 3300 ICP Controller Bootloader](#)). If the RTC card features Bootrom as the bootloader, you must [upgrade the RTC card's bootloader to U-Boot](#).
- You know the active partition number of your disk (see [Determine Last Known Active Partition using U-Boot](#)).

Procedure

1. [Access 3300 ICP Controller Through the Maintenance Port](#).
2. Power on the controller.
3. Stop the auto-boot sequence from the serial port (Maintenance port), by pressing the SPACE key three or more times consecutively within seven seconds at the following message:

```
Press <SPACE> key 3 times within 7 seconds to stop autoboot
```

The system displays the prompt => when the auto-boot sequence stops.

4. Run the following command to set the active partition number as determined earlier:

```
setenv ata_active_part n
```

where **n** is the active partition number

5. Run the following commands to save the change and reboot the controller:

```
env save  
boot
```

6. Wait for the system to boot fully, and the MiVoice Business application to complete the startup (usually takes less than 15 minutes from the moment the system starts booting). From the Maintenance port, log in as the *admin* user to access the Server Console program (see [Accessing Server Console](#)).

NOTE: If the system displays: *ADMIN LOGIN IS BLOCKED UNTIL MIVoice BUSINESS IS STARTED* error message on the console, the MiVoice Business application has still not completed the startup. It usually takes less than 15 minutes for the MiVB to fully boot from the moment the system starts booting. If the application does not complete its startup even after 20 minutes (for example, 3300 ICP controller and/or RTC Card replacement scenarios), search for the *ADMIN LOGIN IS BLOCKED* error in **Ch 4, Software > System Software** of the *MiVoice Business Troubleshooting Guide, Release 9.1*.

7. On the Server Console screen, navigate to and select **Configure this Server**.
8. Enter network configuration settings such as the Primary Domain Name and Local Subnet Mask (for more information, see **Server Console --> Configure the Server** in the *System Administration Tool Help*). After making the necessary changes, the Server Console prompts you to reboot the system. Reboot the system to activate the changes.
9. Allow the system to boot fully.
10. After the system boots, verify that you can access the system over the network.

NOTE: If your system does not respond to pings, see [Recover the VLAN ID of a 3300 ICP Controller](#).

11. Log in to the System Administration Tool and go to the **Alarm Details** form. If you observe Bootrom and/or FPGA alarm, navigate to the **Maintenance Commands** page, and run the UPGRADE-BOOTROM ALL maintenance command. Then, initiate a system reboot for the change to take effect.

NOTE: If you had an MXe III/MXe III-L controller with the FPGA alarm, you must power down and power up the system, instead of a reboot; this is required because the FPGA gets programmed only after power on reset (see [Power Down the Controller](#)).

12. Allow the system to fully boot.
13. Log in to the Server Manager and System Administration Tool to verify that the system is fully functional.

E2T Processor Card (MXe III/MXe III-L Controller)

Overview

This section describes how to install/replace and configure an MXe III/MXe III-L processor card in the E2T card slot (that is, E2T card) of your MXe III/MXe III-L controller running MiVoice Business Release 9.1.

The E2T card is the same card as the as RTC card; the only difference is that the E2T card is used as an expansion card.

NOTE: Refer to the *MiVoice Business Engineering Guidelines* to determine when a second processor is necessary in the MXe III/MXe III-L.

For the replacement of an E2T card, you may choose to install either a brand-new or a used E2T card.

Before you Begin

Ensure that:

- You acquire an E2T card (brand-new or used)
- The E2T card has SATA connectors and 1GB of RAM
- You know the MAC address of the replacement card if you want to use DHCP for its networking configuration (See [Configuring External DHCP Settings for the E2T Card](#))

Procedure

1. To physically replace the E2T card, follow the instructions described in the section, [Physical Installation of RTC Card in MXe III/MXe III-L Controller](#), but install the card into the E2T card's slot.
2. After you fully reassemble the controller, power it on and wait for it to fully boot.
3. Log in to the System Administration Tool, and verify the status of the card in the **Hardware Compute Cards** form. Confirm that the system has detected the presence of the E2T card. If the status of the E2T card is **Not Responding**, see [Unable to Boot the E2T Card on an MXe III/MXe III-L Controller](#).
4. Once the E2T card is properly configured, verify the status of the card in the **Hardware Compute Cards** form; the E2T card details should be displayed here. You should be able to make IP - TDM calls.

Disk Drives (CX II/CXi II/MXe III/MXe III-L)

Disk Drive Replacement Overview

This section describes how to replace the HDD or SSD in your CX II, CXi II or MXe III/MXe III-L controller running MiVoice Business 9.0 or later software.

NOTE: The procedures in this section apply only to controllers with U-Boot as the bootloader.

You can replace the faulty drive with one of the following replacement drives listed in the following table.

Table 7.2: Disk Drive Replacement

Software version on the failed drive	Status of the replacement drive	Software version on the replacement drive	Procedure
MiVoice Business 9.0 or later	New	MiVoice Business 7.2 SP2	<ol style="list-style-type: none"> 1. Disk Drive Replacement 2. New Replacement Drive with MiVB 7.2 SP2 Software or Install System Software Manually on a 3300 ICP Controller
MiVoice Business 9.0 or later	New	MiVoice Business 9.1	<ol style="list-style-type: none"> 1. See Hard Disk Replacement.
MiVoice Business 9.0 or later	Used	Pre-9.0	<ol style="list-style-type: none"> 1. Disk Drive Replacement 2. Used Replacement Drive with Pre-9.0 Software or Install System Software Manually on a 3300 ICP Controller
MiVoice Business 9.0 or later	Used	MiVoice Business 9.0 or later	<ol style="list-style-type: none"> 1. Disk Drive Replacement 2. Used Replacement Drive with MiVB 9.0 or Later Software

CAUTION: You cannot move a drive from one controller type to a different controller type (eg. from a CXi II controller to an MXe III/MXe III-L controller). You can either move compatible HDD/SSD parts between the same controller type only or acquire the appropriate HDD/SSD part from Mitel.

CAUTION: In an MXe III/MXe III-L controller with RAID configuration, the two SATA HDD must have the same accessible capacity. For example, a 60 GB drive from one manufacturer may have a slightly different accessible capacity than that of a 60 GB drive from another manufacturer. To ensure that the drives match, check them carefully before installation.

TIP: You are advised to perform the disk drive replacement outside of business hours.

Disk Drive Replacement

This section describes the prerequisites and procedures to replace a disk drive on your 3300 ICP controller.

Before you Begin

- One of the following replacement drives:
 - A brand-new drive from Mitel: CXi II SSD part number 50006266 (16 GB), with MiVoice Business Release 7.2 SP2 or 9.1 pre-installed.
 - Or,
A brand-new drive from Mitel: MXe III SSD part number 50006268 (60 GB) or MXe III HDD part number 50006513 (250 GB), with MiVoice Business Release 7.2 SP2 or 9.1 pre-installed.
 - A used drive, removed from another controller with a **pre-9.0 software (MCD 6.0 SP3 or higher)**. Before removing the drive, determine its active partition number (1 or 4) by [accessing the controller through the Maintenance port](#) as user *root*, and then running the following command:

```
version
```

You will observe the following system response:

```
VxWorks (for Mitel MMC-C PPC83XX F2500) version5.5.2.
Kernel: WIND version 2.6.
Made on Nov 26 2018, 17:09:58.
Boot line: ata=0(0,0)mn24:/partition1/RTC8260
e=10.211.26.78:ffffff00 b=0 h=10.211.26.201
g=10.211.26.1 u=14-0-3-51 pw=mcdve tn=MN78 s=c
o=qefcc
value = 145 = 0x91
```

In the above system response, the text *partition1* indicates that partition 1 is the active partition.

- A used drive, removed from another controller, with **MiVoice Business 9.0 or later** software. Before removing the drive, you must determine its active partition number (see [Determine Last Known Active Partition using U-Boot](#)).
- Database backup file from the Server Manager.

CX II/CXi II (Single Hard Disk or Solid State Drive)

Replace a Single HDD or SSD in a CX II/CXi II Controller

NOTE: Ensure that the CX II/CXi II controller is grounded during the procedure. See [Safety Instructions](#).

1. Power down the controller.
2. Disconnect the external cables from the controller.
3. Unmount the controller.
4. Remove the controller cover.
5. Unplug the data cable and power cable from the old SSD; see **1** in following figure.

6. Remove the two screws securing the drive to the mounting bracket, and then lift the drive out; see 2 in the following figure.

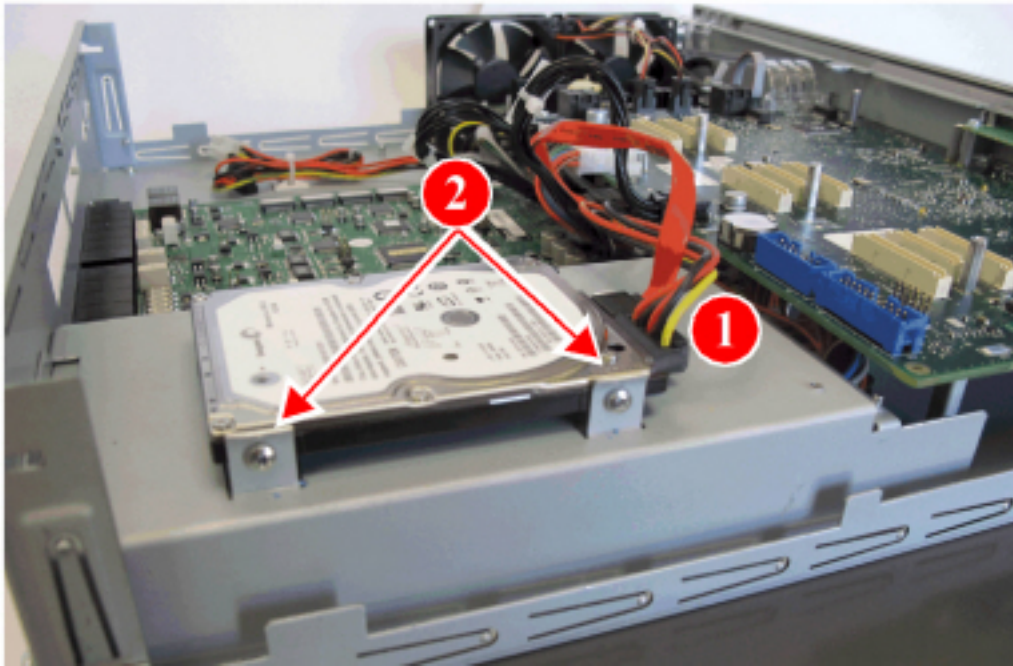


Figure 7.16: CX II/CXi II Hard Disk Drive/Solid State Drive Replacement

7. Replace the old disk drive with the replacement disk drive and secure it to the mounting bracket.
8. Reconnect the data cable and power cable to the SSD. The cables are keyed for proper connection.
9. Replace the controller cover.
10. Remount the controller.
11. Reconnect the power cable and external cables.
12. Continue with [Upgrade Software After Disk Drive Replacement](#).

MXe III/MXe III-L (Single Hard Disk or Solid State Drive)

Replace a Single HDD or SSD in an MXe III/MXe III-L Controller

NOTE: Ensure that the MXe III/MXe III-L controller is grounded during the procedure. See [Safety Instructions](#).

1. Power down the controller.
2. Release the retaining screw securing the bottom drive carrier (HD1) to the controller, and remove the carrier.
3. Place the carrier and drive on a level and stable surface.
4. Remove the four screws that secure the HDD to the carrier and remove the HDD.
5. Slide the replacement drive into the drive carrier.

- Initially, loosely install the top two screws. Ensure the drive is correctly oriented (i.e., right side up as per [Figure 7.18](#)).

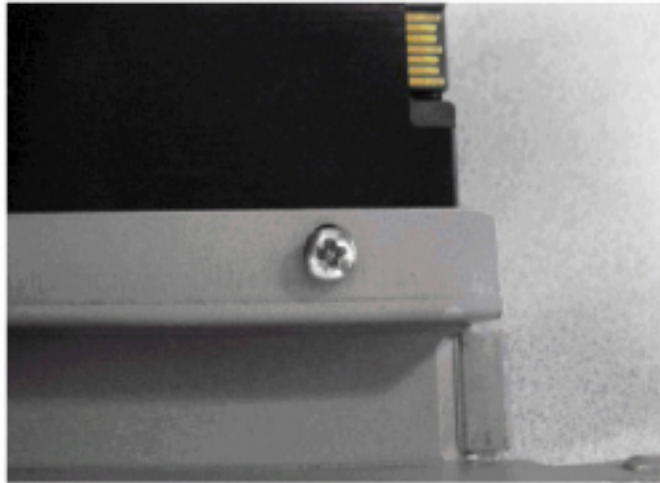


Figure 7.17: Drive Top Mount Screw



Figure 7.18: Hard Drive/SSD Installed in Driver Carrier

- Install and tighten both side mount screws.

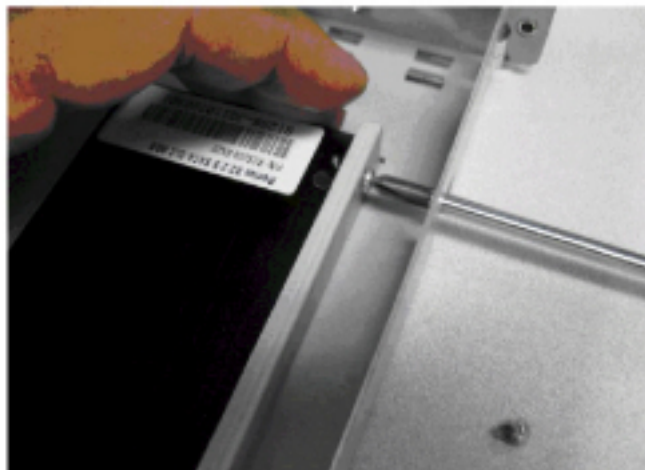


Figure 7.19: Drive Side Mount Screw

- Tighten both drive top mount screws, taking care not to twist or bend the mounting frame.
6. Push to seat the drive into the backplane.
 7. Tighten the captive screw.
 8. Continue with [Upgrade Software After Disk Drive Replacement](#).

9. After upgrading software of the first drive, replace the second drive in the HD2 position, by following [step 4](#) through [step 7](#). The RAID controller will automatically start the rebuild process. The rebuild is complete when the HD2 LED no longer flashes slowly (approximately 80G per hour).
10. After the rebuild process is complete, run the **show status redundant** maintenance command, to confirm that both drives are running. After the rebuild, the second drive (in HD2 position) will have the same MiVoice Business software version as the upgraded drive.

MXe III/MXe III-L (Two disk drives in RAID Configuration)

If the MXe III/MXe III-L has two disk drives (HDD or SSD) in a RAID (Redundant Array of Independent Disks) configuration, you can replace one or both of them.

NOTE: If the system is under warranty, you must replace both disk drives. Before proceeding with a warranty claim, contact Mitel Repair Services (see [Contacting Mitel](#)) to obtain a Return of Merchandise Authorization (RMA) number.

- [Replace one disk drive in an MXe III/MXe III-L](#)
- [Replace both disk drives in an MXe III/MXe III-L](#)

Replace one disk drive in an MXe III/MXe III-L

Replace one disk drive in a RAID configuration if only one disk drive is defective and the system is no longer under warranty.

To replace one disk drive in an MXe III/MXe III-L:

NOTE: The defective disk drive is indicated by a flashing green Host LED.

TIP: Refer to [Table](#) for a complete description of LED activity.

TIP: You do not have to power down the controller for the replacement of only one of the two drives.

1. Release the retaining screw securing the drive carrier to the controller.
2. Slide the defective drive out of the drive carrier.
3. Remove the four screws securing the drive to the drive carrier.
4. Slide the (replacement) hard drive or SSD into the drive carrier.
 - Initially, loosely install the top two screws ([Figure 7.17](#)). Ensure that the drive is correctly oriented (i.e., right side up as per [Figure 7.18](#)).
 - Install and tighten both side mount screws ([Figure 7.19](#)).
 - Tighten both drive top mount screws, taking care not to twist or bend the mounting frame.
5. Slide the drive carrier into the controller.
6. Push to seat the drive carrier into the drive backplane.
7. Tighten the thumb screw.
8. The rebuild process starts automatically. Mirroring is indicated by the HD LEDs. The source drive LED flashes quickly (indicating that the disk is being accessed) while the destination drive flashes slowly. The rebuild is complete when the destination drive LED no longer flashes slowly (approximately 80G per hour).

Replace both disk drives in an MXe III/MXe III-L

Replace both disk drives if they are both defective, or if the system is still under warranty.

NOTE: Contact Mitel Repair Services before proceeding with warranty work.

To replace both disk drives in an MXe III/MXe III-L:

1. Power down the controller.
2. Loosen the captive screws and slide both the drives from the drive carrier.
3. Clear the sockets using the following steps unique to MXe III/MXe III-L:
 - a. System must be powered down.
 - b. Both drives must be removed from the system.
 - c. With serial port connected, power on system and wait for system to report:

```
SATA RAID Controller Detected.
Bay 1 is empty.
Bay 2 is empty.
ERROR !!!! No Valid Drives Found.
Clearing the socket....Done.
Rebooting...
```

- d. Power down the system.
4. Slide the (replacement) drive into the bottom drive carrier.

CAUTION: You must install only the first drive into the bottom carrier (HD1) before you boot the system. After the system is fully booted, slide the second drive into the HD2 position.

 - a. Initially, loosely install the top two screws ([Figure 7.17](#)). Make sure it is correctly oriented (that is, right side up as per [Figure 7.18](#)).
 - b. Install and tighten both side mount screws ([Figure 7.19](#)).
 - c. Tighten both drive top mount screws, taking care not to twist or bend the mounting frame.
5. Slide the first drive into the HD1 position.
6. Push to seat the first drive into the drive backplane.
7. Tighten the thumb screw.
8. Continue with [Upgrade Software After Disk Drive Replacement](#).

Upgrade Software After Disk Drive Replacement

Overview

After disk drive replacement, you must perform a software upgrade of the replacement drive to MiVoice Business Release 9.0 or later. The software upgrade process varies depending upon the status of the replacement drive (new or used) and the MiVoice Business software version on the replacement drive; the three sections below describe the software upgrade process for each possible case:

- [New Replacement Drive with MiVB 7.2 SP2 Software](#)

- [Used Replacement Drive with Pre-9.0 Software](#)
- [Used Replacement Drive with MiVB 9.0 or Later Software](#)

NOTE: In the case of [replacement of one disk drive of an MXe III/MXe III-L controller with RAID configuration](#), a software upgrade of the replacement drive is not required.

New Replacement Drive with MiVB 7.2 SP2 Software

Overview

Use this procedure to upgrade the software on the replacement drive to MiVoice Business 9.0 or later (9.1 or later for the MXe III-L controller), if the replacement drive is a new drive with MiVoice Business 7.2 SP2 software.

NOTE: You can optionally Install System Software Manually on a 3300 ICP Controller to upgrade software.

1. [Access 3300 ICP Controller Through the Maintenance Port](#).
2. Power on the controller.
3. The U-Boot (3300 ICP controller bootloader) performs auto-discovery and boots the MiVoice Business 7.2 SP2 software load from partition 1. After the system boots, run the following command to check the system's bootline configuration and change any boot parameters if required:

```
bootChange
```

NOTE: If you modified either the *e* or *g* parameters, then you must reboot the controller for the change to take effect before continuing. Run the *reboot* command to reboot the controller.

4. Log in to the System Administration Tool after the software load boots successfully.
5. Change the default password to any password of your choice to be entered in the Migration Tool in the next step.

NOTE: During a database restore from the Server Manager, the password from the backed up database file is restored; and not the password set in this step.

6. Perform a full migration of the system to MiVoice Business Release 9.0 or later (9.1 or later for the MXe III-L controller) using the MiVoice Business Migration Tool (See [Installation of the MiVoice Business Migration Tool](#)). Ensure that you do the following:
 - Clear the **Perform Pre-Migration Audit** check box.
 - Clear the **Database Backup if No Audit Errors** check box.
 - The Migration Tool, by default assigns licenses to the system based on the information in the **License and Option Selection** form in the System Administration Tool. Ensure that the information in the **License and Option Selection** form is accurate.
 - Clear the **Database Restore** check box.
7. After the migration completes successfully, restore the database (the backed up database or the most recent Server Manager database) using the Server Manager (Administration > Restore).
8. After the database restore completes successfully (during which the system may reboot multiple times), log in to the System Administration Tool to verify that the installation is successful.

Used Replacement Drive with Pre-9.0 Software

Overview

Use this procedure to upgrade the software on the replacement drive to MiVoice Business 9.0 or later, if the replacement drive is a used drive with pre-9.0 MiVoice Business software.

NOTE: You can optionally Install System Software Manually on a 3300 ICP Controller to upgrade software.

1. [Access 3300 ICP Controller Through the Maintenance Port.](#)
2. Power on the controller.
3. Stop the auto-boot sequence from the serial port (Maintenance port), by pressing the SPACE key three or more times consecutively within seven seconds at the following prompt:

Press <SPACE> key 3 times within 7 seconds to stop autoboot.

The system displays => prompt when the auto-boot sequence stops.

4. Boot the pre-9.0 MiVoice Business software load from the active partition in one of the following two ways:
 - Run the `vxbootcfg` command (available only for U-Boot 1.0.3.11 or later) to boot the pre-9.0 MiVoice Business software load from the active partition, **1** or **4** (See the section, [Before you Begin](#) to determine the active partition number):

```
run vxbootcfg
```

Press the ENTER key until the `vxworks_active_partition` parameter is displayed; enter its value as either **1** or **4**.

Or,

- Run the `setenv` command to boot the pre-9.0 MiVoice Business software load from the active partition:

```
setenv vxworks_active_partition x (where x is either 1 or 4).
```

5. Save the changes and boot the system:

```
env save
boot
```

6. After the system boots, run the following command if you want to change any boot parameters (for example, network configuration):

```
bootChange
```

NOTE: If you modified either the *e* or *g* parameters, then you must reboot the controller for the change to take effect before continuing. Run the `reboot` command to reboot the controller.

7. Log in to the System Administration Tool after the software load boots successfully.
8. Change the default password to any password of your choice to be entered in the Migration Tool in the next step.

NOTE: During a database restore from the Server Manager, the password from the backed up database file is restored; and not the password set in this step.

9. Perform a full migration of the system to MiVoice Business Release 9.0 or later using the MiVoice Business Migration Tool (See [Installation of the MiVoice Business Migration Tool](#)). Ensure that you do the following:
 - Clear the **Perform Pre-Migration Audit** check box.
 - Clear the **Database Backup if No Audit Errors** check box.
 - The Migration Tool, by default assigns licenses to the system based on the information in the **License and Option Selection** form in the System Administration Tool. Ensure that the information in the **License and Option Selection** form is accurate.
 - Clear the **Database Restore** check box.
10. After the migration completes successfully, restore the database (the backed up database or the most recent Server Manager database) using the Server Manager (Administration > Restore).
11. After the database restore completes successfully (during which the system may reboot multiple times), log in to the System Administration Tool to verify that the installation is successful.

Used Replacement Drive with MiVB 9.0 or Later Software

Overview

Use this procedure to upgrade the software on the replacement drive to MiVoice Business 9.0 or later, if the replacement drive is a used drive with MiVoice Business 9.0 or later software.

NOTE: If the active partition number of the replacement drive happens to be the same as the active partition number of the failed drive, then the controller automatically boots the software load. In this case, go directly to Step 6.

1. [Access 3300 ICP Controller Through the Maintenance Port](#).
2. Power on the controller.
3. Stop the auto-boot sequence from the serial port (Maintenance port), by pressing the SPACE key three or more times consecutively within seven seconds at the following prompt:

```
Press <SPACE> key 3 times within 7 seconds to stop autoboot
```

The system displays `=>` prompt when the auto-boot sequence stops.

4. Boot the pre-9.0 MiVoice Business software load from the active partition in one of the following two ways:
 - Run the `ubootcfg` command (available only for U-Boot 1.0.3.11 or later) to boot the pre-9.0 MiVoice Business software load from the active partition, **1** or **2** (See the section, [Before you Begin](#) to determine the active partition number):


```
run ubootcfg
```

Press the ENTER key until the `ata_active_part` parameter is displayed; enter its value as either 1 or 2.

Or,
 - Run the `setenv` command to boot the pre-9.0 MiVoice Business software load from the active partition:


```
setenv ata_active_part x (where x is either 1 or 2).
```

5. Save the changes and boot the system:


```
env save  
boot
```

6. Configure network parameters for the controller on the Server Console. See [Configuring the Server using Server Console](#).

NOTE: If the MiVoice Business application does not complete the startup within 30 minutes, the system will reboot and attempt the MiVoice Business application startup again. To recover the system, see [Note](#) in section [Accessing Server Console](#).

7. Log in to the Server Manager and upgrade to the required software version (**ServiceLink > System Upgrade**).

Fan Complex

MXe III/MXe III-L

To replace the fan in an MXe III/MXe III-L:

1. Remove the controller cover (see [Remove Controller Cover](#)).
2. Remove the two screws that fasten the fan to the cabinet frame (see [Figure 7.20](#)).

NOTE: The fan depicted in [Figure 7.20](#) is the early version. The new version uses longer cables that must be tied off as shown in [Figure 7.21](#).

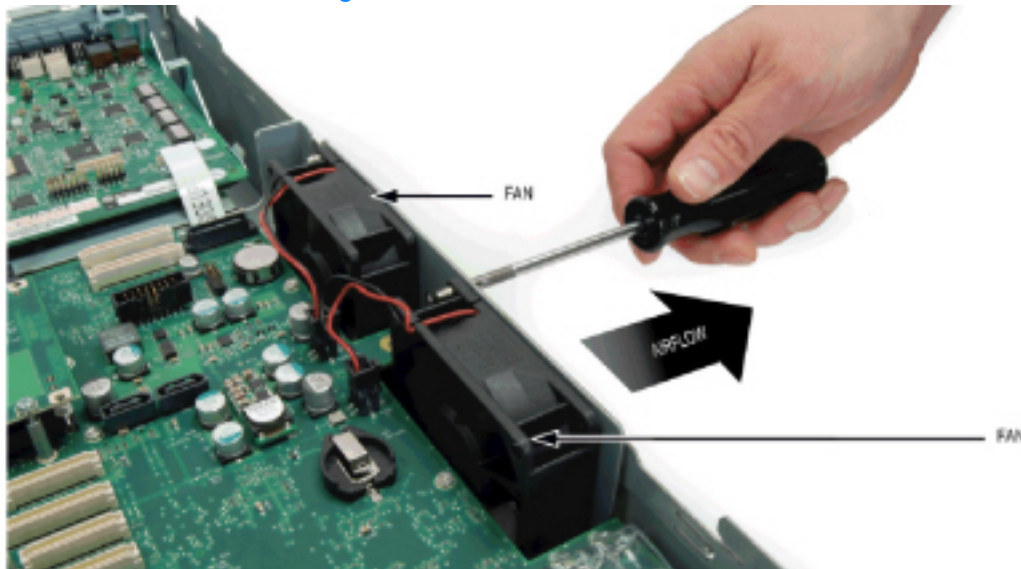


Figure 7.20: Fan Removal

3. Remove the fan power connector from the MXe III/MXe III-L chassis board and remove the faulty fan.
4. Insert the replacement fan so that
 - the power cables exit the fan closest to the fan power connector, and
 - the sticker label on the center of the fan is facing out from the cabinet towards the grill.

For proper air flow, the fan sticker label must be facing the cabinet grill.

5. If you have a new fan assembly with longer cables, loop and tie them together using the supplied cable ties as shown in Figure 40.

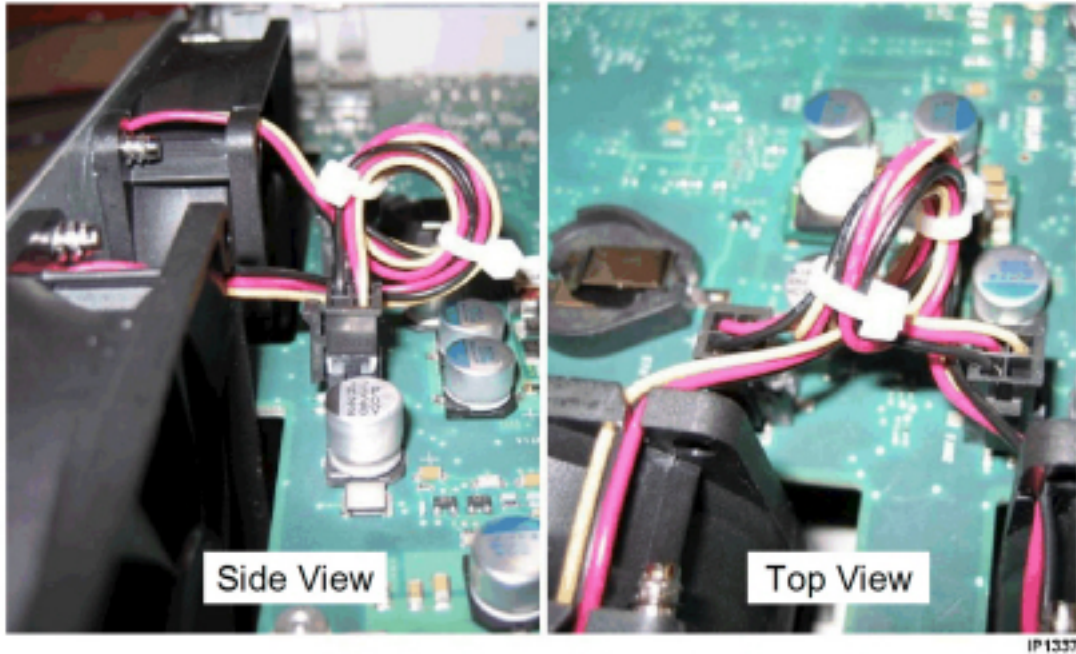


Figure 7.21: Fan Cable Management (New Fan Assembly)

6. Replace the fan screws.
7. Plug in the fan power connector.
8. Replace the cabinet cover and secure with screw.

AX

To replace the fan in an AX controller:

1. Loosen the captive screws; one at each end of the fan assembly.
2. Pull out the fan unit carefully. The cable is attached to the back of the fan unit at the right side.
3. Disconnect the cable by squeezing the latch at the cable end of the connector and carefully wiggling the connector out.
4. Connect the new fan unit cable and set the new fan assembly in place.
5. Tighten the two fan assembly screws.

CX II/CXi II

To replace the AMB in a CX II/CXi II:

1. Power down the controller and remove the controller cover; see [Power Down the Controller](#) for procedure.
2. Remove the Analog Option Board, if one has been installed. Remove by reversing the steps on [Analog Option Board](#) of this document.

3. Remove the AMB as follows referring to [Figure 7.22](#):
 - Disconnect the power supply cable on the AMB.
 - Disconnect the ribbon cable on the AMB (not from the main board).
 - Unfasten the four screws holding the AMB to the controller chassis.
 - Remove the AMB by pushing it toward the front on the controller, and then tipping it upwards.
4. Insert the new AMB and secure it to the chassis using the supplied screws.
5. Reconnect ribbon cable.
6. Reconnect the power cable to the new AMB.
7. Replace the Analog Option Board (if previously removed).

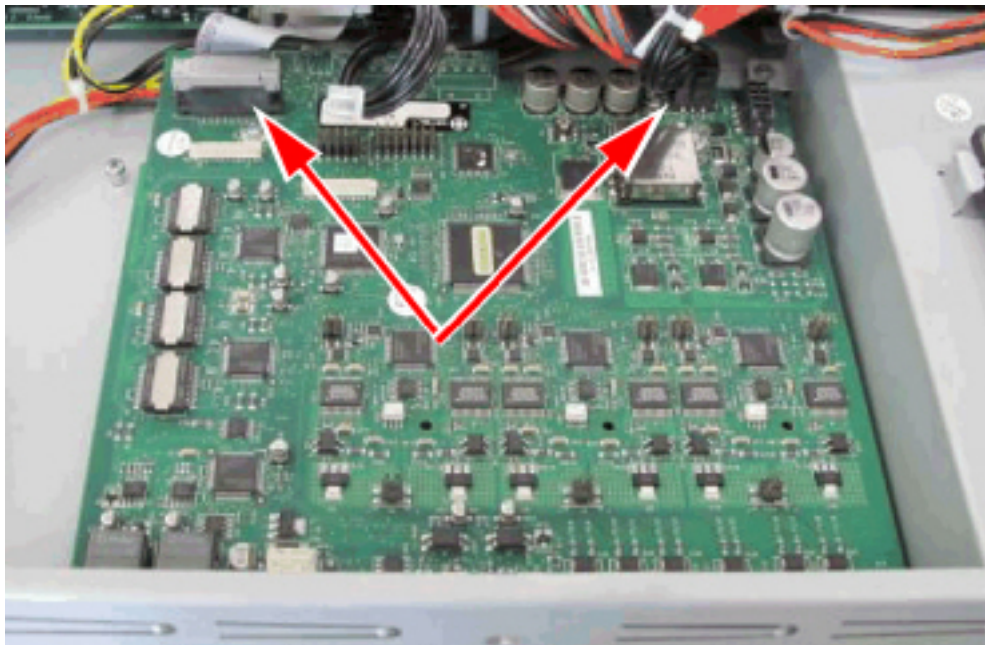


Figure 7.22: AMB - Disconnect Cables

Power Supply Unit

MXe III/MXe III-L, AX

To replace a power supply unit in a single power supply MXe III/MXe III-L or AX:

1. Turn off the power switch on power supply.
2. Remove the power cord from the power supply AC receptacle.
3. Loosen the thumb screw with a Phillips screwdriver on the power supply and slide it out.
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 tighten it with a Phillips screwdriver.
8. Connect the power cord and set the AC power switch to ON.

ASU II

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 using a Phillips screwdriver.
3. Pull the power supply out.
4. Slide the new power supply into the slot on the rear of the ASU II, with the thumb screw on the bottom.
5. Push to seat the new power supply into the system.
6. Secure the thumb screw and tighten it with a Phillips screwdriver.
7. Insert the AC power cord into the power supply AC receptacle.

Redundant Power Supply

AX, MxIII/MxIII-L

To add or replace a redundant power supply in an AX and MxIII/MxIII-L:

TIP: If two power supplies are installed, one can be swapped out without turning the other off. The system can remain running on one power supply while the other is replaced.

1. Set the AC power switch to OFF, and remove the power cord from the AC receptacle on the power supply.
2. Loosen the thumb screw on the power supply with a Phillips screwdriver.
3. If replacing a power supply, slide the power supply unit out of the power supply carrier on the rear of the controller or If adding a power supply, remove the power supply unit blanking panel.
4. Slide the new power supply unit into the power supply carrier on the rear of the controller.
5. Push to seat the power supply into the power supply backplane.
6. Secure the thumb screw with a Phillips screwdriver and connect the power cord.
7. Set the AC power switch to ON. AC and DC LEDs will illuminate.

RAID Controllers

The RAID (Redundant Array of Independent Disks) controller mirrors all data on two disk drives. In the event that one drive fails, the system continues 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.

MXe III/MXe III-L

To add a RAID controller in an MXe III/MXe III-L:

1. Access the MXe III/MXe III-L carrier board (see [Remove Controller Cover](#)).
2. Remove the Stratum 3 clock module and keep the screws.
3. Before you install the RAID controller, first remove the grey plastic bezel that covers the RAID controller LED and push button holes. The bezel is located on the rear panel of the controller.
4. On the inside of the cover, insert a thin, pointed object through an LED hole. Push the bezel cover out far enough to allow you to grasp the top and bottom edges. Pull the bezel cover off the controller cover.
5. Position the new RAID controller board by carefully inserting the LED indicators into the holes in the controller rear panel (see [Figure 7.23](#)).

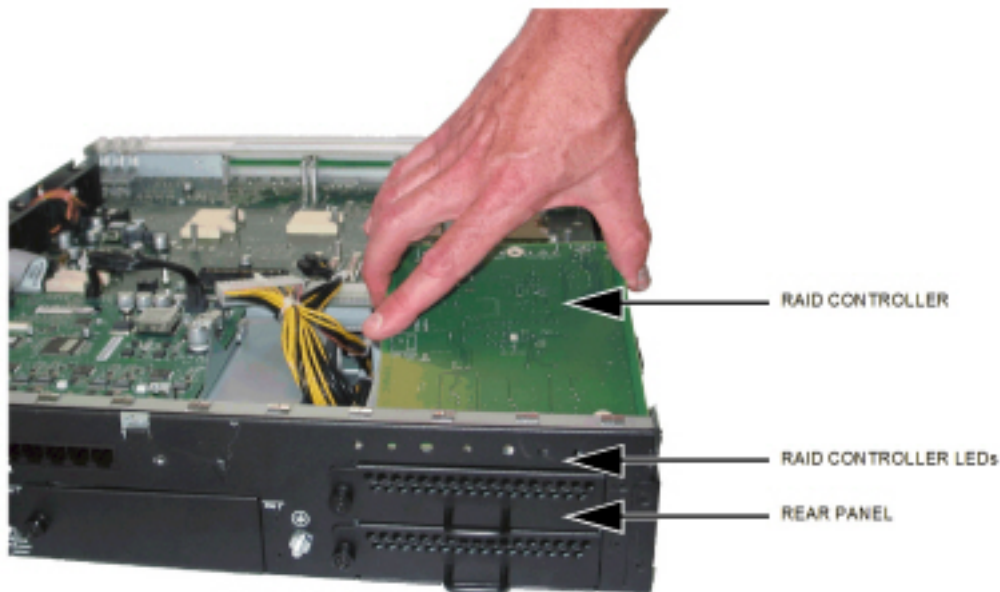


Figure 7.23: Disconnecting the AMB Power Connector

6. Slowly retract the RAID controller from the LED holes until the mounting holes align with the standoffs.
7. Secure the RAID controller to the standoffs with the three (3) screws.

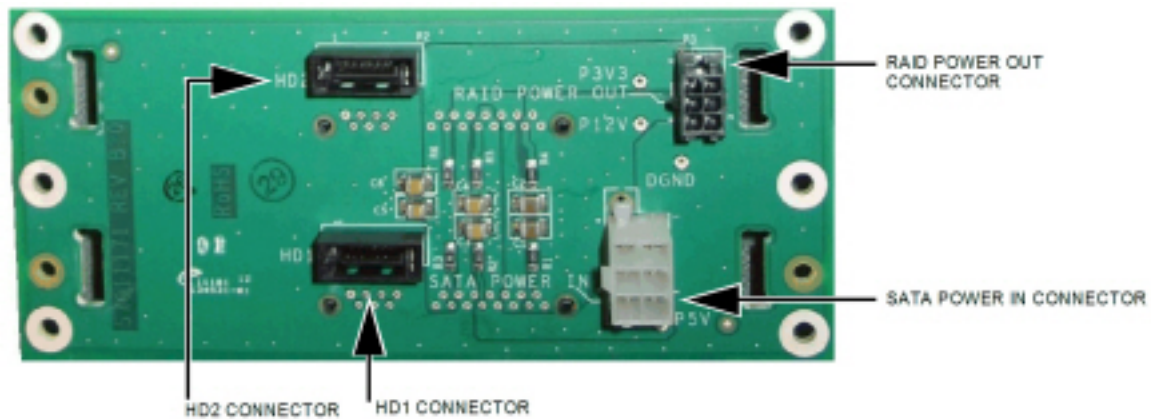


Figure 7.24: Hard Drive Backplane Connectors

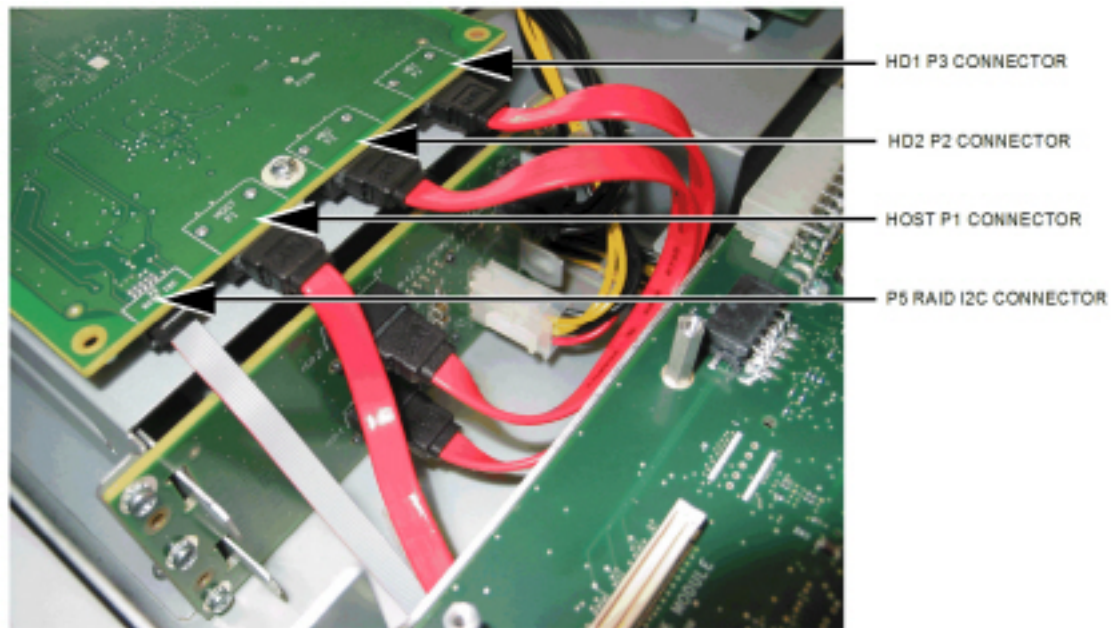


Figure 7.25: RAID Controller Connectors

8. Cut the cable tie joining the I2C (small ribbon) cable to the SATA cable.
9. Connect the I2C (small ribbon) cable to the P5 RAID I2C connector on the RAID controller.
10. Disconnect the SATA cable from the HD1 connector on the HD backplane and reconnect it to the Host P1 connector on the RAID controller.
11. Using one of the supplied SATA cables, connect the HD1 connector on the HD backplane to the HD1 P3 connector on the RAID controller.
12. Using the second SATA cable, connect the HD2 connector on the HD backplane to the HD2 P2 connector on the RAID controller.

13. Using the supplied power cable, connect the RAID POWER OUT connector on the HD backplane to the SATA BCKPLNE POWER connector on the RAID controller.

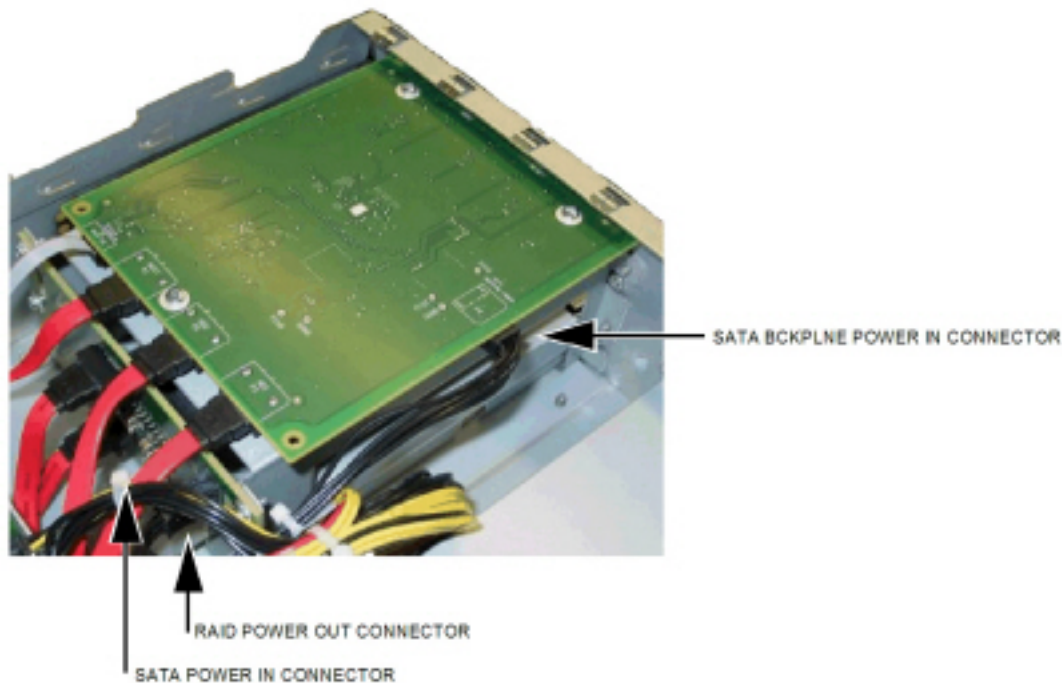


Figure 7.26: Power Connectors

CAUTION: Push the SATA, I2C and power cables out of the way so that they are not pinched by the top cover.

14. Reinstall the Stratum 3 clock module with the retained screws.
15. Replace the top cover and secure with screw.
16. Power on controller and proceed with step 7 of section [Replace One disk drive in an MxIII/MxIII-L](#).

To replace a faulty RAID controller:

1. Remove the controller cover (see [Remove Controller Cover](#)).
2. Disconnect the three SATA cables, the I2C cable, and the power cable from the faulty RAID controller.
3. Using a Phillips #2 screwdriver, remove the three screws from the RAID controller.
4. Remove the faulty RAID controller and place it in an anti-static bag.
5. Remove the replacement RAID controller from the anti-static bag.
6. Position the replacement RAID controller by carefully inserting the LED indicators into the holes in the controller rear panel.
7. Slowly retract the RAID controller from the LED holes until the mounting holes align with the standoffs.
8. Secure the replacement RAID controller to the standoffs with the three (3) screws.
9. Reconnect the power cable to the RAID controller.
10. Carefully reconnect the three SATA cables:
 - Connect the RTC (under chassis) to the Host P1 connector on the RAID controller.

- Connect the HD1 connector on the HD backplane to the HD1 P3 connector on the RAID controller.
 - Connect the HD2 connector on the HD backplane to the HD2 P2 connector on the RAID controller.
11. Connect the I2C (small ribbon) cable to the P5 RAID I2C connector on the RAID controller.
 12. Replace the top cover. Using a #1 Phillips screwdriver, tighten the screw that fastens the top cover to the chassis.

Line Cards

AX

To install 24 Port ONS, 16 Port ONS, or 4+12 Port Combo line cards:

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.

ASU II

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.

NOTE: You must buy a license for each ASU II you install.

To install 24 Port ONS, 16 Port ONS, or 4+12 Port Combo line cards:

1. If necessary, loosen the thumbscrew using a Phillips screwdriver 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 thumbscrew with a Phillips screwdriver.
4. Connect the Amphenol cable and secure the strap.

Controller Card (AX)

Before you begin

Ensure that:

- You have a replacement AX controller card (brand-new or used)
- You have access to the controller's Maintenance port
- You know the active partition number on the Compact Flash (CF); this is important because you must boot the system from the active partition. If you do not know the active partition number, see [Determine Last Known Active Partition using U-Boot](#)

- You know the VLAN ID for which the system was configured. If you do not know the VLAN ID, follow the procedure below to determine the VLAN ID; please note that a system reboot would be required to configure the correct VLAN ID

To replace the AX controller card

1. *Power down the controller* and disconnect cables.
2. From the rear of the controller, loosen the lock screw at the bottom of the controller card.
3. Lift the lock latch and slide the controller card from the chassis.
4. Transfer the i-Button, flash card(s), and MMCs to the new controller card. The AX controller contains a single 16 GB CF that must be installed in the COMPACT FLASH 2 slot.
5. Slide the replacement controller card into the chassis.
6. Push the lock latch down and tighten the lock screw.
7. Connect the cables
8. *Access 3300 ICP Controller Through the Maintenance Port.*
9. Power on the controller, and stop the auto-boot by pressing the SPACE key three or more times consecutively when the countdown starts.

Then, *Determine 3300 ICP Controller Bootloader type*. If the bootloader is:

- U-Boot - Skip the rest of this step
- Bootrom - Execute the following steps to upgrade the card's bootloader to U-Boot:
 - i. Execute the `version` command, and verify that the bootline is configured to boot from the partition 1 (**/partition1/RTC8260**). Otherwise, execute the `bootChange` command and modify the file name parameter to point to partition 1.
 - ii. Execute the `@` command to boot the image from the partition 1. The Bootrom boots the VxWorks development image from **/partition1/RTC8260** automatically and displays the `->` prompt.
 - iii. From the communication application, run the following VxWorks shell commands:


```
Upgrade_Xilinx
Upgrade_Bootrom
reboot
```

10. From the communication application, stop the auto-boot sequence by pressing the SPACE key three or more times consecutively within seven seconds at the following prompt:

```
Press <SPACE> key 3 times within 7 seconds to stop autoboot
```

The system displays `=>` prompt.

11. Run the `ubootprint` command (available only for U-Boot 1.0.3.11 or later) to determine whether the bootloader is configured with the correct active partition number on the Compact Flash (CF):

```
run ubootprint
```

The `ata_active_part` parameter displays either 2 or 3 as its value.

You can also run the following command to check the value of the `ata_active_part` parameter:

```
print ata_active_part
```

The system displays either 2 or 3 as the active partition number.

12. If the bootloader is configured with an incorrect active partition number, you can configure the bootloader with the correct active partition number in one of the following two ways:

- Run the `ubootcfg` command (available only for U-Boot 1.0.3.11 or later):

```
run ubootcfg
```

Press the ENTER key until the `ata_active_part` parameter is displayed, and enter its value as either 2 or 3.

Or,

- You can run the following command to configure the bootloader with the correct active partition number:

```
setenv ata_active_part x
```

where x is either 2 or 3.

13. If the system was configured on a different VLAN than the default VLAN (1), then run the following command to modify the VLAN:

```
setenv vlan x
```

where x is the VLAN ID of the system

If you do not know the VLAN ID, then let the default value remain. If your system was upgraded to MiVoice Business Release 9.1 or later, the system will auto-discover and auto-correct the VLAN ID on the new AX Controller card (the system performs an extra reboot to achieve this). If your system still runs the default factory image (9.1.0.75), then you must manually recover the VLAN ID, later, as part of Step 16.

14. Run the following commands:

```
env save
```

```
boot
```

15. After the system boots, log in to the Server Console using Method 1 (see [Configure the Server Using Server Console](#)), configure the system, and then reboot the system.
16. If your system was upgraded to MiVoice Business 9.1 or later prior to the AX controller card replacement, skip this step. If your system is still running the default factory image (9.1.0.75) and you did not set the correct VLAN ID in Step 13, wait for the system to fully boot and then manually [recover the VLAN ID of a 3300 ICP controller](#).
17. After the system boots, verify that you can access the system over the network.
18. Log in to the Server Manager and System Administration Tool to verify that the system is fully functional.

Compact Flash Cards (AX)

In MiVoice Business Release 9.1 or later, the AX Controller requires a single 16 GB Compact Flash (CF). The 16 GB CF must be inserted in the Compact Flash 2 slot of the controller, leaving the Compact Flash 1 slot empty.

NOTE: In the pre-9.0 MiVoice Business release, the AX controller required two Compact Flash cards:

- Voice Mail (4 GB) flash: inserted in the Compact Flash 1 slot
- System (2 GB) flash: inserted in the Compact Flash 2 slot

Before you begin

Ensure that:

- You have a replacement (new or used) 16 GB CF with the required MiVoice Business 9.1 software version installed.
NOTE: If you have a used 16 GB CF, you must know its active partition number (2 or 3).
NOTE: If you want to run a pre-9.0 MiVoice Business software version on your AX controller (that is currently running MiVoice Business 9.1 or later), you must have a 2 GB/4 GB CF combo with the required pre-9.0 MiVoice Business (or earlier) load on it.
- You have access to the controller's Maintenance port.

To replace a 16 GB Compact Flash Card in the AX:

1. Shut down the system from the Server Manager (see **Administration > Shutdown or reboot** in the Server Manager).
*NOTE: If you are unable to log in to the Server Manager, then log in as the root user through the maintenance port and run the command: **poweroff**. Next, see [Step 2](#).*
If you are unable to log in through the maintenance port, power down the controller and skip [Step 2](#).
2. Observe the output on the Maintenance port, and power down the controller when you observe the message: **System Halted, OK to turn off power**.
3. Remove the controller card ([Controller Card \(AX\)](#)).
4. If you do not have an expansion card installed in the MMC-A slot 1, directly remove the current 16 GB CF from the Compact Flash 2 slot. Skip to [Step 6](#).
5. If you have an expansion card installed in the MMC-A slot 1, you must first remove the MMC-A slot 1 card. Next, remove the current 16 GB CF from the Compact Flash 2 slot.

6. Insert the replacement 16 GB CF in the Compact Flash 2 slot.

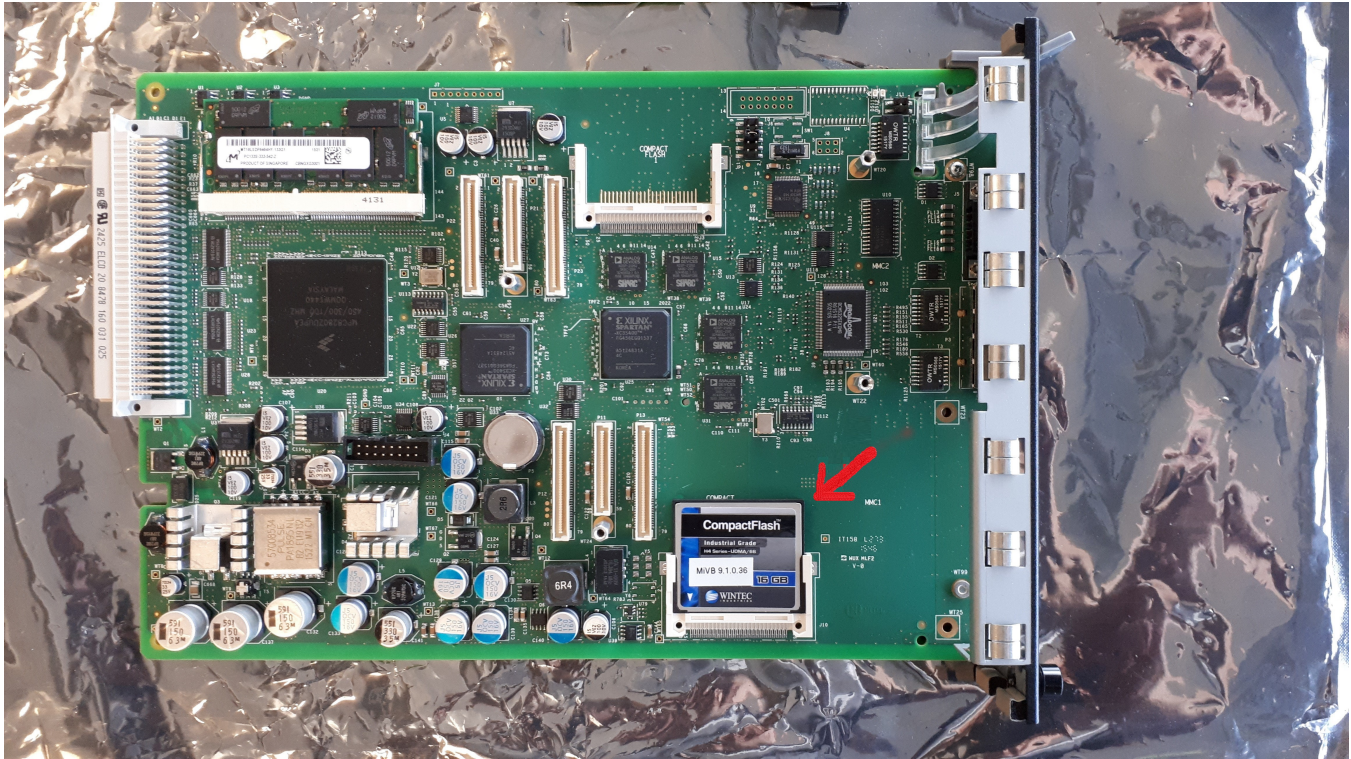


Figure 7.27: 16 GB CF placed in the Compact Flash 2 slot

7. Reinsert the AX controller card into its shelf and reconnect the cables.
8. If you have a brand-new replacement 16 GB CF, then:
 - a. U-Boot boots the system software from a partition number of its choice (2 or 3).
 - b. The system will display the End User Licence Agreement screen of the Bootstrap Console on the communication application. Read the entire EULA text; if you are in agreement, select **Accept** to proceed with the configuration of Server Manager (see [Set Network Configuration on 3300 ICP Controller with a New HDD](#)).
9. If you have a used replacement 16 GB CF, then:
 - a. *Determine its active partition number.* Use the following command to set the correct active partition number (available only for U-Boot 1.0.3.11 or later):

```
run ubootcfg
```

Press the ENTER key until the `ata_active_part` parameter is displayed; enter its value as either 1 or 2.

You can also run the `setenv` command to set the correct active partition number:

```
setenv ata_active_part x (where x is the active partition number of the used 16 GB CF)
```

- b. Save the changes and boot the system:

```
saveenv
```

```
boot
```

- c. After the system boots, log in to the Server Console using Method 1 (see [Configuring the Server using Server Console](#)).

10. After the system boots fully, verify that you can access the system over the network. If the system does not respond to pings, you must make sure that the system's VLAN ID was configured properly; see [Recover the VLAN ID of a 3300 ICP Controller](#).
11. Log in to the Server Manager and System Administration Tool to verify that the system is fully functional.

Memory Module (AX, CX II, CXi II, MxIII)

Follow this procedure to upgrade the following factory-installed memory modules:

- 256M RAM to 512M (for AX)
- 512M to 1GB (for MxIII, CX II, CXi II)

NOTES:

- a. For the CX II and CXi II controllers, the memory module is located on the underside of the main board making it less accessible and thus more difficult to replace (see [Figure 7.28](#)). It is strongly recommended that you practice this procedure before attempting to perform it on the customer's side.
 - b. To install the 50006727 (1 GB RAM Module Upgrade) part, a prerequisite is that the system runs at least MCD6.0 and that there is no active bootrom alarm. This ensures that the bootrom is at 3.1.0.11 version, the first one that supports 1GB RAM.
1. Power down the controller (see [Power Down the Controller](#)) and disconnect all cables.
 2. Remove the controller cover (see [Remove Controller Cover](#)). For the AX controller, remove the controller card ([Controller Card \(AX\)](#)).
 3. Locate the memory module.



Figure 7.28: Memory Module - AX, MxIII

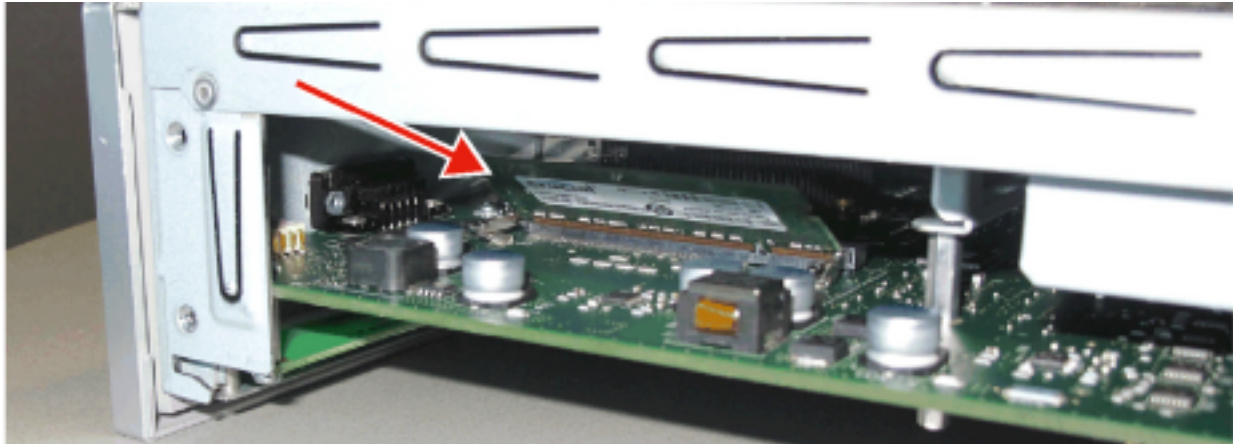


Figure 7.29: Memory Module (partially removed) on CX II, CXi II (shown in upside down position)

NOTE: On the CX II and CXi II controllers, the memory module is located on the underside of the main board.

4. For MXe III/MXe III-L only, complete the following steps, then continue with Step 6.
 - a. Access the RTC - follow steps 2 to 8 in the [Accessing the MXe III/MXe III-L Carrier Board](#).
 - b. Set the main board on a flat surface with the underside facing up. See [RTC Processor](#).
5. For CX II or CXi II only, complete the following steps:
 - a. In a well lit area, place the controller on a flat surface with the underside facing up. See [Figure 7.29](#).
 - b. With your index fingers, reach inside the controller to the memory module and release the retainer clips (see the figure below).

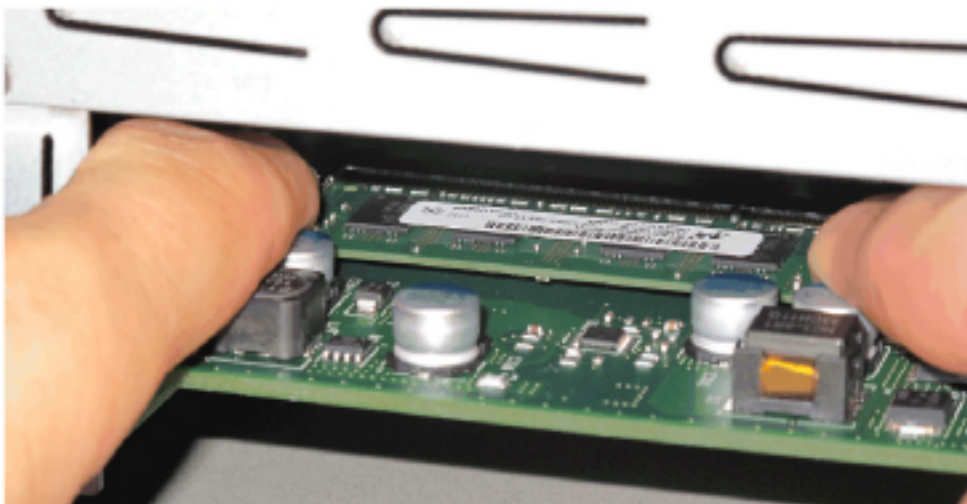


Figure 7.30: Memory Module Removal on CX II, CXi II

6. Remove the installed memory module as follows:
 - pull both spring retainer clips on either side of the module outward (see the figure below).

- grasp the module by the sides, and carefully pull it out of its connector. Place it in an antistatic bag.

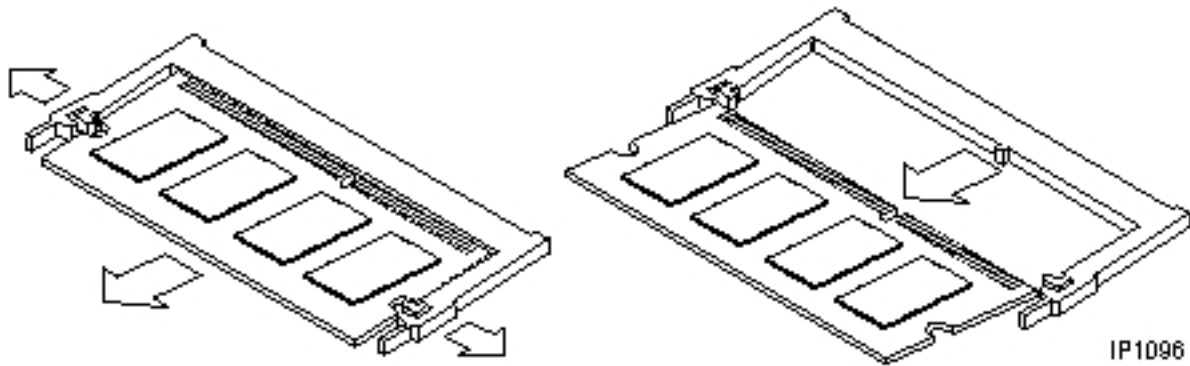


Figure 7.31: Memory Module Removal

7. Install the replacement memory module as follows:

- remove the module from its protective packaging, holding the module only by the edges.
- holding the module at approximately a 30-degree angle to the board, insert the bottom edge of the module into the slot's connector (see [Figure 7.32](#)).

The socket and module are both keyed (notched), which means the module can be installed one way only (see [Figure 7.33](#)).

For CX II or CXi II, ensure that the notch along the bottom edge of the module is on the right side (see [Figure 7.33](#)).

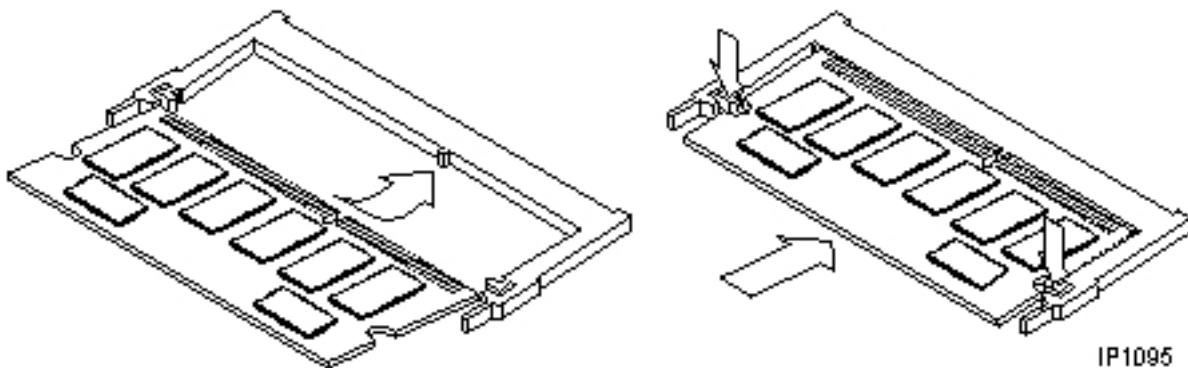


Figure 7.32: Memory Module Installation

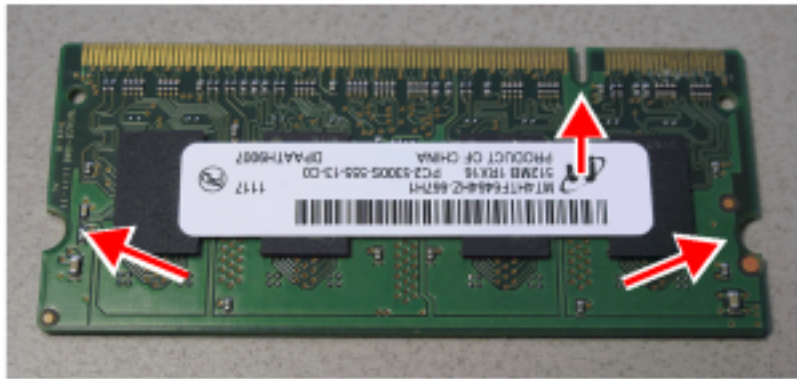


Figure 7.33: Notch Location

8. With even pressure, push simultaneously on both upper corners of the module until its bottom edge is firmly seated in the connector.
9. Press the top edge of the module toward the board until the retainer clips click into place.
10. Affix the label included with the replacement module to the main board. The label ensures proper handling should you need to return the controller to Mitel for repair.
11. For MXe III/MXe III-L only, complete the following steps:
 - a. Reach underneath the carrier board and re-connect the I2C and SATA cables as follows:
 - I2C cable to the RTC (host) connector
 - SATA cable to the SATA1 connector on the RTC
 - both cables to the hard drive backplane (or RAID controller if installed)
 - b. Reverse steps 7 to 2 from procedure [Accessing the MXe III/MXe III-L Carrier Board](#).
12. Replace the cover and reconnect power.
13. Verify that the module and software is properly installed by powering up the controller and confirming that it boots up.

Install Cabinet FRUs

Refer to the 3300 R7.0 version of the Technician's Handbook for peripheral cabinet procedures.

Appendix A: Hardware Reference

System Configurations

There are several basic versions of the 3300ICP:

- AX Controller
- MxIII/MxIII-L Controller
- CXi II system with embedded Analog and an Ethernet Layer 2 switch
- CX II system with embedded Analog and without Ethernet Layer 2 switch

Controller Hardware Details

For detailed information on the 3300 ICP components, see the *3300 ICP Hardware Technical Reference Manual* in the [Document Center](#).

TIP: Refer to the 3300 R7.0 version of the Technician's Handbook for hardware details of the older controllers.

Controller Components

TIP: For each module, the leftmost connectors correspond to Port 1 for that module, and the rightmost to Port 2.

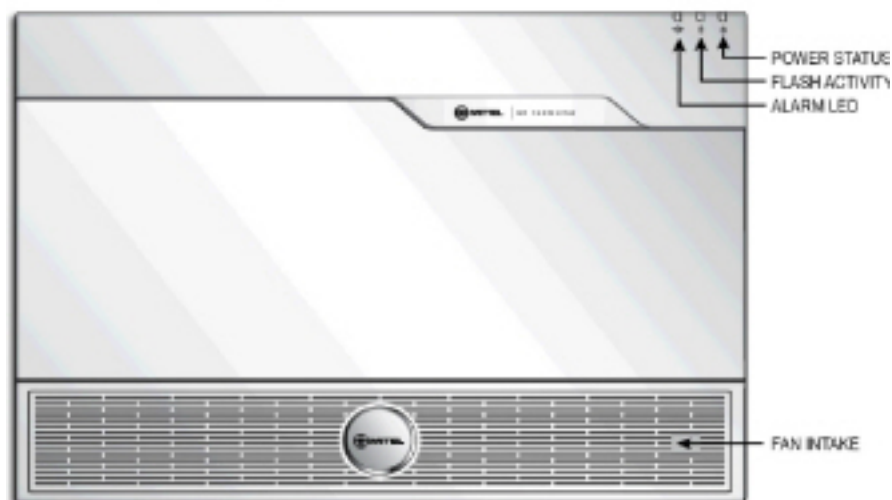


Figure 8.1: AX Controller – Front Panel

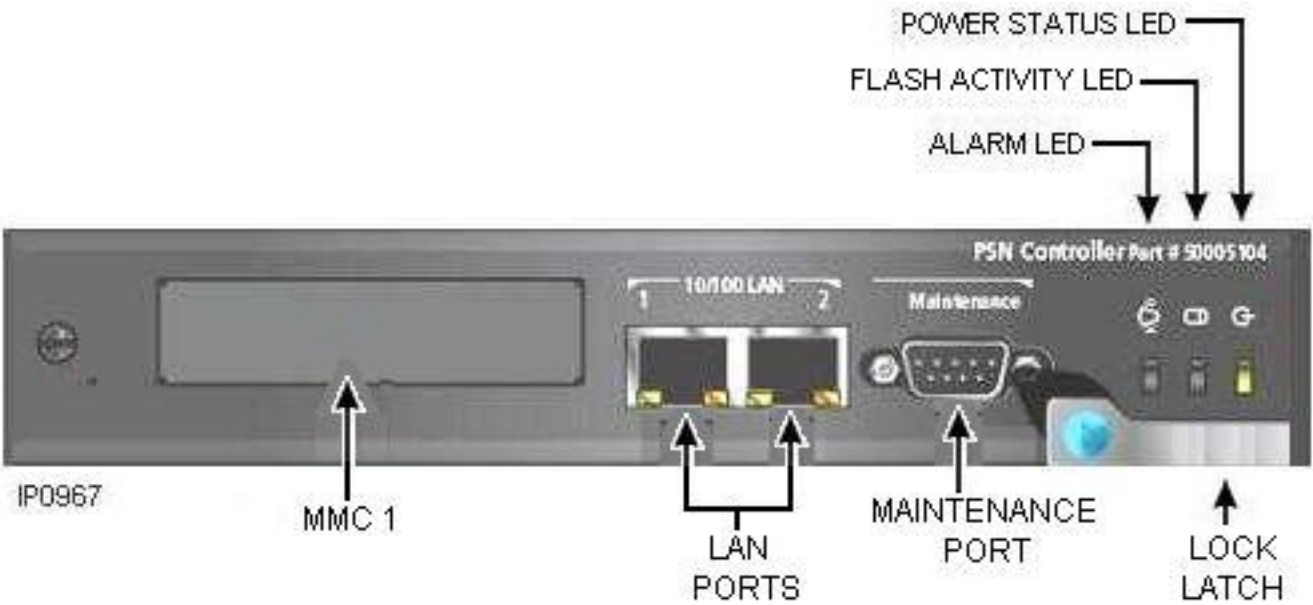


Figure 8.2: AX Controller Card View



Figure 8.3: AX Controller – Rear Panel

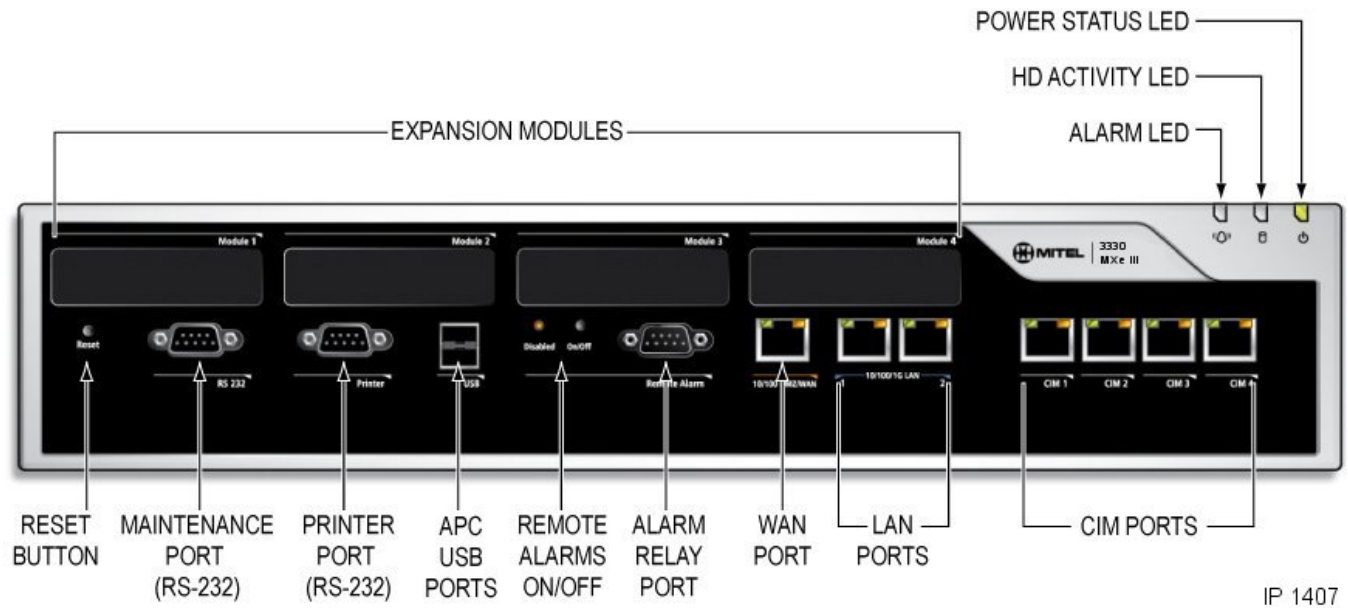


Figure 8.4: MXe III Controller – Front Panel

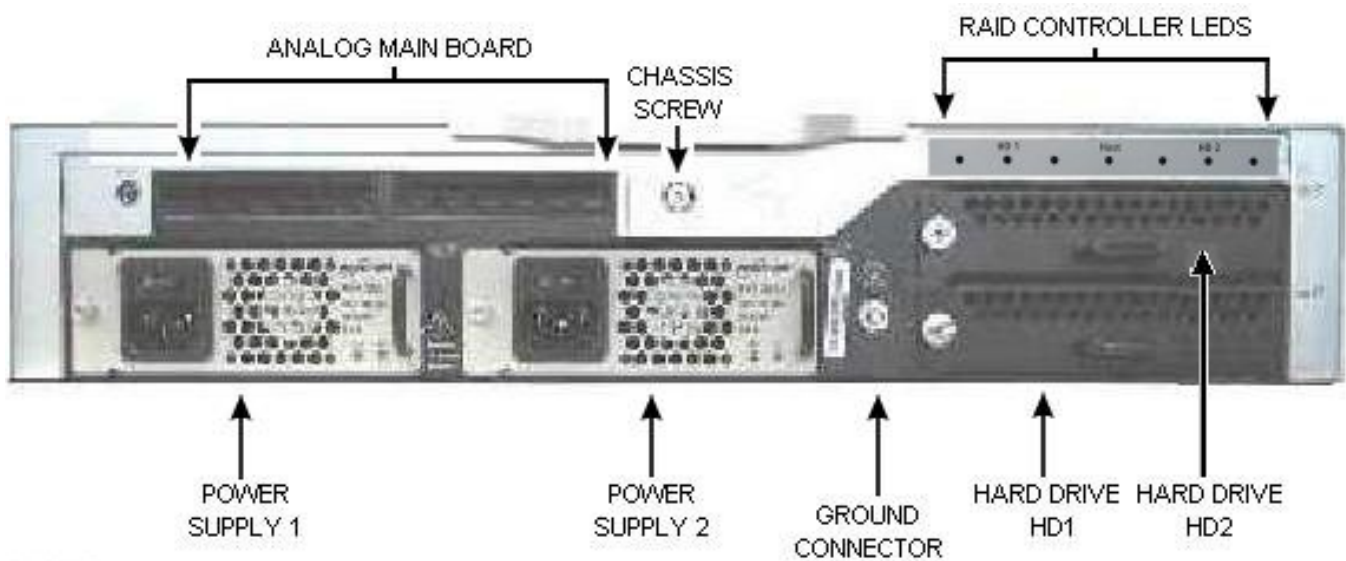


Figure 8.5: MXe III/MXe III-L Controller – Back Panel, Redundant

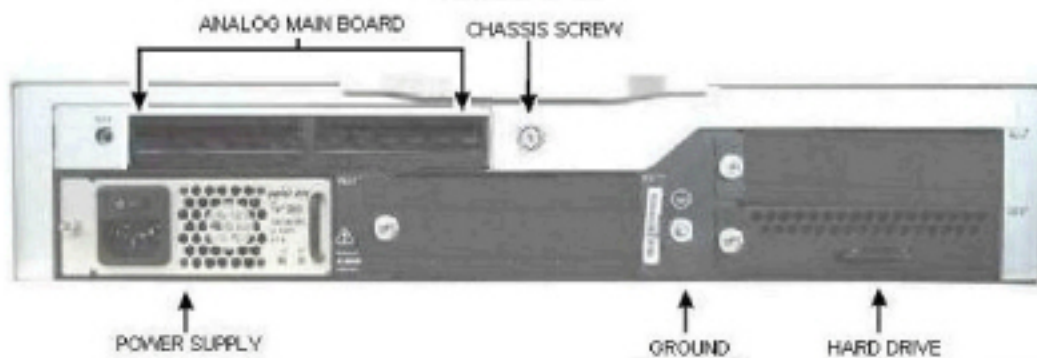
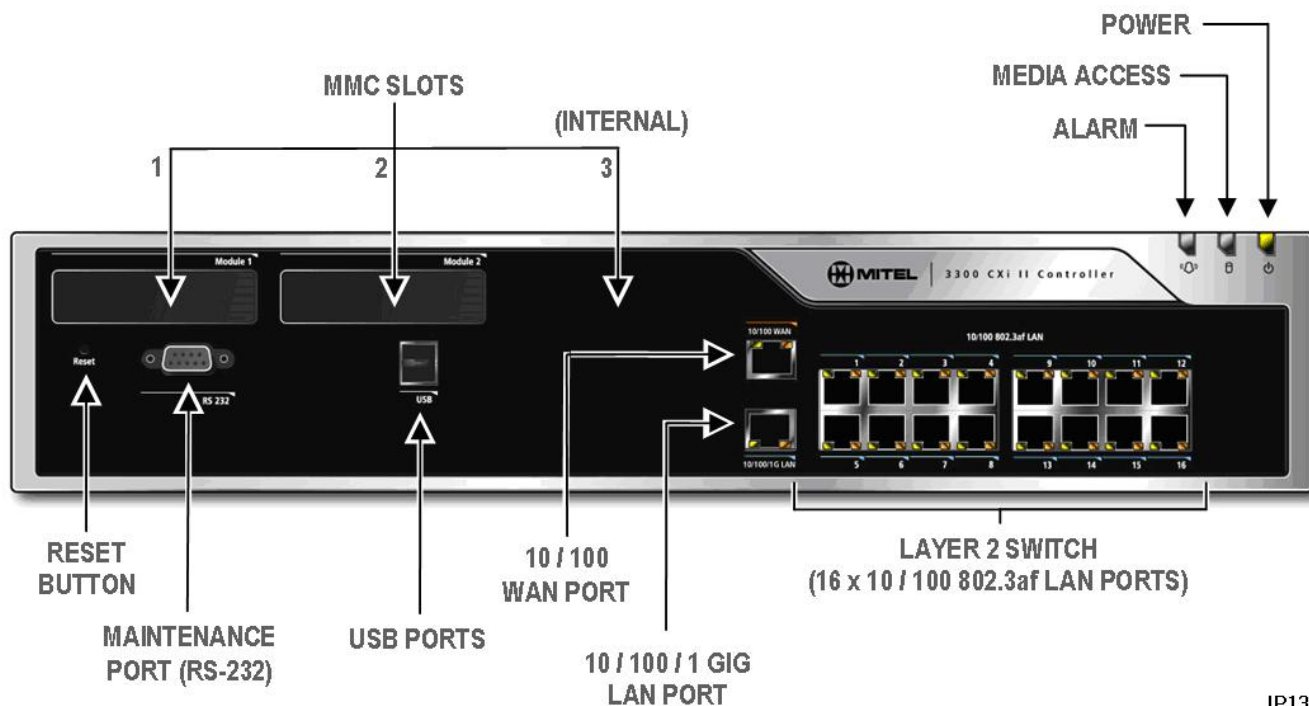


Figure 8.6: MXe III/MXe III-L Controller – Back Panel, Non-Redundant

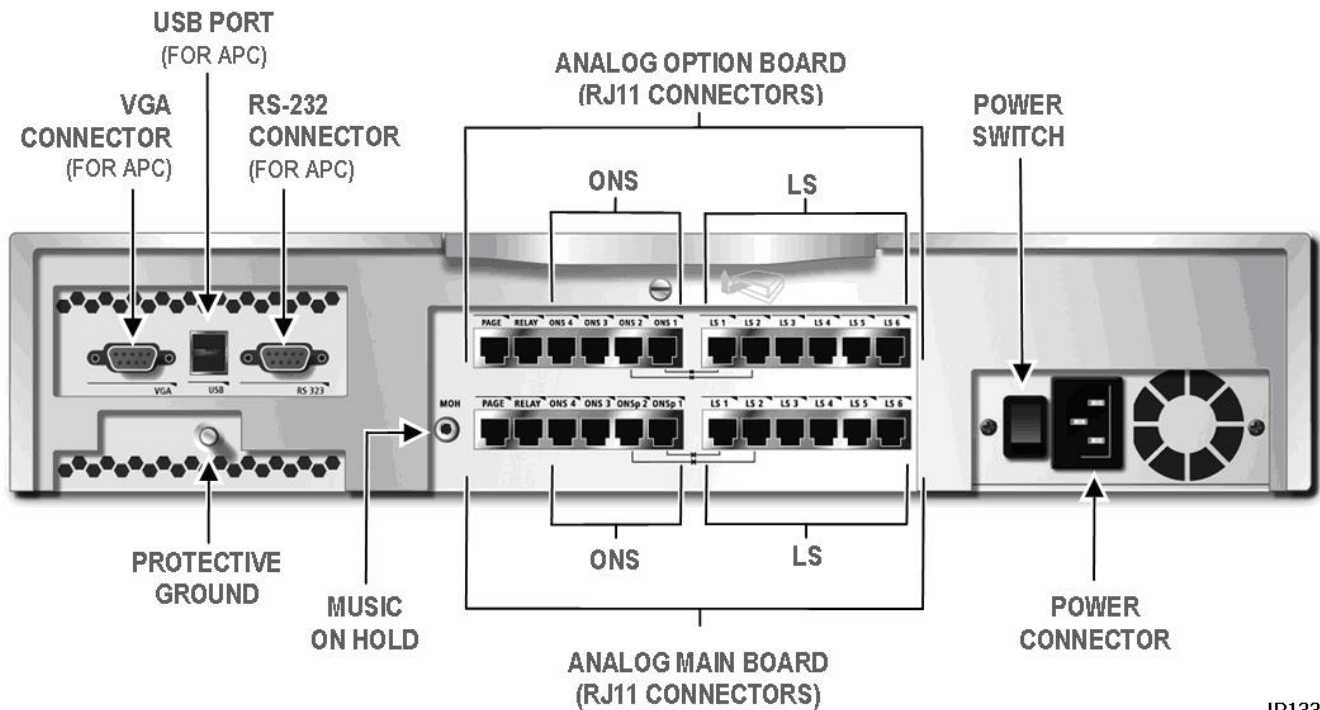


Figure 8.7: MXe III-L Controller - Front Panel



IP1333

Figure 8.8: CXi II Controller - Front Panel



IP1332

Figure 8.9: CX II and CXi II - Back Panel

Controller Cabinet Numbering

- Cabinet 1 (hardcoded): internal.
- Cabinets 2 to 21(highest): module ports (left to right).

NOTE: MxIII/MxIII-L have 4 embedded CIM ports. All systems except for MxIII Server have Embedded Analog.

T1/E1 Combo Card

The T1/E1 combo module provides T1 trunking and DSP functionality for all controllers (266/300 MHz minimum) with 3300 R7.0 software (MCD 4.0 on the CX II/CXi II). The DSP provides resources for CLASS

tone generation, Record a Call conferences, DMTF receivers, voice compression. The card also provides voice echo cancellation.

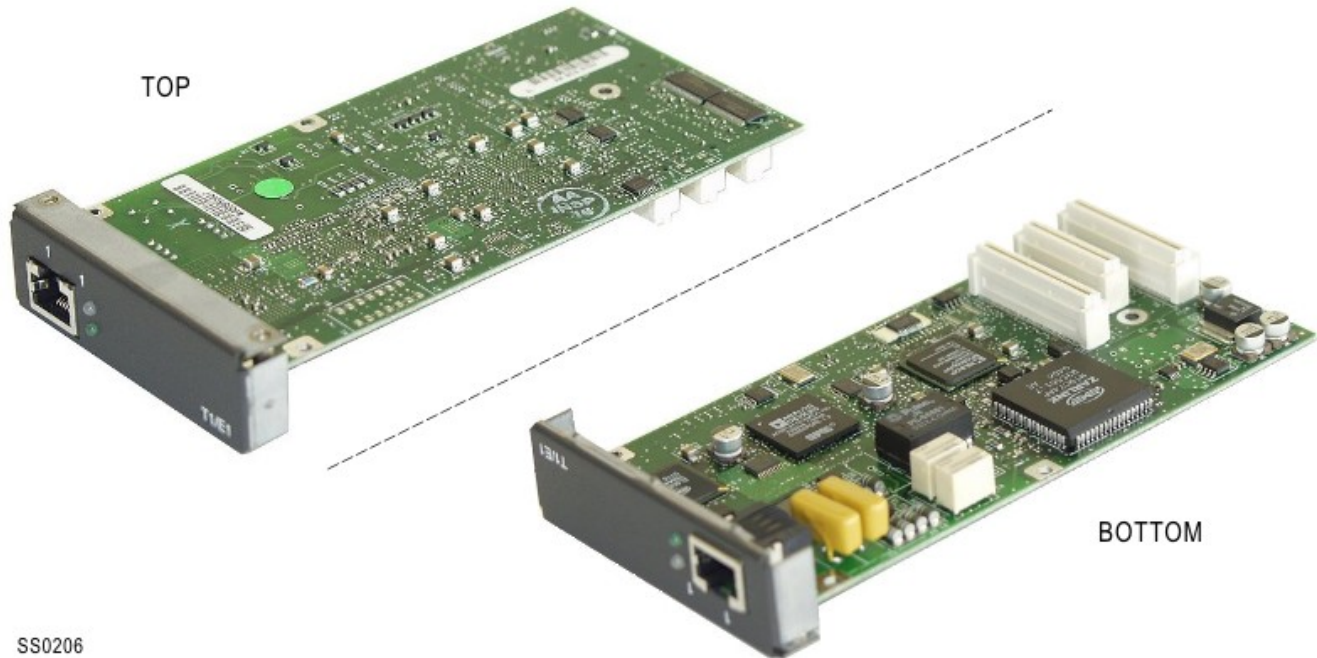


Figure 8.10: T1/E1 Combo Card (prior to 3300 R7.0)

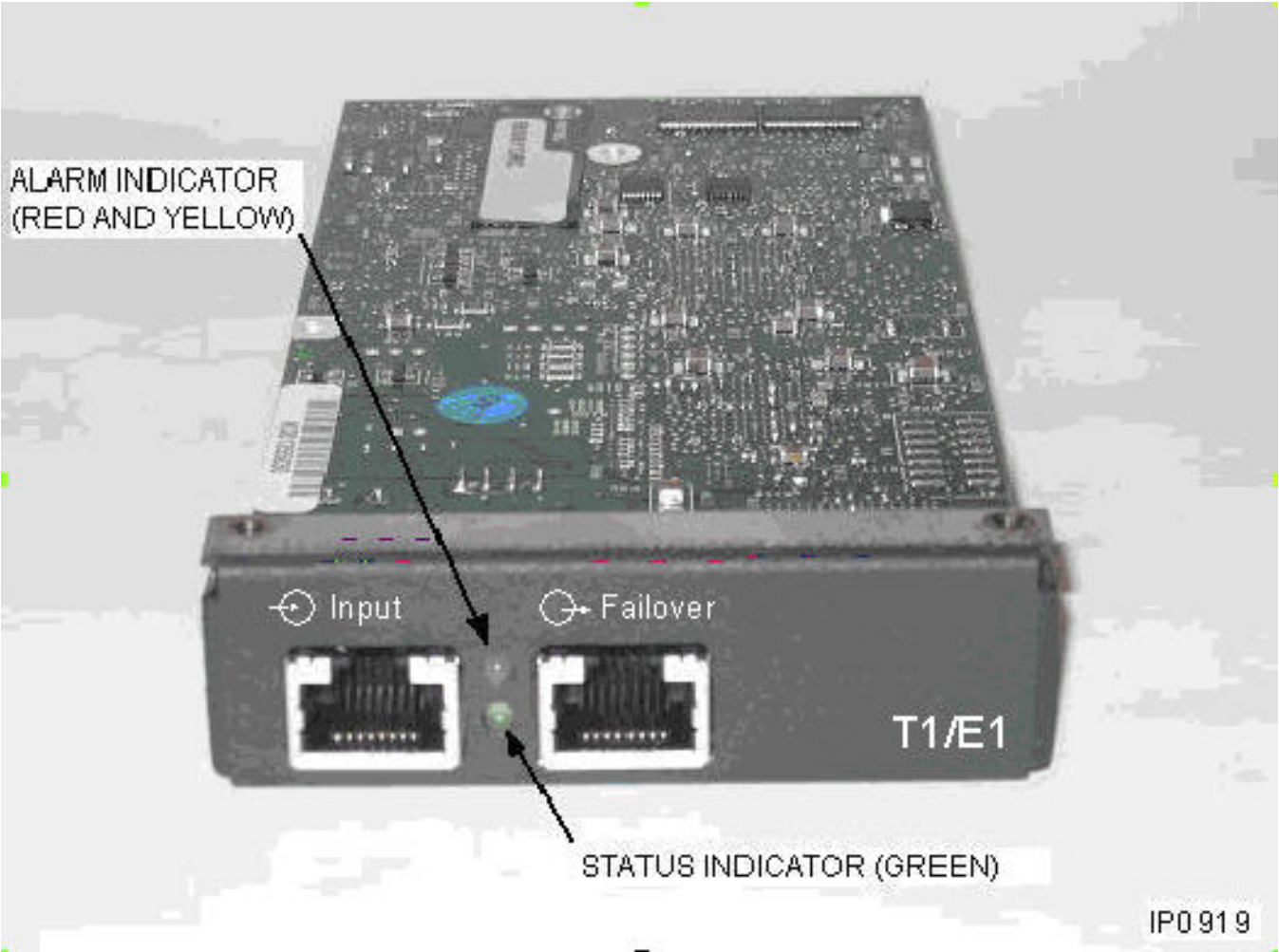


Figure 8.11: T1/E1 Combo Card - Resilient, from 3300 R7.0

Table 8.1: T1/E1 Combo Card Tip/Ring Assignments (Sheet 1 of 2)

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	--	--

Table 8.1: T1/E1 Combo Card Tip/Ring Assignments (Continued) (Sheet 2 of 2)

Pin	Signal	NT/LT Settings	
		NT (Default)	LT
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

The figure below shows the dual T1/E1 module, which provides embedded PRI and embedded T1/D4 functionality to a minimum 300 MHz controller.

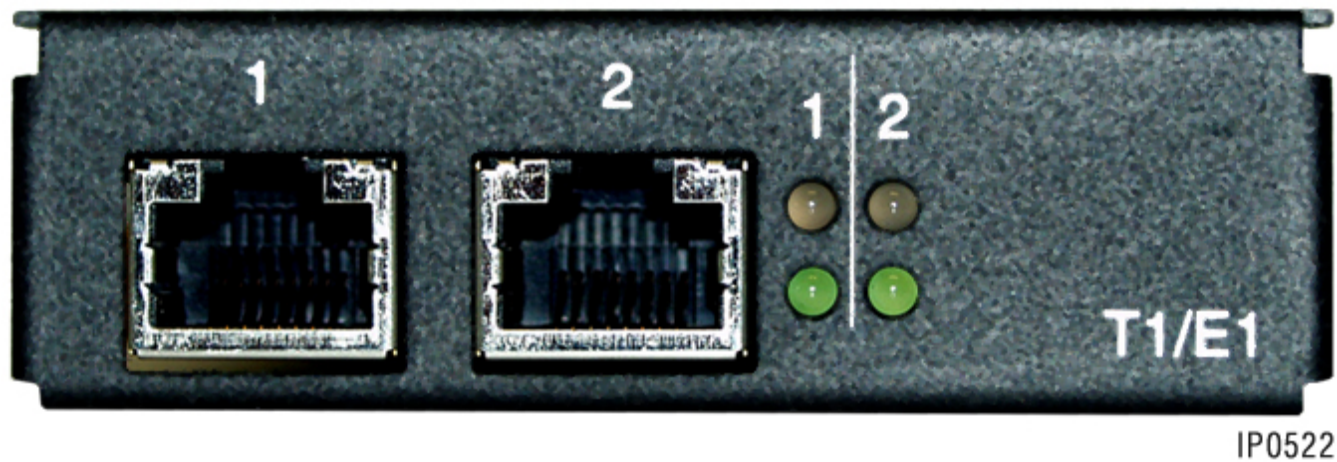


Figure 8.12: Dual T1/E1 Framer

Quad BRI Framer

The figure below shows the Quad BRI module which provides embedded BRI functionality to a minimum 300 MHz controller.

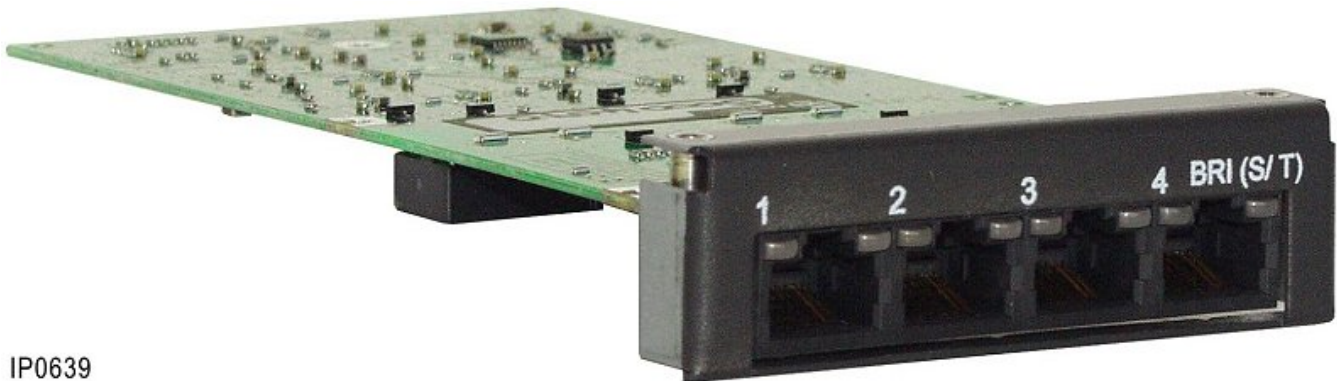


Figure 8.13: Quad BRI Framer

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.

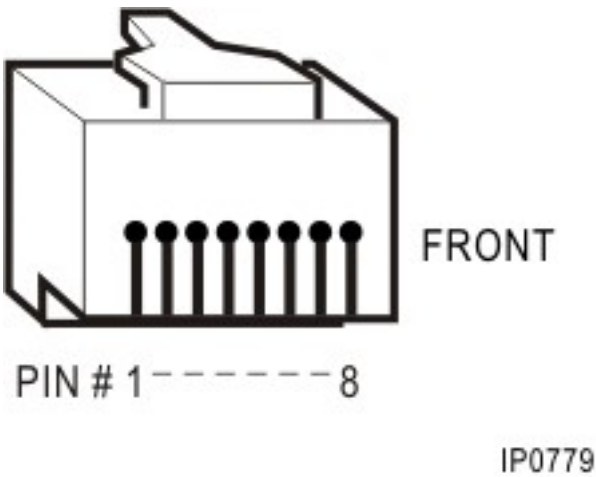


Figure 8.14: RJ-45 pin orientation

Analog Board (CX II/CXi II and MXe III/MXe III-L Controllers)

Analog Boards provide connectivity for analog trunks and telephones.

Table 8.2: Embedded Analog - Circuits/Ports

Circuits/Ports	Analog Main Board CX/CXi, CX II/CXi II and MXe III/MXe III-L	Analog Option Board CX/CXi 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	1

Table 8.3: Analog Main Board/Analog Option Board Port Assignment

Analog Option Board Ports (CX/CXi, CX II/CXi II only)											
Page	Relay	ONS Ports				LS Ports					
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/CXi, CX II/CXi II, and MXe III/MXe III-L)											
Page	Relay	ONS Ports				LS Ports					
1	1/2	4	3	2	1	1	2	3	4	5	6
n/a	(see note 2)	4114	4113	4112	4111	4115	4116	4117	4118	4119	41110
NOTE: 1. 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 2. Reserved for future development.											

Table 8.4: Analog Main Board/Analog Option Board Pinouts (Sheet 1 of 2)

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 (not used) ¹	3	RLY1_Common
	4	RLY1_NO (normally open)
	6	RLY1_NC (normally closed)
	2	RLY2_Common
	5	RLY2_NO (normally open)
	1	RLY2_NC (normally closed)
Paging	3	Paging signal

Table 8.4: Analog Main Board/Analog Option Board Pinouts (Continued) (Sheet 2 of 2)

Port	Pin Number	Function
	4	Paging signal
	6	Not used
	2	Paging relay common
	5	Paging relay NO (normally open)
	1	Paging relay NC (normally closed)
¹ Reserved for future development.		

Table 8.5: 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 3.5 mm 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.		

Line Cards (AX Controller)

The AX controller line cards are the same as those for the ASU II. See [Table 8.8](#), [Table 8.9](#), and [Table 8.11](#).

Controller Alarm Port Pinouts

TIP: The alarm port is not available on the AX, CX/CXi, and CX II/CXi II controllers.

Table 8.6: Controller Alarm Port Pinout (Sheet 1 of 2)

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

Table 8.6: Controller Alarm Port Pinout (Continued) (Sheet 2 of 2)

Pin	Signal	Pin	Signal
5	Major Alarm Return		
NOTES: <ol style="list-style-type: none"> 1. Contacts closed when alarm is present. 2. Loss of power to the controller trips (closes) the Critical Alarm relay. 			

Controller Remote Alarm Behavior

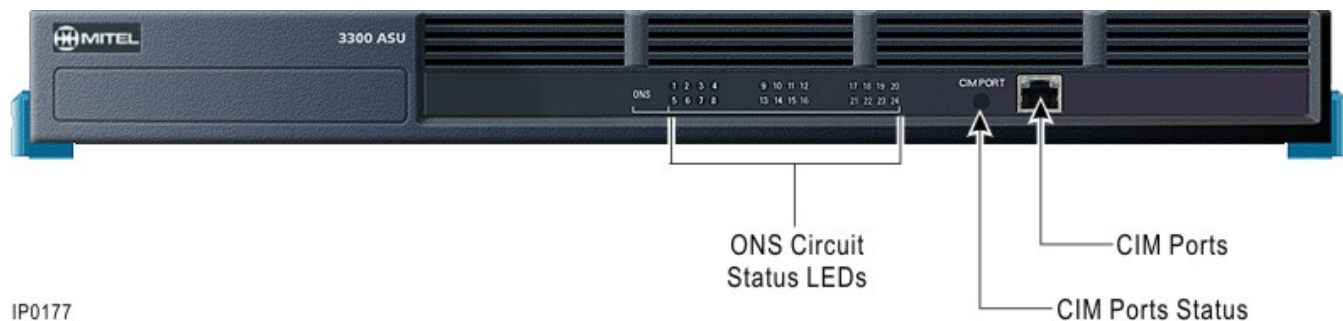
Table 8.7: Controller Remote Alarm Behavior

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 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, by default.

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 3300 R7.0 and later).



IP0177

Figure 8.15: ASU – Front Panel

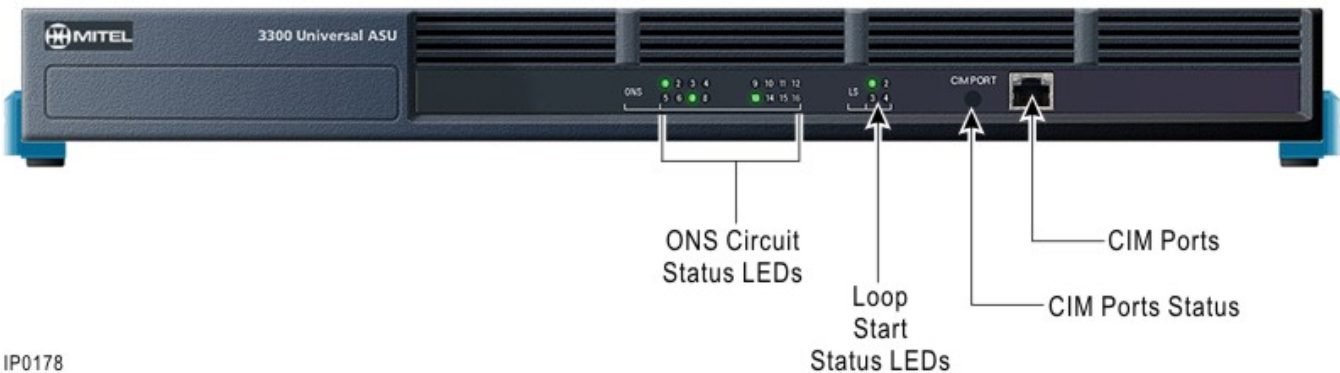


Figure 8.16: Universal ASU – Front Panel

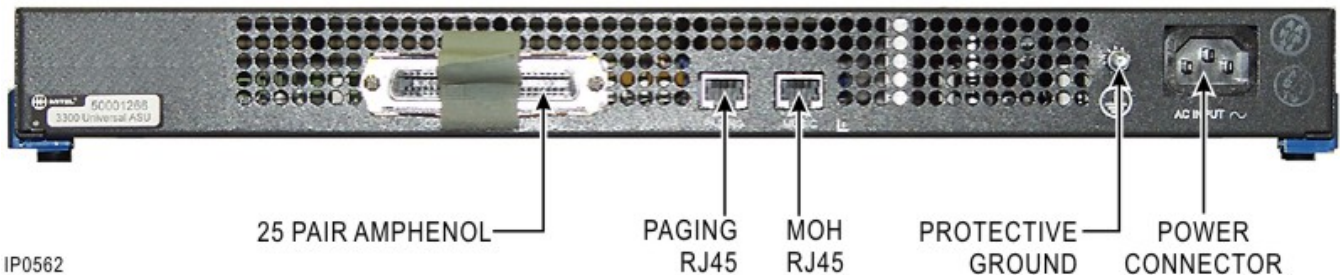


Figure 8.17: Universal ASU – Back Panel

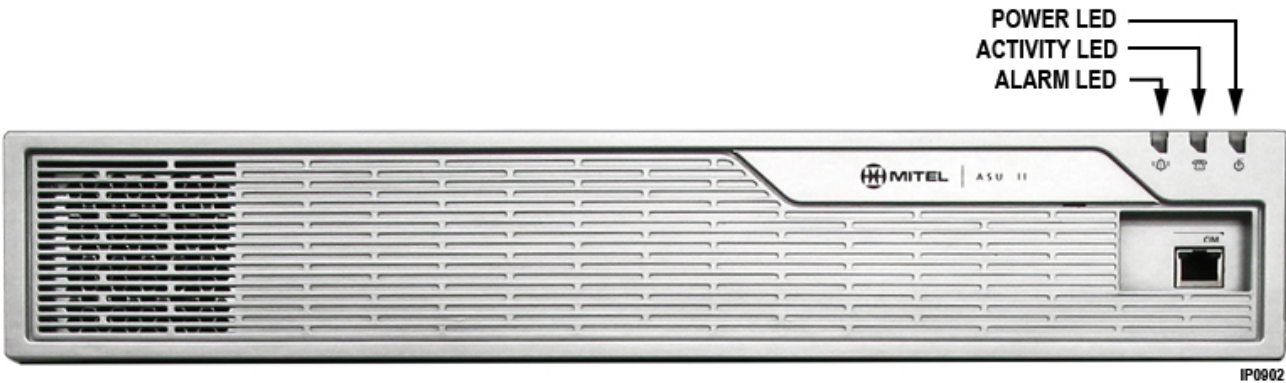


Figure 8.18: ASU II – Front Panel

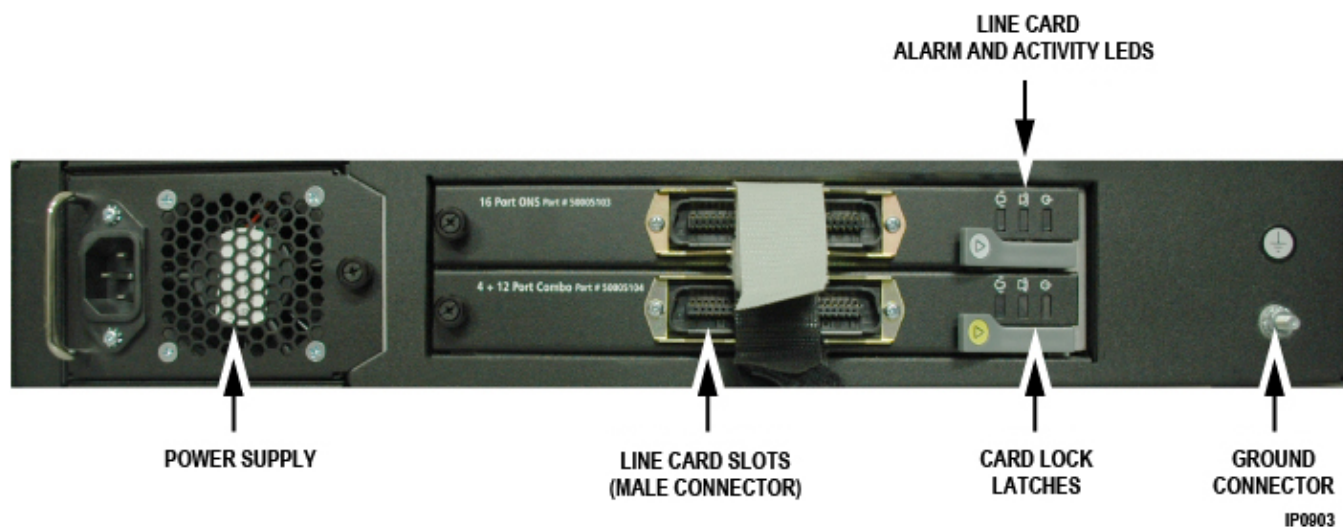


Figure 8.19: ASU II – Back Panel with a Line Card

There are three line cards available for the ASU II:

- 24 Port ONSP card
- 16 port ONSP card
- 4 + 12 port Combo card (4 LS trunks and 12 ONS lines).

Table 8.8: ASU II/AX Line Card Lock Latch Color Code

Card Type	Latch Color
24 and 16 Port ONSP Cards	White
4 + 12 Port Combo	Green

Table 8.9: ASU II/AX 25-Pair Male D-Type Connector Pinout (Sheet 1 of 3)

Pin	Color Code	16 port and 24 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

Table 8.9: ASU II/AX 25-Pair Male D-Type Connector Pinout (Continued) (Sheet 2 of 3)

Pin	Color Code	16 port and 24 port ONS	PLID	4 + 12 port Combo	PLID
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	ONS Tip/Ring 17	n 1 x 17	N/C	
43/18	Y/G, G/Y	ONS Tip/Ring 18	n 1 x 18	N/C	
44/19	Y/BR, BR/Y	ONS Tip/Ring 19	n 1 x 19	N/C	
45/20	Y/S, S/Y	ONS Tip/Ring 20	n 1 x 20	N/C	
46/21	V/BL, BL/V	ONS Tip/Ring 21	n 1 x 21	LS Ring/Tip 1	n 1 x 13
47/22	V/O, O/V	ONS Tip/Ring 22	n 1 x 22	LS Ring/Tip 2	n 1 x 14

Table 8.9: ASU II/AX 25-Pair Male D-Type Connector Pinout (Continued) (Sheet 3 of 3)

Pin	Color Code	16 port and 24 port ONS	PLID	4 + 12 port Combo	PLID
48/23	V/G, G/V	ONS Tip/Ring 23	n 1 x 23	LS Ring/Tip 3	n 1 x 15
49/24	V/BR, BR/V	ONS Tip/Ring 24	n 1 x 24	LS Ring/Tip 4	n 1 x 16
50/25	V/S, S/V			N/C	
NOTES: <ol style="list-style-type: none"> 1. 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). 2. ONS Tip/Ring 17 to ONS Tip/Ring 24 apply to 24-port ONS card only. 3. There is a limit the number of ONS ports on a single card that belong to a specific suite or ring group. When you connect ports that will be configured as part of a common suite or ring group, spread the ports across multiple cards, with a maximum of three ports on any one card. 					

Table 8.10: ASU 25-Pair D-Type Connector Pinout (Sheet 1 of 2)

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

Table 8.10: ASU 25-Pair D-Type Connector Pinout (Continued) (Sheet 2 of 2)

Pin	Color Code	ASU	PLID	Universal ASU	PLID
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.. 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 8.11: ASU II/AX 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 8.12: 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	$n\ 1\ 4\ 4$
NOTES: 1. CIM 1: $n = 2$. CIM 2: $n = 3$. 2. 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 8.13: Universal ASU Pager Connector Pinout (Sheet 1 of 2)

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	

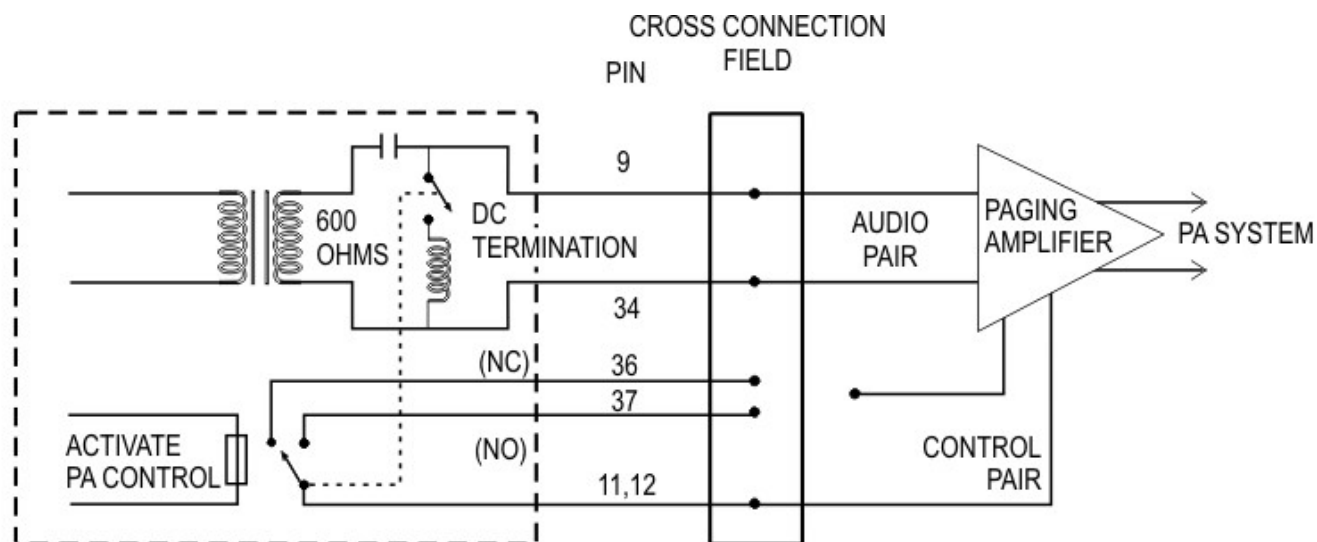
Table 8.13: Universal ASU Pager Connector Pinout (Continued) (Sheet 2 of 2)

Pin	Signal	Zone	Virtual Circuit
NOTES: <ol style="list-style-type: none"> 1. CIM 1: $n = 2$. CIM 2: $n = 3$. 2. The Paging port is a standard 8-pin modular RJ-45 connector on the rear panel. 3. 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 8.14: 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 8.20: 5485 IP Paging Unit Cross Connection

Appendix B: Installation Planner

Reserved IP Addresses

The following table identifies the IP addresses that are reserved for the Analog Main Board (AMB) and the CIMs on the ASUs and ASU IIs.

Table 9.1: Reserved IP Addresses

Prior to 3300 R7.0	3300 R7.0 and later
192.168.10.0 to 192.168.10.15	169.254.10.0 to 169.254.10.15
192.168.11.0 to 192.168.11.15	169.254.11.0 to 169.254.11.15
192.168.12.0 to 192.168.12.15	169.254.12.0 to 169.254.12.15
192.168.13.0 to 192.168.13.15	169.254.13.0 to 169.254.13.15
	169.254.14.0 to 169.254.14.15
	169.254.15.0 to 169.254.15.15
	169.254.16.0 to 169.254.16.15
	169.254.17.0 to 169.254.17.15
	169.254.18.0 to 169.254.18.15
	169.254.19.0 to 169.254.19.15
	169.254.20.0 to 169.254.20.15
	169.254.21.0 to 169.254.21.15
	169.254.22.0 to 169.254.22.15
	169.254.23.0 to 169.254.23.15
	169.254.24.0 to 169.254.24.15
	169.254.25.0 to 169.254.25.15
	169.254.26.0 to 169.254.26.15
	169.254.27.0 to 169.254.27.15
	169.254.28.0 to 169.254.28.15
	169.254.29.0 to 169.254.29.15
	169.254.30.0 to 169.254.30.15

The addresses are assigned on a first-come, first-served basis. Under normal conditions, the AMB gets the first address assigned and after that, each CIM is assigned an address as the CIM is used.

Controller Configuration Settings (RTC)

You can configure controller's (3300 ICP) settings using Server Console (see [Configure the Server using Server Console](#)).

System Administration Tool Settings

Record the following settings:

- username (default, system): _____
- password (default, password): _____

IP Phone Settings

Record the following setting codes (see System Option Assignment):

- IP set registration code
- IP set replacement code

Telephone Programming Guide

Collect the following information for programming the phones:

- User name
- Location
- Set type
- Number
- MAC Address (optional).

Table 9.2: Telephone Compression Conditions (Sheet 1 of 2)

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

Table 9.2: Telephone Compression Conditions (Continued) (Sheet 2 of 2)

Call setup conditions	G729 compression supported	Compression DSP required
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
any call to or from Nupoint IP	No	No
any call to or from Teleworker (See Note)	No	No
any call to or from Mobile Extension (ME) (See Note)	No	No
NOTE: The application server may support compression for these telephones. Refer to application documentation for more information.		

Increasing DSP Resources

You can add Dual or Quad DSP modules to

- increase the number of voice mail ports
- increase telephony resources to support more TDM devices
- add compression channels (limited applications)

You can add DSP II modules to

- add compression channels
- provide FAX Relay (T.38) support

TIP: Make sure you have the appropriate compression licenses for compression or T.38 licenses for FAX over IP support (FAX Relay) before installing DSP modules.

NOTE: Installing DSP II module(s) in an MxIII/MxIII-L controller may define one of the 192 Channel PSTN Gateway configurations that does not allow any embedded Voice Mail ports (see the table, [MxIII/MxIII-L and 192 Channel PSTN Gateway DSP Resources](#)). If this DSP II module installation is part of an upgrade to an existing system, embedded Voice Mail must be disabled (i.e., moved to another node in the network or an external server) before saving and restoring the database.

About the DSP II Module

- The DSP II is only supported in the MxIII/MxIII-L controller, AX controller, and CX II/CXi II controller.
- The DSP II supports compression (G.729a) and FAX Relay (T.38). It has replaced the existing DSP module for compression in the MxIII/MxIII-L and AX controllers. FAX Relay (T.38) is only supported by the DSP II module.
- After a DSP II module is installed in the controller, compression is not supported on any existing installed DSP modules. All compression will be supported by the DSP II module.
- T.38 licenses take precedence over compression licenses. If the combined number of licenses exceeds the DSP II card resources, the T.38 licenses will be loaded first.
- To increase the number of available T.38 channels you must reduce the number of G.729 channels.
- You can increase the number of available T.38 channels by reducing the number of G.729 channels. To obtain the first eight T.38 channels, you must reduce the number G.729 channels by 32. For each additional eight T.38 channels you must reduce the number of G.729 channels by 16.
- The MxIII/MxIII-L controller features AD21363 DSPs on the motherboard. The embedded DSP resources on the controller are sufficient to support all telephony services, conferencing, and voice mail. However, DSP II card is required for G.729a compression or FAX Relay (T.38).

The table below shows the maximum number of G.729 and T.38 channels that are available for use in a single DSP II module in the various systems. Note that the base configuration in the CX II includes the first 8 T.38 channels. A second DSP II module can be added in the MxIII/MxIII-L for more G.729 channels, but the number of T.38 channels available does not increase.

Table 9.3: DSP II Channel Capacities

System	G.729	T.38
MxIII/MxIII-L	128	0
	96	8
	80	16
AX	64	0
	32	8
	16	16
CX/CXi	64	8
CX II/CXi II	64	8

MxIII/MxIII-L Controller - DSP Resources

The following table identifies the DSP resources available for the MxIII/MxIII-L controller:

Table 9.4: MxIII/MxIII-L and 192 Channel PSTN Gateway DSP Resources (Sheet 1 of 2)

MxIII/MxIII-L Config	Maximum Resources Supported								
	Dual Framers	E2T Ports	Echo Canceled	G729a Licenses	T.38 Licenses	Max # of IP Sets in IP Page	Max # of Conferers	RFC4733 DTMF	Voice Mail
MxIII/MxIII-L Standard 1 x DSP II	2 (96 T1) (120 E1)	64	64	64	16	64 ¹	64	64	30
MxIII/MxIII-L Expanded 2 x 161 MMCs 1 x 128 VEC	3 (144 T1) (180 E1)	192	128	64	0	64 ²	64	128	30
MxIII/MxIII-L Expanded 1 x DSP II, 1 x 128 VEC	3 (144 T1) (180 E1)	192	128	128 (80)	0 (16)	64 ²	64	128	30
192 Gateway 3 1 x DSP II, 2 x 128 VEC	3 (144 T1) (180 E1)	192	192	128 (80)	0 (16)	64	64	192	30
192 Gateway 3,4 2 x DSP II, 1 x 128 VEC	3 (144 T1) (180 E1)	192	192	192	16	64	64	192	0
192 Gateway 3 1 x DSP II, 1 x 128 VEC	2 (96 T1) (120 E1) + 2 FIM	192	128	128	16	64	64	192	30
192 Gateway 3,4 1 x DSP II, 1 x 128 VEC	4 (192 T1)	192	192	128 (80)	0 (16)	64	64	192	0

Table 9.4: MxIII/MxIII-L and 192 Channel PSTN Gateway DSP Resources (Continued) (Sheet 2 of 2)

MxIII/MxIII-L Config	Maximum Resources Supported								
	Dual Framers	E2T Ports	Echo Canceled	G729a Licenses	T.38 Licenses	Max # of IP Sets in IP Page	Max # of Conferers	RFC4733 DTMF	Voice Mail
NOTE: <ol style="list-style-type: none"> All 3300 systems can support a maximum of 64 members in a group page. However, the MxIII/MxIII-L Standard with 64 E2T channels should restrict the number of members in a group page to less than 32 to reduce the risk of conflict with trunk E2T channels. In these configurations there are always more E2T sessions available than can be used by the T1/E1 trunks, and the full balance of 64 can be used in a group page with no restrictions. The 192 Gateway is not defined in any software setup procedures, but is a special case of the resource allocations based on the specific hardware modules installed. When the system boots up, if it detects either of the following hardware configurations, the number of voice mail ports will be automatically reset to zero: <ul style="list-style-type: none"> two DSP II modules and one VEC module, or one DSP II module and four dual T1/E1 framers The MxIII can be configured as a 192 channel TDM gateway, as shown in this table. The maximum of 192 E2T channels is available only when used with 53xx phones using Mitel proprietary encryption, or with 53xx, 69xx and SIP phones using no encryption. The maximum capacity of the E2T card is reduced to 123 channels when all the concurrent calls are G711 with SRTP and to 185 channels when all the concurrent calls are G.729 with SRTP. 									

CX II/CXI II Configurations - DSP Resources

The following tables list the DSP resources available on the CXi II with and without a DSP II module installed.

Table 9.5: CX II/CXi II DSP Configurations without DSP II (Sheet 1 of 2)

Configuration	# of DSPs	Echo Canceled	G729	Conf	E2T	T.38	DTMF Receivers	Voice Mail
Base System	2	32	0	10X3	64	0	64+	16
Base + one T1/E1 Combo	3	64	0	10X3	64	0	64+	16
Base + two T1/E1 Combo	4	96	0	10X3	64	0	64+	16

Table 9.5: CX II/CXi II DSP Configurations without DSP II (Continued) (Sheet 2 of 2)

Configuration	# of DSPs	Echo Cancellor	G729	Conf	E2T	T.38	DTMF Receivers	Voice Mail
NOTE: The number of voice mail and conference channels is fixed at 16 and 30 respectively.								

Table 9.6: CX II/CXi II DSP Configurations with DSP II

Configuration	# of DSPs	Echo Cancellor	G729	Conf	E2T	T.38	V21	DTMF Receivers	Voice Mail
Base + DSP II	8	32	64	10X3	64	8	64	64+	16
Base + oneT1/E1 Combo+ DSP II	9	64	64	10X3	64	8	64	64+	16
Base + twoT1/E1 Combo+ DSP II	10	96	64	10X3	64	8	64	64+	16
NOTE: Compression and T.38 are licensable options and are determined by the number of licenses purchased.									

DSP Notes

Voice Mail

- Program the additional voice mail ports, then add the DSP MMCs if necessary (for the AX and MXe III/MXe III-L, you need to add DSP resources only if you need compression or FAX Relay (T.38)).
- When you increase the number of ports you may also have to add DSPs to handle the increased demand for voice compression (G729).

Compression

- You must purchase compression licenses before adding DSP modules for compression.
- Upgrading to 64 compression channels requires a minimum 300 MHz controller.

Telecom

If the system needs compression channels and/or 30 voice mail ports and/or increased telephony resources to support more TDM devices, then additional DSPs may be necessary (see [Appendix E: FRU Part Numbers](#) for the part numbers of the DSP modules). To determine the number of DSP modules required in a system, refer to the table above.

- MXe III/MXe III-L and AX controllers ship with embedded DSP sufficient to support a 400-user system
- CX II/CXi II (IP plus analog) controllers ship with a Dual Embedded DSP on the main board. The T1/E1 Combo also includes DSP resources.

NOTE: 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.

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 controllers

- [Configuration 1: One DHCP Server per VLAN](#)
- [Configuration 2: One DHCP Server for two VLANs](#)
- [Configuration 3: Router on a Stick](#) (one router interface to multiple VLANs).

NOTE: [CXi/CXi II/MXe III Server Configuration](#) for CXi/CXi II-specific configuration examples.

NOTE: [AX Configuration Procedures](#) illustrates the two most common AX system configurations.

DHCP Server Settings

DHCP Server Settings

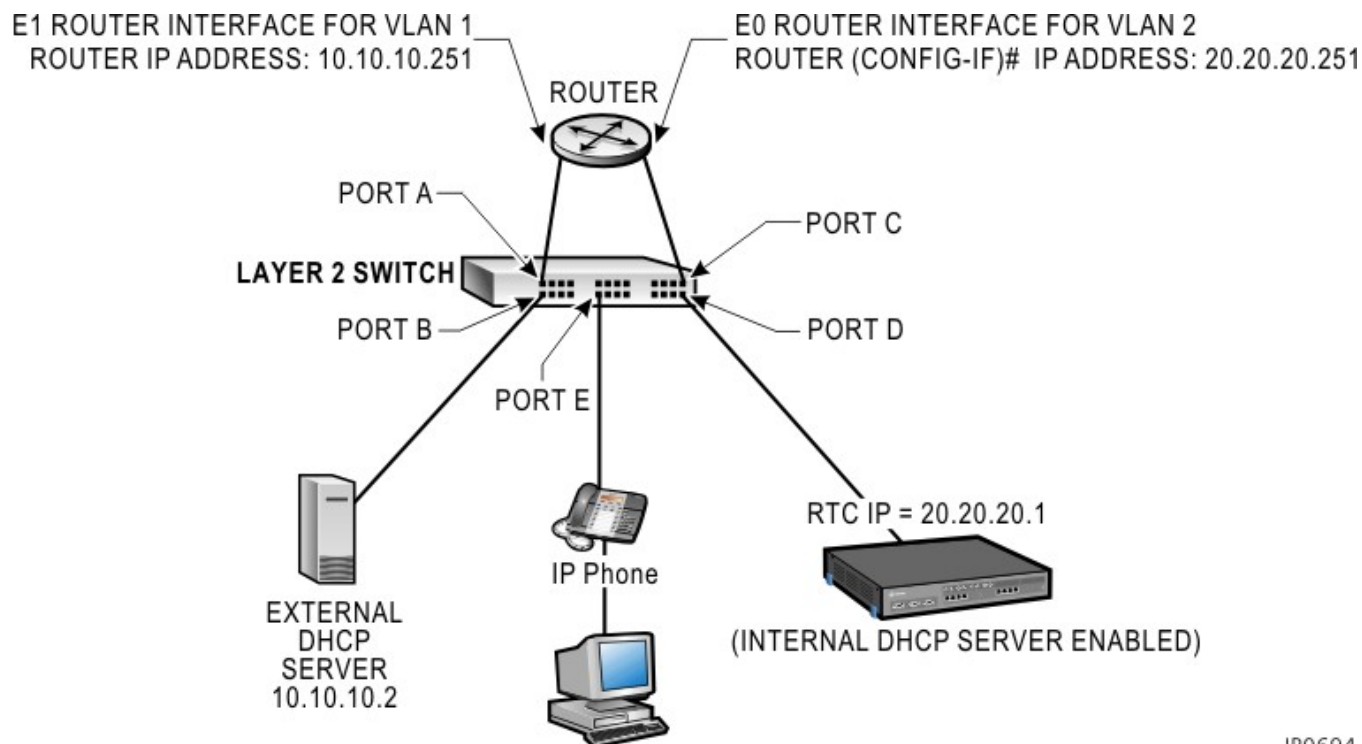
The following settings must be programmed in the DHCP server for each of the configurations shown in this chapter:

- | | |
|---|---------------------------------------|
| • DHCP IP Address Range | • Option 128 (TFTP Server IP Address) |
| • Subnet Mask | • Option 129 (RTC IP Address) |
| • Option 03 (Router) | • Option 130 (MITEL IP PHONE) |
| • Option 125 or 43 (Mitel configuration string) | • Option 132 (VLAN ID) |
| | • Option 133 (Priority) |

NOTE: Option 125 (preferred) or Option 43 should be used for 3300 R7.0. Options 128-133 may be required for backward compatibility during upgrades. For earlier releases, use options 128-133.

TIP: See [Configuring a Windows 2019 DHCP Server \(3300 R7.0 and later\)](#) for information on programming 3300 DHCP settings on a Windows 2000 DHCP server.

Configuration 1: One DHCP Server per VLAN



IP0694

The following table shows the DHCP settings programmed for this configuration.

Table 10.1: DHCP Settings Example - Configuration 1 (Sheet 1 of 2)

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 (3300 R7.0>)	id:ipphone.mitel.com;sw_tftp=20.20.20.1;call_srv=20.20.20.1;vlan=2;l2p= 6;dscp=46;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	—

Table 10.1: DHCP Settings Example - Configuration 1 (Continued) (Sheet 2 of 2)

Setting	DHCP Server on VLAN 1 (IP: 10.10.10.2) Scope 1	Internal DHCP Server on Controller Scope 1
* Required on 3300 R7.0 systems to allow IP sets to upgrade to firmware that supports options 125 and 43.		

Layer 2 Switch Settings (Example)

[Table 10.2](#) and [Table 10.3](#) show examples of settings on a Cisco and an HP Layer 2 switch for this example. See for the port numbers.

TIP: These settings also apply for the other network configuration examples.

Table 10.2: Cisco Layer 2 Switch Settings Example - Configurations 1, 2 and 3

Port	Use	Command
A	Access port for VLAN 1	None (by default, all ports belong to VLAN 1)
B		
C	Access port for VLAN 2	Router(config-if)#switchport mode access Router(config-if)#switchport access VLAN 2
D		
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 10.3: HP Layer 2 Switch Settings Example - Configurations 1, 2 and 3

Port	Use	Command (on HP VLAN menu)
A	Access port for VLAN 1	VLAN 1 = untagged VLAN 2 = NO
B		
C	Access port for VLAN 2	VLAN 1 = NO VLAN 2 = untagged
D		
E	Trunk port	VLAN 1 = untagged VLAN 2 = tagged

NOTE: For additional switch setting examples, refer to the Network Configuration Specifics chapter in the *MiVoice Business Engineering Guidelines*.

Configuration 2: One DHCP Server for Two VLANs

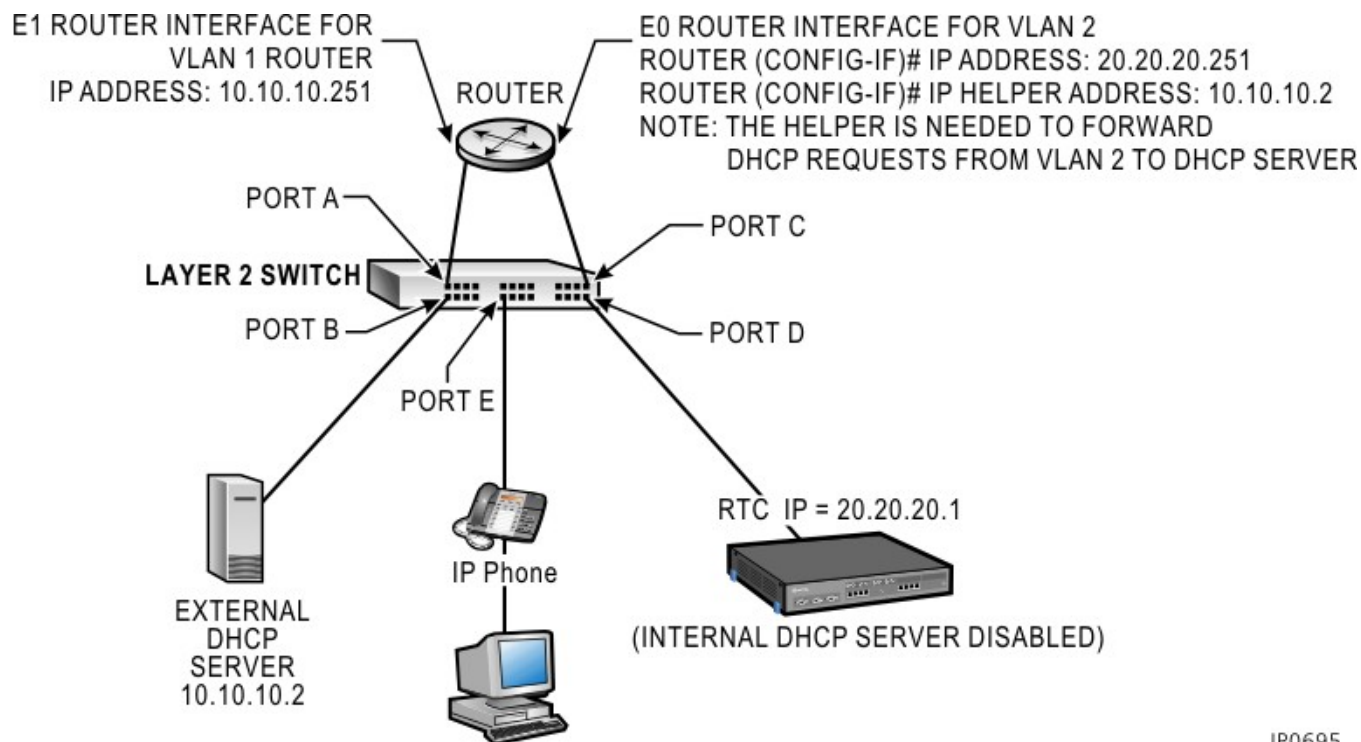


Figure 10.1: One DHCP Server for two VLANs - Example

The following table shows the DHCP settings programmed for this configuration.

Table 10.4: DHCP Settings Example - Configurations 2 and 3 (Sheet 1 of 2)

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 (3300 R7.0>)	id:ipphone.mitel.com;sw_tftp=20.20.20.1;call_srv=20.20.20.1;vlan=2;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

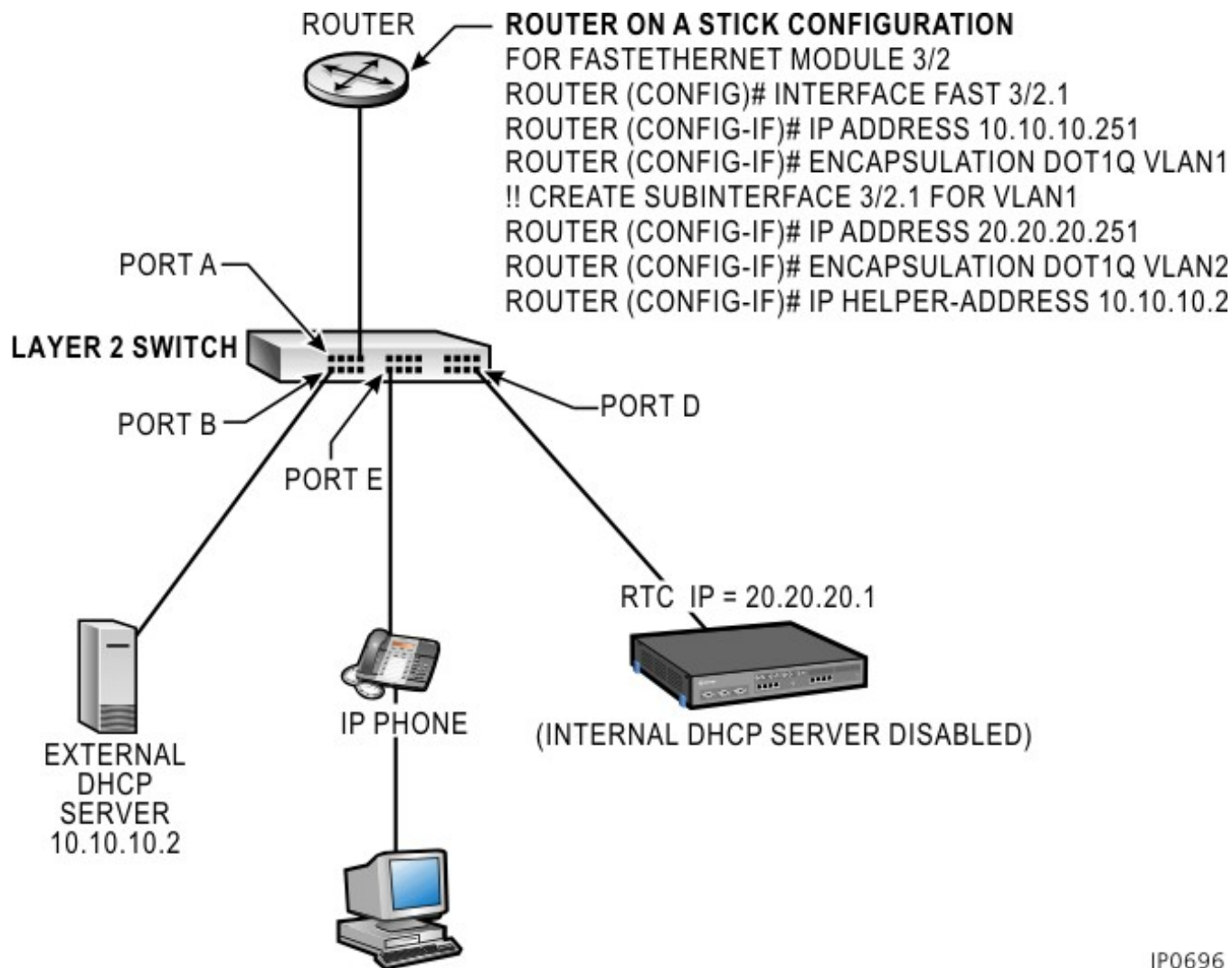
Table 10.4:DHCP Settings Example - Configurations 2 and 3 (Continued) (Sheet 2 of 2)

Setting	DHCP Server on VLAN 1 (IP: 10.10.10.2)	
	Scope 1	Scope 2
* Required on 3300 R7.0 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 \(Example\)](#).

Configuration 3: Router on a Stick

**Figure 10.2:** Configuration 3 Example

[Table 10.4](#) shows the DHCP settings for this configuration.

Layer 2 Switch Settings (Example)

See [Layer 2 Switch Settings \(Example\)](#).

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 *MiVoice Business Engineering Guidelines* for details.

Cisco Discovery Protocol (CDP)

Prior to 3300 R5.1 the Mitel IP devices discovered VLAN information dynamically through DHCP. With R5.1, 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 *MiVoice Business Engineering Guidelines*, available in the [Document Center](#).

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/CXi II/MXe III Server Configuration

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 10.5:Port Forward Table (CXi II/MXe III 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 10.6:PPTP (CXi II/MXe III only)

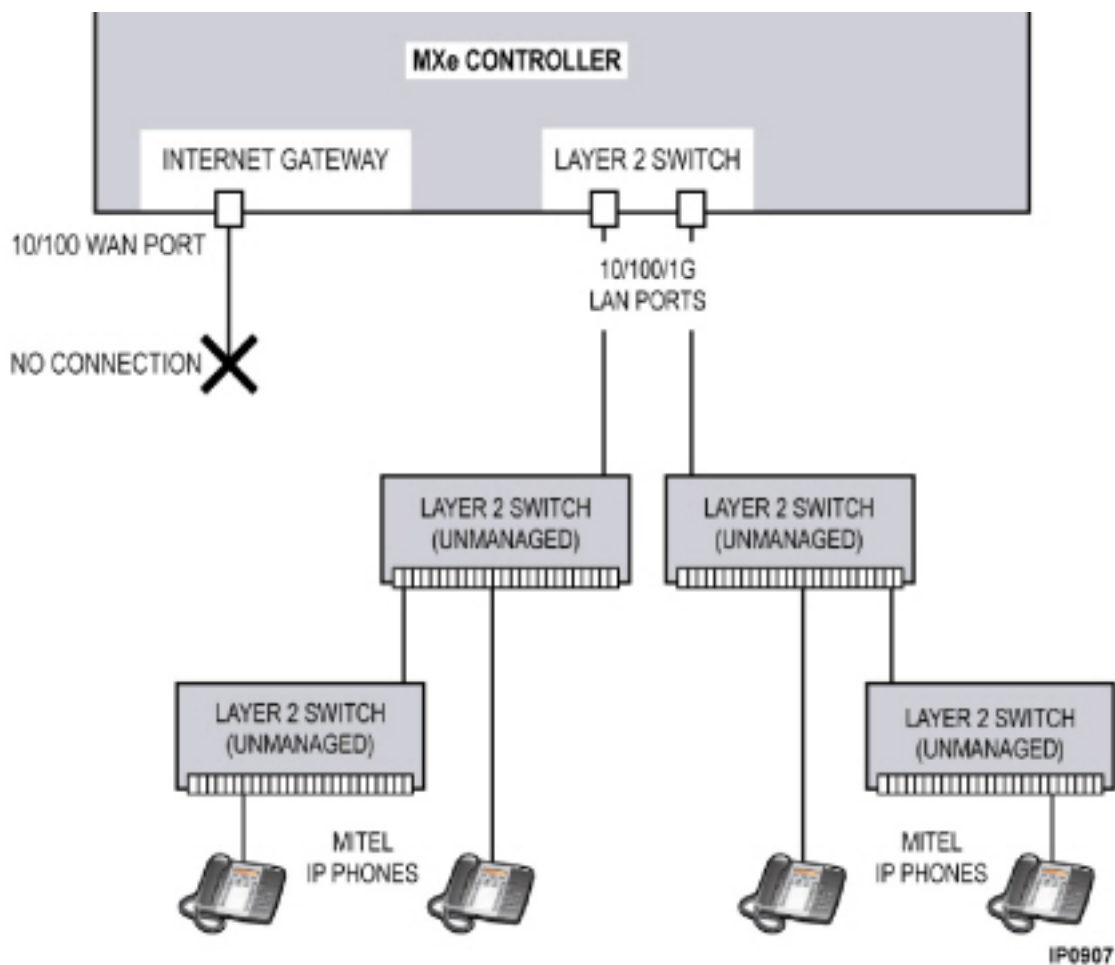
Parameter	Function/Values
User Name	The user name that the server uses to authenticate the remote client.
Password	Password that the server uses to authenticate the remote client.
Client IP Address	Address that the remote PPTP client uses on the LAN.
PPTP Access	Set to “Enable” to enable PPTP remote 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 chapters in the *MiVoice Business Engineering Guidelines*.

Configuration B: MXe III/MXe III-L Typical Voice-Only Network**Figure 10.3:** MXe III/MXe III-L Voice-Only Configuration Example

NOTE: For the MXe III-L controller, only L2 Port 1 can be used.

IP Address	192.168.1.2
Subnet	255.255.255.0
Gateway	192.168.1.1
Layer 2 (excludes MXe III-L)	192.168.1.3

AX Configuration Procedures

AX Typical Voice-Only Network

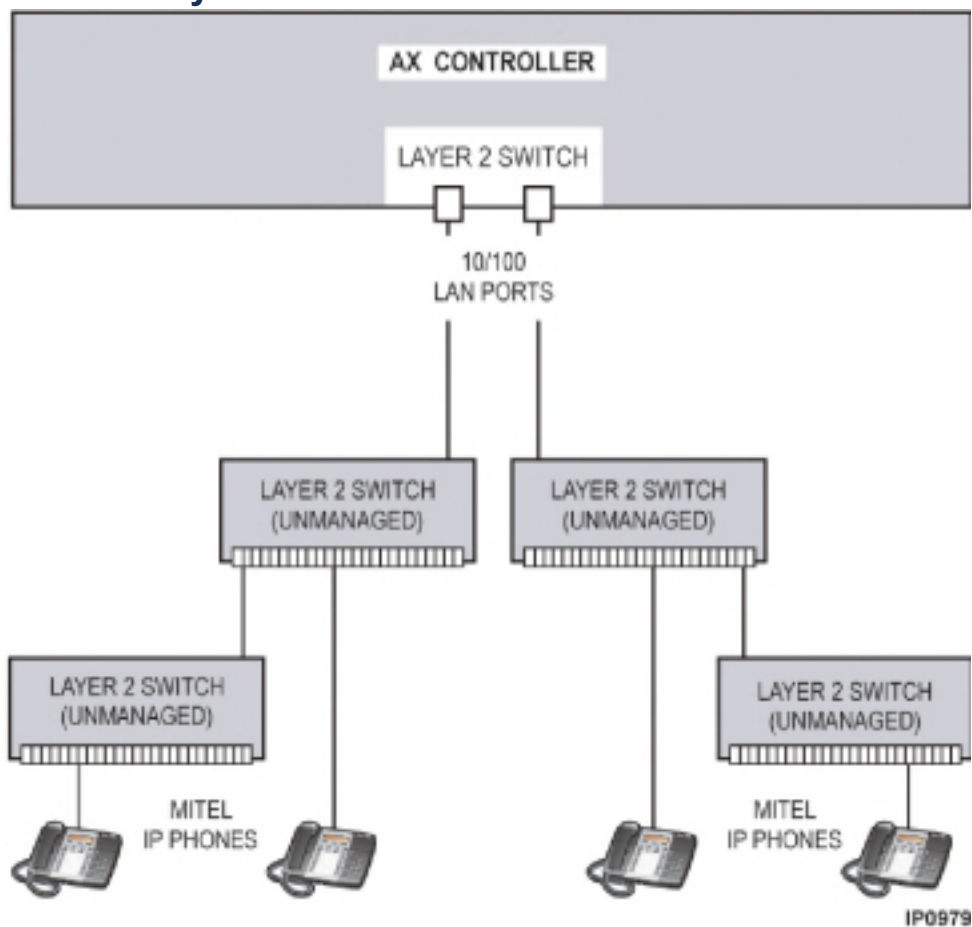


Figure 10.4: AX Voice-Only Configuration Example

IP Address	192.168.1.2
Subnet	255.255.255.0
Gateway	192.168.1.1

AX Typical Voice and Data Network

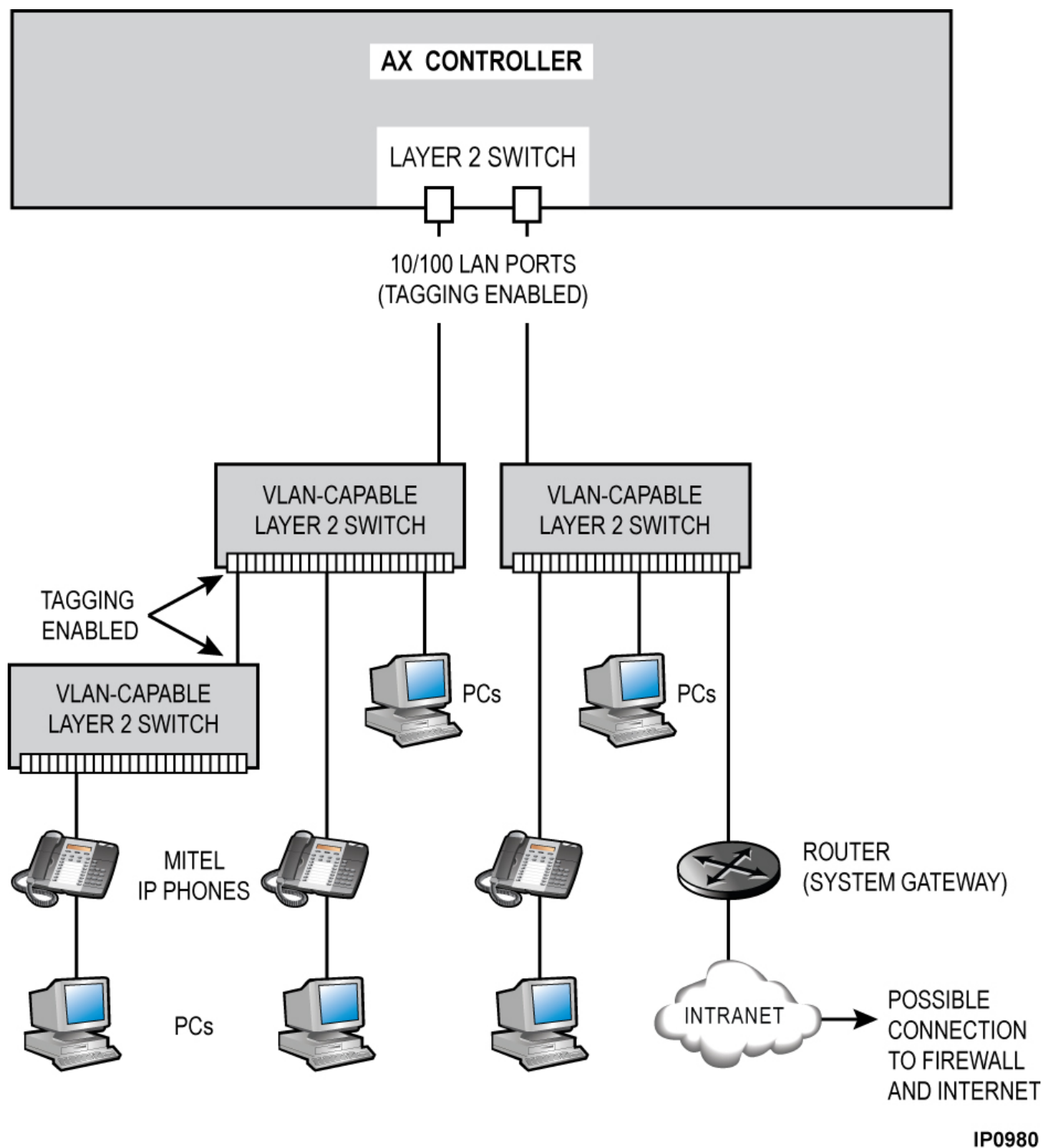


Figure 10.5: AX Voice and Data Configuration Example

IP Address	192.168.1.2
------------	-------------

Subnet	255.255.255.0
Gateway (Router)	192.168.1.1

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.

CXi II, MxIII/MxIII-L and AX-Specific Guidelines

This section describes VLAN behavior, and the different types of network configurations: voice-only, voice and data, and the programming and configuration requirements for CXi II, MxIII/MxIII-L and AX.

The CXi II, MxIII and AX controllers each include an internal L2 switch that is VLAN-capable. These controllers need to be treated as an integral part of the L2 networking infrastructure.

CXi II, MxIII/MxIII-L and AX VLAN Behavior

NOTE: For quick installation, the CXi II, MxIII/MxIII-L and AX can be installed using only the default VLAN (VLAN 1). VLAN1 carries both voice and data. If desired, the Administrator can program additional VLANs at a later date.

Default VLAN1

When the CXi II/MxIII/MxIII-L/AX is on the default VLAN, it accepts untagged frames and tagged VLAN 1 frames. Any non-VLAN 1 tagged frames are dropped. The CXi II/MxIII/MxIII-L/AX treats untagged frames as VLAN 1 frames. The CXi II/MxIII/MxIII-L/AX prioritizes traffic based on the priority tag.

When the CXi II/MxIII/MxIII-L/AX is programmed with a Voice VLAN, the switch will allow untagged frames and tagged VLAN 1 frames as well as Voice VLAN frames. All other VLAN tagged frames will be dropped. The priority of tagged frames are preserved and queued accordingly. On egress, Voice VLAN traffic is either tagged on all ports (prior to 3300 R9.0) or configured as tagged or untagged on a port-by-port basis (R9.0 and later). Untagged frames are treated as VLAN 1 and forwarded to an external layer 2 switch.

Voice VLAN

When the CXi II/MxIII/MxIII-L/AX is programmed with a Voice VLAN, the switch will allow untagged frames and tagged VLAN 1 frames as well as Voice VLAN frames. All other VLAN tagged frames will be dropped. The priority of tagged frames are preserved and queued accordingly. On egress, Voice VLAN traffic is either tagged on all ports (prior to 3300 R9.0) or configured as tagged or untagged on a port-by-port basis (R9.0 and later). Untagged frames are treated as VLAN 1 and forwarded to an external layer 2 switch.

CXi II: When the phones are on the Layer 2 switch of the CXi II, the phones and the CXi II switch must be on the same the Voice VLAN for the phones to communicate with call control.

Data VLAN (CXi II)

The CXi II switch can be assigned a data VLAN to override the default VLAN 1. By default, all ports on the CXi II switch belong to VLAN 1.

In addition, VLAN membership can be assigned on a per port basis. Each port can be assigned as tagged or untagged on the data VLAN as well as the Voice VLAN. The default is tagged.

VLAN Routing

The installation remains the same as the CX II, MX, and LX because the CXi II, MXe III/MXe III-L and AX rely on external routers to perform VLAN routing.

An externally managed L2 switch connected to the AX/CXi II/MXe III/MXe III-L uplink port(s) must tag Voice VLAN traffic unlike the setup for the other controllers that do not have this requirement.

Figure 10.6 illustrates VLAN behavior by showing the CXi II integrated into a network carrying both voice and data.

In the figure, VLAN 1 is used for non-voice traffic and the Voice VLAN is used for voice traffic. A VLAN-capable, managed L2 switch is connected to the CXi II Gigabit Ethernet Uplink port for expansion purposes. An external DHCP server is set up to serve VLAN 1 and the CXi II internal DHCP server is used to serve the Voice VLAN. *Figure 10.6* shows the usage of VLANs on the various network segments.

NOTE: You can configure the CXi II/MXe III/MXe III-L/AX internal DHCP server to provide DHCP services to both VLAN 1 and the Voice VLAN. In this case, an external DHCP server would not be required, but the external router in the corporate network would need to be configured to support routing from VLAN 1 to the Voice VLAN and DHCP forwarding would have to be enabled on the router.

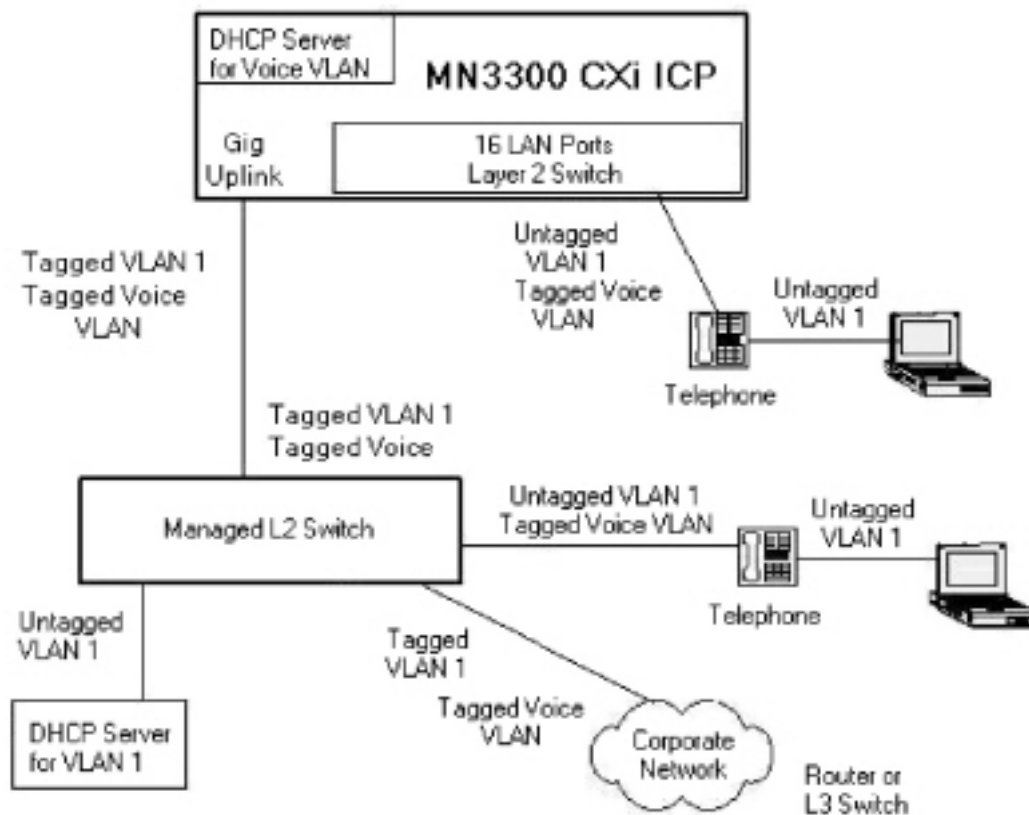


Figure 10.6: CXi II VLAN Behavior

NOTE: The default VLAN may not be 1, but it is untagged.

Implementing a Voice-Only Network

In a voice-only network, IP telephony devices are the only devices connected to the controller's network interfaces.



Figure 10.7: CXi II-based Typical Voice-Only Network

MxIII/AX/CXi II IP Settings

No changes to the controller's default IP settings are required for a voice-only network:

- CXi II - plug up to 16 IP phones into the internal Layer 2 switch ports (marked 10/100 802.3af) and plug up to 84 phones into the external L2 switches for a total of up to 100 IP phones.
- AX - connect up to 100 IP phones to the two 10/100 Mbps Ethernet ports.
- Base MxIII /MxIII-L- connect up to 350 IP phones to external switches. For MxIII, split phones between the two 10/100/1G LAN ports.



Figure 10.8: MxIII based Typical Voice-Only Network

Implementing a Voice and Data Network

Using a CXi II ICP

A voice and data network uses the CXi II controller's network interfaces to provide services for IP phones and PCs plus a firewall-protected connection to the Internet.

The 10/100/1G LAN port in the illustration is connected to a pair of Layer 2 switches. These two 24-port switches, daisy-chained together, provide an additional 48 ports. A single 48-port switch could also be used. Note that the maximum number of IP phones supported is 150 on the CXi II.

PCs are shown connected to the network in two ways: directly to the Layer 2 switch and indirectly through a dual-port IP Phone.

CAUTION: To ensure optimum network performance, DO NOT connect servers to the 2nd port on IP phones.

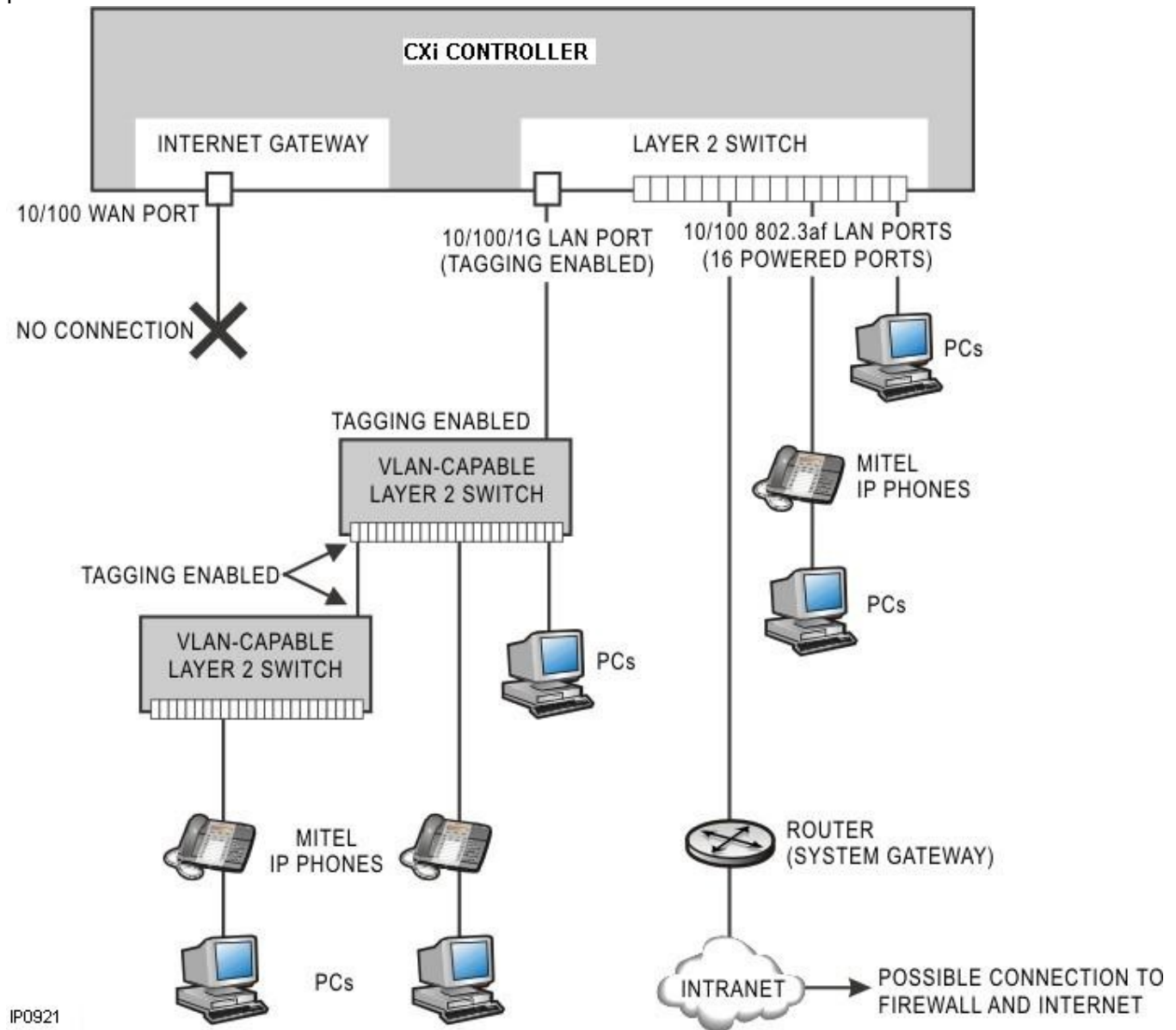
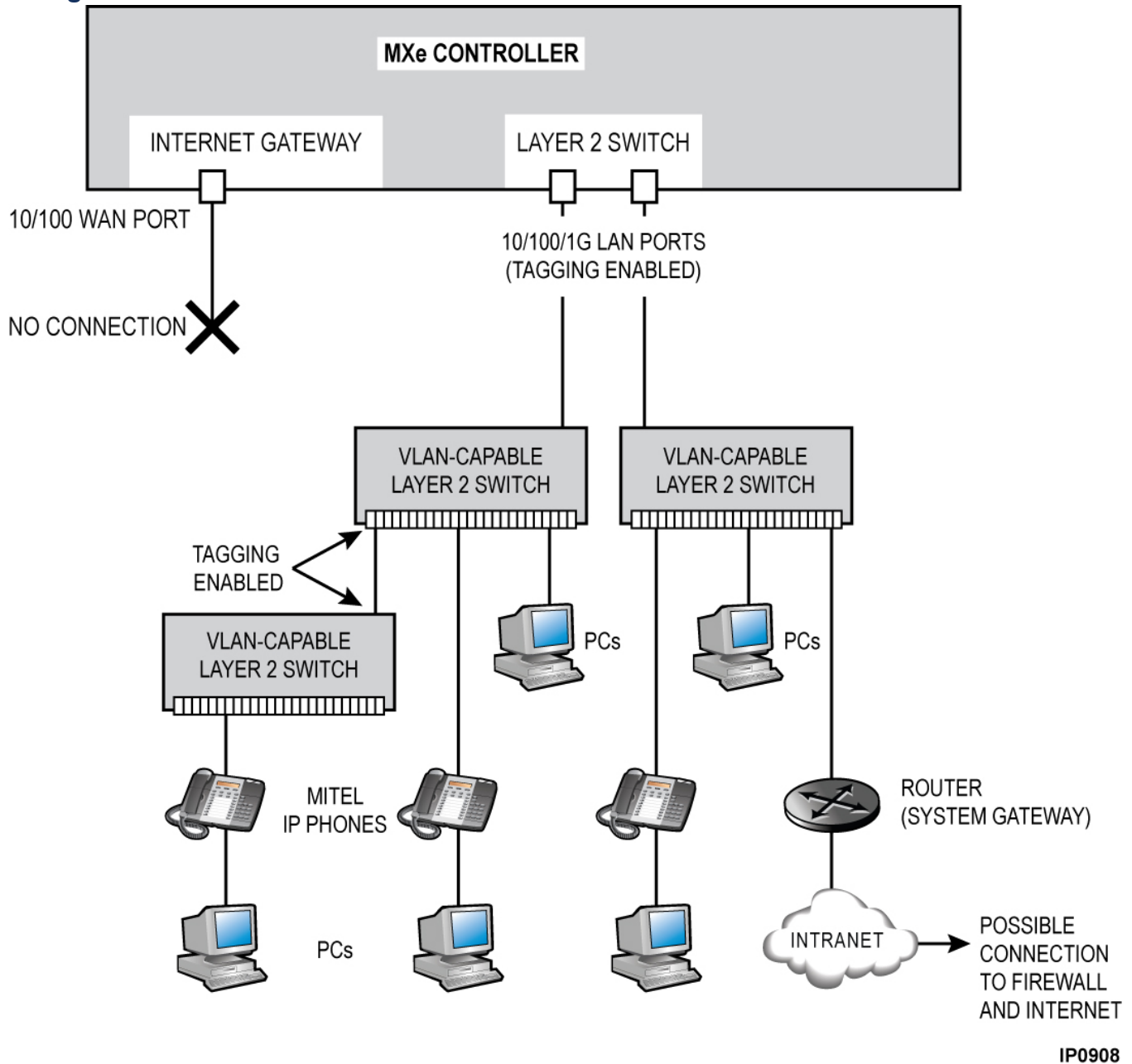


Figure 10.9: CXi II-based Typical Voice and Data Network

Using an MxIII or AX ICP

**Figure 10.10:** MxIII-based Typical Voice and Data Network

NOTE: The AX controller does not have a built in Internet Gateway like the MxIII does. Thus, the Internet Gateway features supported on the MxIII, such as firewall, NAT, and remote routing are not available on the AX.

Programming of VLANs on the AX differs from the CXi II and the MxIII. On the AX, the 4 least significant bits must be unique for all VLANs.

This means that if VLAN 1 is already in use for the default data VLAN, then the voice VLAN cannot be VLAN 1, 17, 33, 49 or so on. If you try to program a non-valid VLAN, System Administration Tool displays a warning.

In the case where VLAN 1 is used for the data VLAN, the allowable VLAN values for voice exclude numbers where the least significant 4 bits are the same as VLAN 1. These values are $1 + n * 16$, where n is 1 to 255.

DHCP Server: The default address information and options may need to be changed when installing the controller on a network with multiple subnets. If you are using an external DHCP server, disable the one in the controller. For programming instructions, refer to the System Administration Tool Help.

CXi II and MxIII Configuration Requirements

Controller

- Internet Gateway (WAN port)
 - Use of the Internet Gateway is optional, but if you wish to use the Internet Gateway, you must specify the address assignment (PPPoE, DHCP client, static or Applications Processor Card), and program the firewall.
- Layer 2 switch
 - Depending on which IP addresses are already used in the network, you may have to change IP addresses to prevent IP conflicts. IP address changes may also be required to allow for traffic between the local and remote subnets, and to ensure quality of service for phone calls with VLAN prioritization.
- DHCP Server
 - The default address information and options may need to be changed when installing the controller on a network with multiple subnets. If you are using an external DHCP server, disable the one in the controller.

NOTE: For programming instructions, refer to the *System Administration Tool Help*.

Other network devices

- External Layer 2 Switches
 - If a VLAN-capable switch is connected to the 10/100/1G port on the MxIII, program its uplink port to send and receive tagged packets on the default VLAN (1), and make sure that it treats packets with priority 6 as the highest priority. If another VLAN-capable switch is connected to the first, program it with the same settings.
 - On the CXi II, enable VLAN tagging on the 10/100/1G (port 17).
 - On the MxIII enable VLAN tagging on both of the 10/100/1G ports.

VLAN tagging is accomplished with the same setting in the System Administration Tool Layer 2 (L2) Switch form, “Tag VLAN 1 on Trunk Ports”. This setup allows the VLAN-capable switches to provide the same VLAN prioritization services as the internal Layer 2 switch on the CXi II, the MxIII and the AX.

- Router
 - If a router is connected to the local internal network, designate it as the default gateway to the other networks. Program its IP address as the System Gateway IP on the CXi II and MxIII. If an external router is present on the LAN, disable the Router Discovery Protocol on the CXi II and MxIII.

Installing External Layer 2 Switches

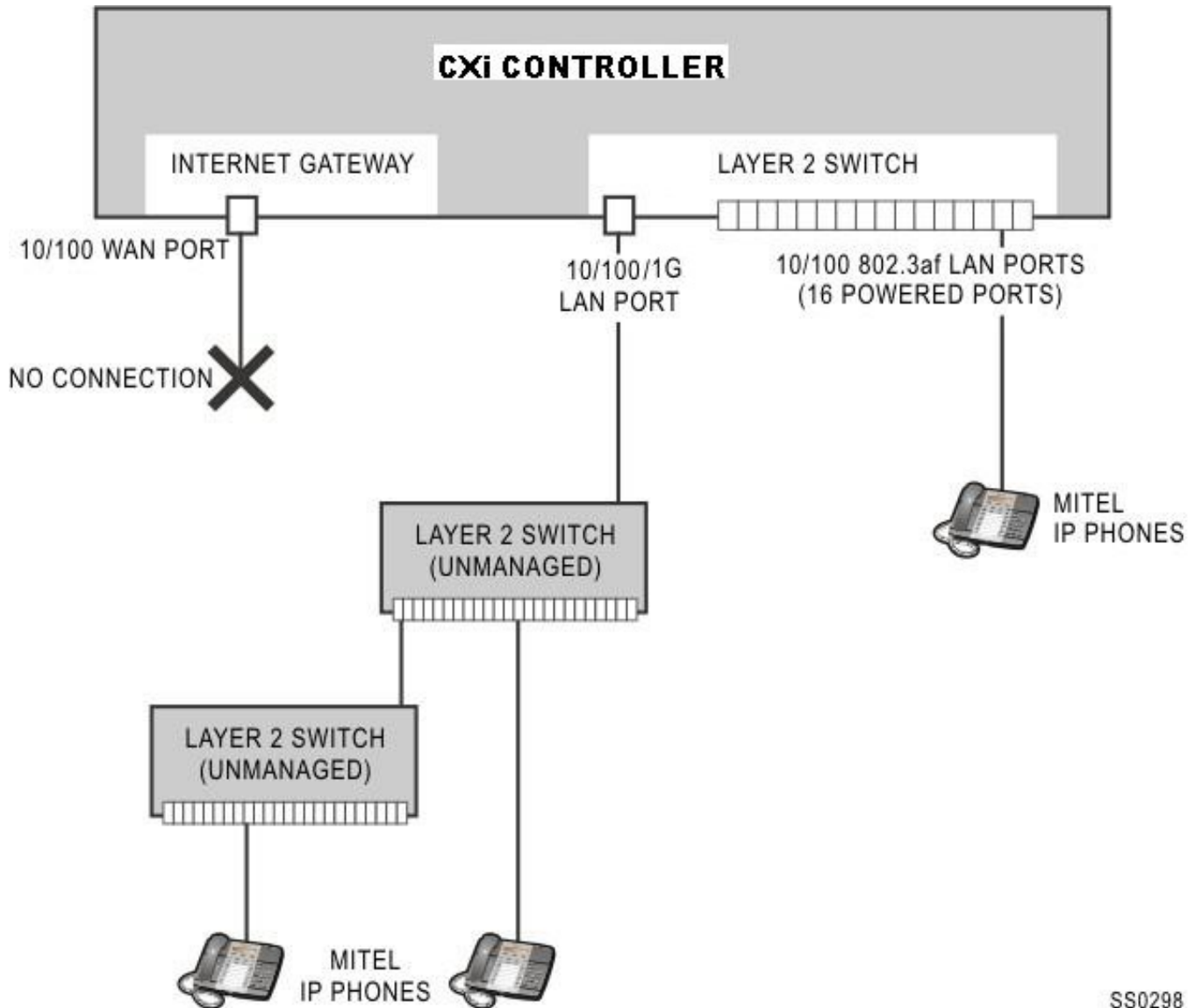
Voice Only Networks

The CXi II provides 16 integrated Ethernet ports that can support up to 16 IP phones.

As a minimum, the L2 switches should support 10/100 BaseT. Because some programming may be necessary (e.g. port speeds), the L2 switches require a management interface.

Guidelines:

- When installing the CXi II, connect a single expansion Layer 2 switch to the 10/100/1G LAN port only. If using two 24-port switches, connect the second switch to the first in a daisy chain. Do not connect expansion switches to the 10/100 802.3af LAN ports on the CXi II.
- Mitel telephones require power, which they can receive from an adapter or power brick, or from a powered Ethernet connection. The 10/100 802.3af LAN ports of the CXi II provide Power over Ethernet (PoE), as do some expansion switches. The 10/ 100/1G LAN port on the CXi II does not provide PoE.
- The MXe III and AX do not support PoE. The phones need to be powered from an adapter or power brick, or from a powered Ethernet connection. A variety of L2 switches provide PoE.
- Category 5 cable is required for the uplink connection between the expansion switches and the CXi II/MXe III/AX, and is recommended for all other Ethernet connections. Category 3 cable can be used to connect single IP Phones directly to the expansion switches or to the Layer 2 switch of the CXi II.
- L2 switches for voice-only networks do not require VLAN capability.



SS0298

Figure 10.11: Expanded Voice only System

Voice and Data Networks

You can connect additional IP phones to the AX, MXe III and CXi II controllers. Use one or two switches connected in a daisy chain. The L2 switches connect to the Ethernet ports or to the controller.

NOTE: The expansion switches must be manageable and must adhere to the 802.1p/Q VLAN standard.

Program the uplink port of the expansion switches to send and receive tagged packets on the default VLAN (1), and make sure that the expansion switches treat packets with priority value 6 as highest priority (this is the default setting on most switches).

Program the CXi II/MXe III/AX to tag packets on their 10/100/1G LAN port(s).

NOTE: This assumes that the data VLAN is 1, and this is not always the case. You have to use untagged native to change this.

Guidelines

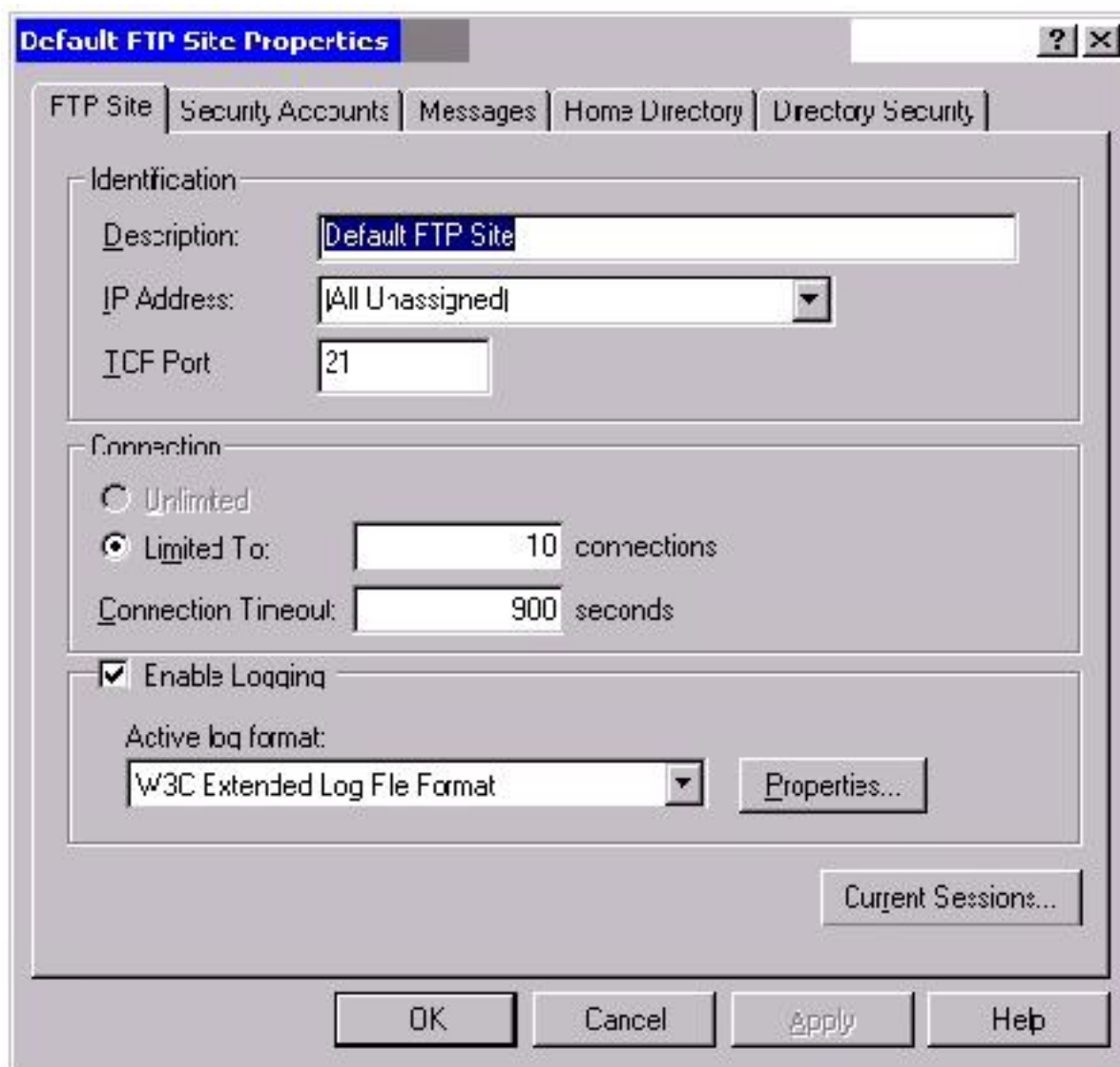
1. When connecting an expansion L2 switch to the CXi II, ensure that the switch is only connected to the 10/100/1G LAN port. If using two 24-port switches, connect the second switch to the first in a daisy chain.
2. When connecting expansion L2 switches to the CXi II, ensure that VLAN tagging is enabled on all trunk links that connect the expansion switches together. For two expansion switches, you need to enable VLAN tags for VLAN 1 on:
 - 10/100/1G LAN port of CXi II (port 17)
 - Switch port on first expansion switch; connects to port 17
 - Switch port on first expansion switch; connects to second switch
 - Switch port on first expansion switch; connects to first switch
3. When connecting L2 switches to the MxIII or AX, ensure that VLAN tagging is enabled on all trunk links that are used to connect L2 switches together. Enable VLAN tags for VLAN 1 on the LAN ports of the MxIII/AX and the switch ports on the L2 switches that connect to the MxIII/AX.
4. Connect the port(s) to the highest speed port on the first expansion switch, preferably a 1G port.
5. By default, all ports of the internal Layer 2 switch are on the default VLAN (1). This setting cannot be changed except on a CXi II.
6. Connect IP devices (PCs) to the voice and data network directly through a switch or indirectly through a dual-port IP phone. Servers must be connected to the network directly via a switch.
7. Dual-port phones use the same port speed as the connected PCs. For this reason, PCs with 100 Mbps Ethernet cards are recommended.
8. Mitel telephones can receive power from an adapter, a power brick or a powered Ethernet connection. The 10/100 802.3af LAN ports on the CXi II provide Power over Ethernet (PoE), as do some expansion switches. The 10/100/1G LAN port does not provide PoE and the MxIII and AX do not provide PoE.
9. Category 5 or better cable is recommended for all Ethernet connections in a mixed voice and data environment.

Windows 2000 FTP Server

Figure 10.12, *Figure 10.13* and *Figure 10.14* 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 10.12:** Windows 2000 FTP Site Tab

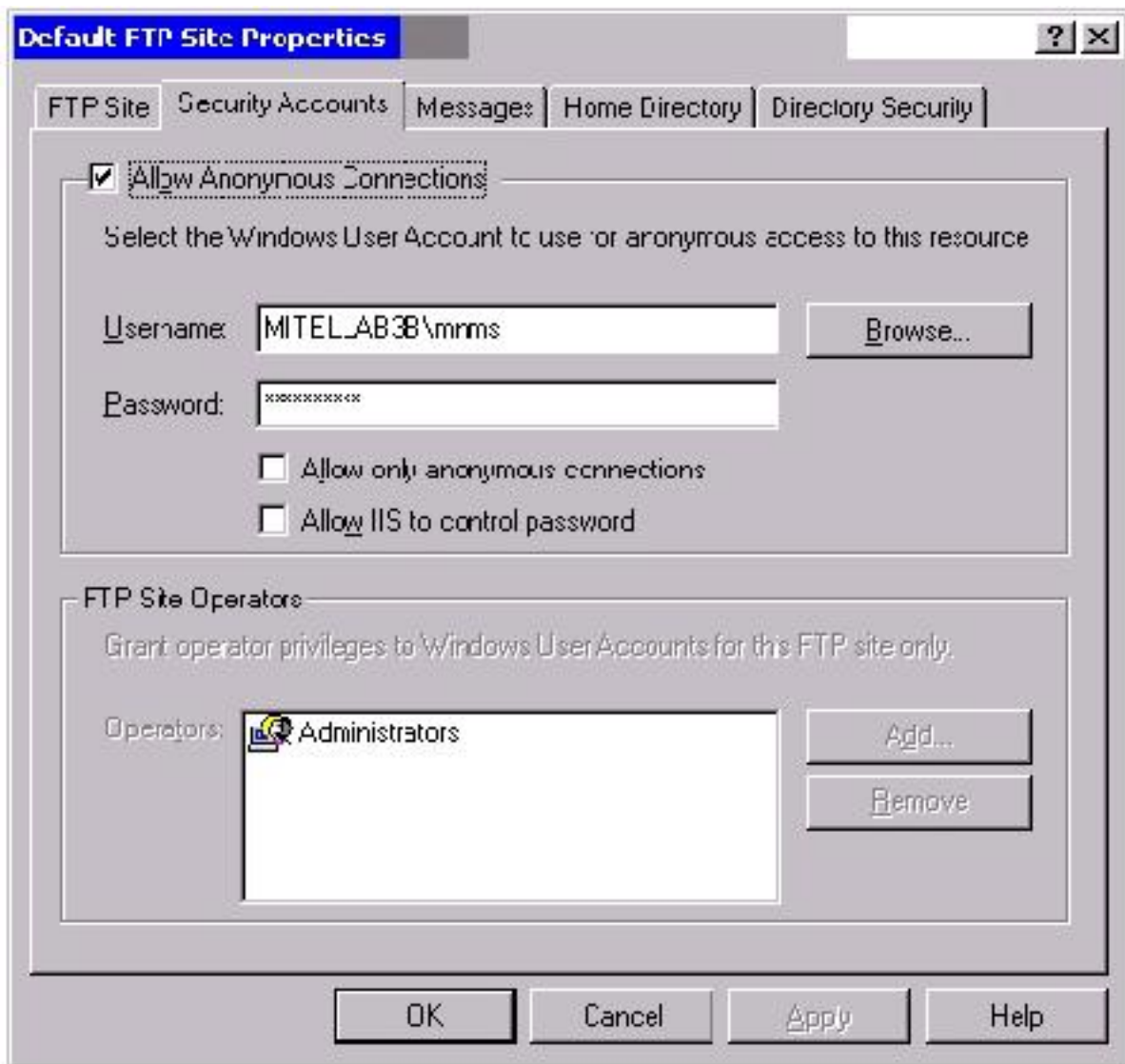


Figure 10.13: Windows 2000 Security Accounts Tab

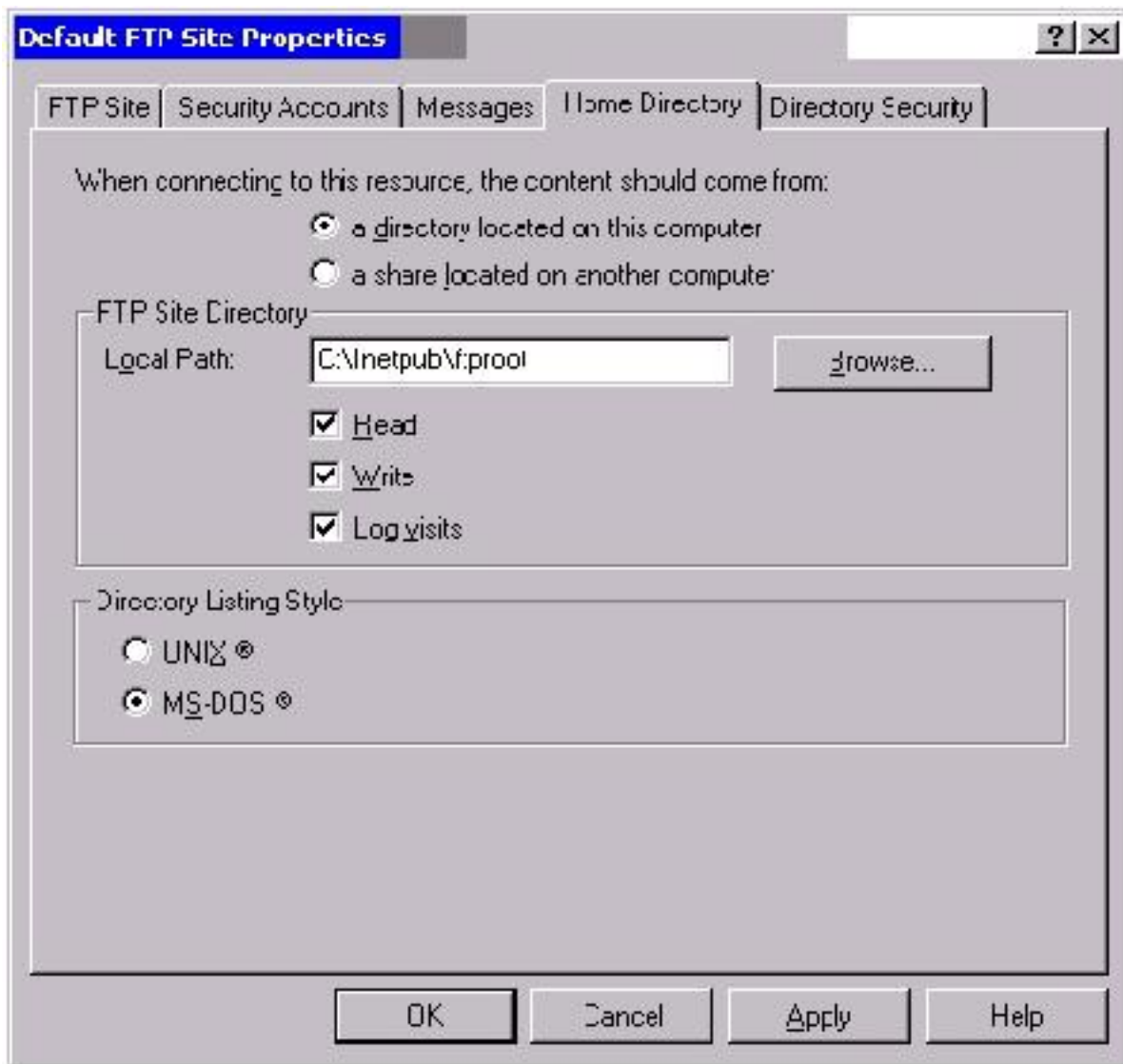


Figure 10.14: Windows 2000 Home Directory Tab

Appendix D: Status LEDs

Overview

This appendix describes the following LEDs in the 3300 ICP.

- [Controller LEDs](#)
- [Analog Services Unit LEDs](#)
- [IP Phone and IP Appliance LAN LEDs](#)
- [Peripheral Cabinet LEDs](#)
- [In-Line Power Unit LEDs](#)

For detail on any alarms, see the 3300 ICP Troubleshooting Guide.

Controller LEDs

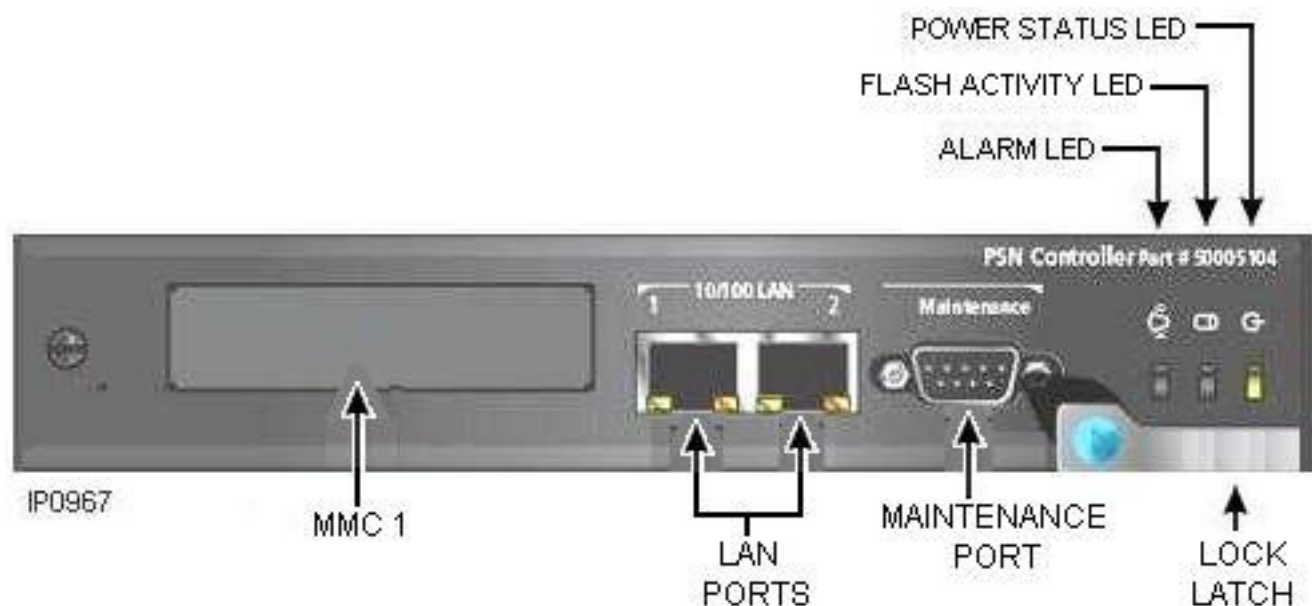


Figure 11.1: AX Controller Card LEDs

Power LED (page 270)	T1/E1 Combo (page 276)
Flash Activity LED (page 270)	Dual T1/E1 Framer (page 275)
Alarm LED (page 270)	Quad BRI Framer (page 278)
CIM LEDs (page 273)	Ethernet LEDs (page 273)

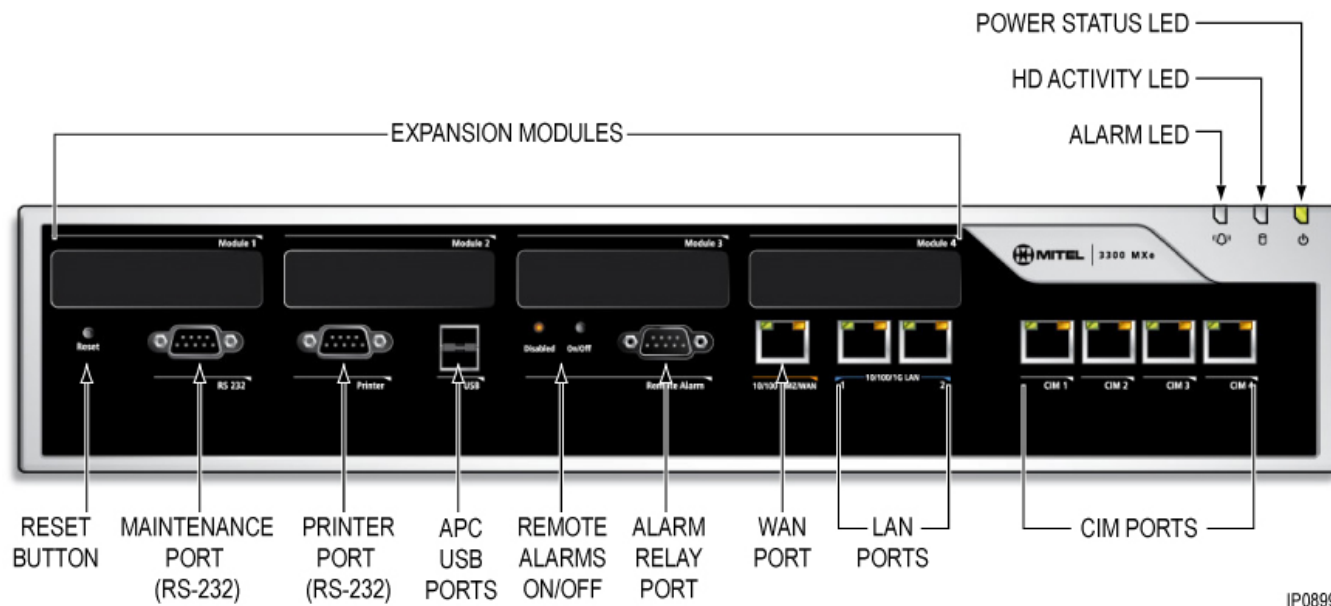


Figure 11.2: MXe III Front Panel

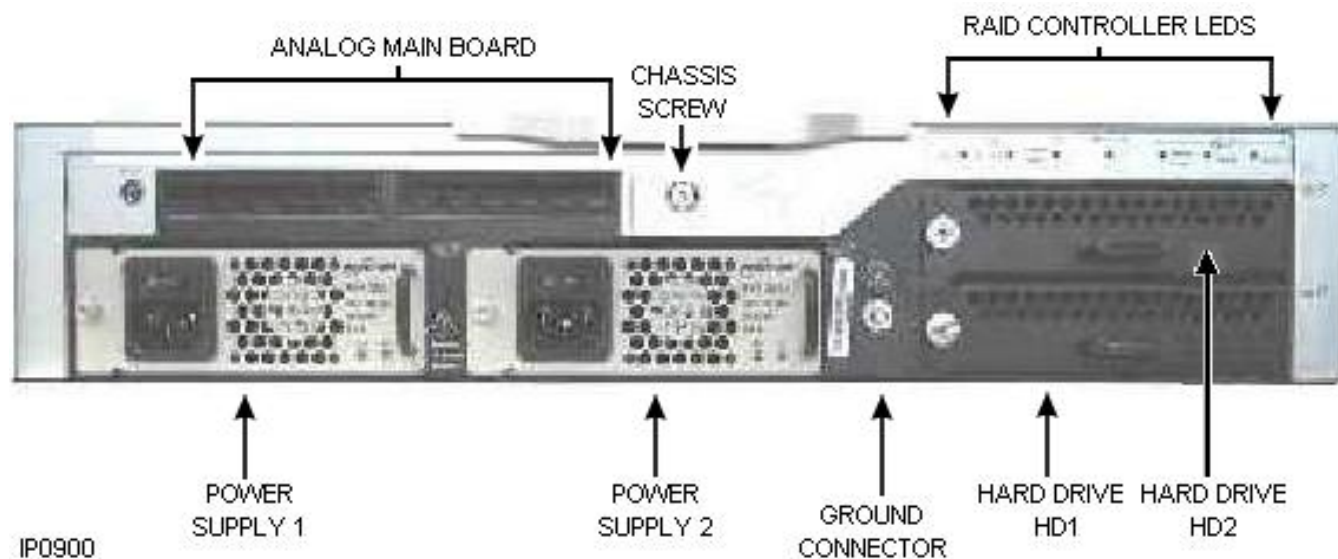
Power LED ([page 270](#))Hard Drive LED ([page 270](#))FIM LEDs ([page 272](#))Ethernet WAN/LEDs ([page 273](#))Alarm LED ([page 270](#))CIM LEDs ([page 273](#))T1/E1 Combo Card ([page 277](#))Dual T1/E1 Framer ([page 275](#))Quad BRI Framer ([page 278](#))Remote Alarms On/Off ([page 274](#))

Figure 11.3: MXe III Controller – Rear Panel with Analog

Power Supply LED ([page 275](#))RAID Controller LEDs ([page 271](#))

Controller Alarm LEDs (AX, MxIII/MxIII-L)

Table 11.1: CX II/CXi II, AX and MxIII/MxIII-L Controller Alarm LED

LED Status	Meaning
OFF	There is no system alarm.
Yellow flashing	Minor alarm.
Orange flashing	Major alarm.
Red flashing	Critical alarm.

Controller Power LED (AX, MxIII/MxIII-L, CX II/CXi II)

Table 11.2: Controller Power LED

LED Status	Meaning
Green on solid	The system booted successfully and is operating normally.
Red - two flashes	The unit is starting up properly (seen only during boot process). Not applicable to the CX II/CXi II. On the CX II/CXi II the LED is always GREEN during startup unless an error occurs. On an error the LED turns solid RED.
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. In the case of the AX, the LED is also off during boot-up.

Hard Drive or Flash Activity

Table 11.3: Hard Drive/Flash Activity LED (Media Access)

LED Status	Meaning
Off	The hard drive or flash is inactive.
On flashing	The internal hard disk or either of the flashes is being accessed.

RAID Controller

Refer to Knowledge Base Article 11-5191-00213 “SATA RAID Controller Operations Manual” for RAID operation details.

MXe III/MXe III-L

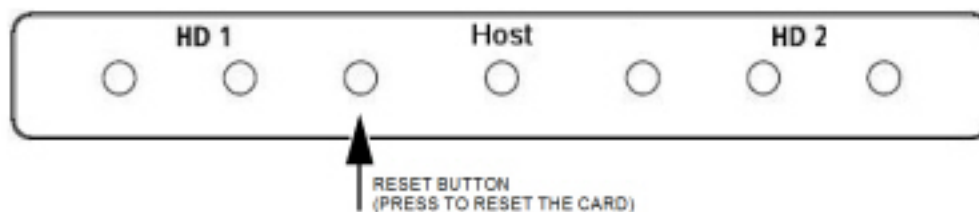


Figure 11.4: MXe III/MXe III-L RAID Controller LEDs

Table 11.4: MXe III/MXe III-L RAID Controller LEDs

Host	Meaning
OFF	<ul style="list-style-type: none"> System off or reset Hard disks disconnected
Green ON	Host idle
Flashing Green	Disks being accessed

Table 11.5: MXe III/MXe III-L RAID Link LEDs (Sheet 1 of 2)

Hard Drive State	HD 1	HD 2	Description
Idle	BLUE	BLUE	Disk idle state
Normal	BLUE flashing	BLUE flashing	Disk read or write
Off-line	OFF	OFF	No power, cable disconnected, or hard drives absent

Table 11.5: MxIII/MxIII-L RAID Link LEDs (Continued) (Sheet 2 of 2)

Hard Drive State	HD 1	HD 2	Description
No host	ON	OFF	HD 2 absent
	OFF	ON	HD 1 absent
Rebuilding	Fast BLUE flashing	Slow BLUE flashing	HD 2 being updated
	Slow BLUE flashing	Fast BLUE flashing	HD 1 being updated
Failure	BLUE	Slow BLUE flashing	HD 2 failed or out of date
	Slow BLUE flashing	BLUE	HD 1 failed or out of date
Mismatch	BLUE	BLUE flashing SOS signal (Three quick flashes followed by three slow flashes)	HD 2 was swapped but does not match
	BLUE flashing SOS signal	BLUE	HD 1 was swapped but does not match

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 11.6: Controller FIM LEDs (LX)

LED Status	Meaning (Both LEDs)
ON	In-frame synchronization.
Flashing	Out of synchronization <i>OR</i> Tx and Rx fiber optic cables reversed.
OFF	Power off <i>OR</i> held in reset.

LAN Ethernet Ports

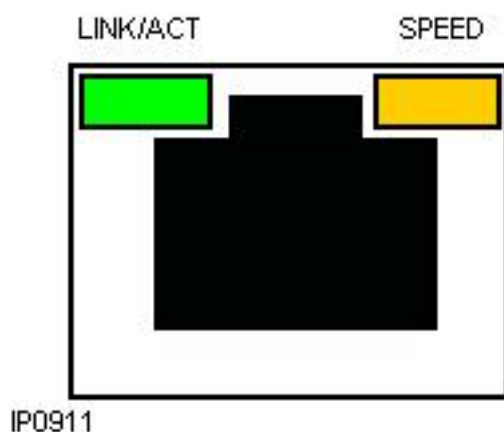


Figure 11.5: Controller LAN Ethernet Port LEDs (AX, CX II/CXi II/MXe III/MXe III-L)

Table 11.7: WAN/LAN Port LEDs (CX II/CXi II/MXe III/MXe III-L, AX)

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.
NOTE: The AX and MXe III-L controllers do not support a WAN interface.	

CIM, Embedded and Quad MMC

Table 11.8: Controller CIM LEDs

LED Status	Meaning (Both LEDs)
ON	In-frame synchronization.
Flashing	Out of synchronization or Tx and Rx copper cables reversed.
OFF	Power off or held in reset.

Controller Alarm

The table below shows the meaning of the alarm LEDs.

Table 11.9: Controller Alarm LEDs (CX II/CXi II/MXe III/MXe III-L, AX) (Sheet 1 of 2)

Alarm		LED State	Meaning
AX	CX II/CXi II/MXe III/MXe III-L		
Critical	Critical	Red flashing	Service is lost; immediate maintenance required (system fail transfer invoked if enabled) OR Power on reset ongoing.
Major	Major	Orange flashing	Service has degraded beyond predetermined threshold. OR Embedded voice mail is not functioning or disk space is at 98%.
Minor	Minor	Yellow flashing	Minor malfunction in system (minor alarm raised when system not fully operational). OR Embedded voice mail disk space is at 90%.
n/a	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.

Table 11.9:Controller Alarm LEDs (CX II/CXi II/MXe III/MXe III-L, AX) (Continued) (Sheet 2 of 2)

Alarm		LED State	Meaning
AX	CX II/CXi II/MXe III/MXe III-L		
	Remote Disabled (MXe III/MXe III-L only)	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.

Power Supply Unit LEDs

LED	Status	Meaning
Input OK	Green ON	Input is within parameters.
	OFF	Power supply is OFF
Output OK	Green ON	Output voltage is within normal operating range.

Dual T1/E1 Framer Module

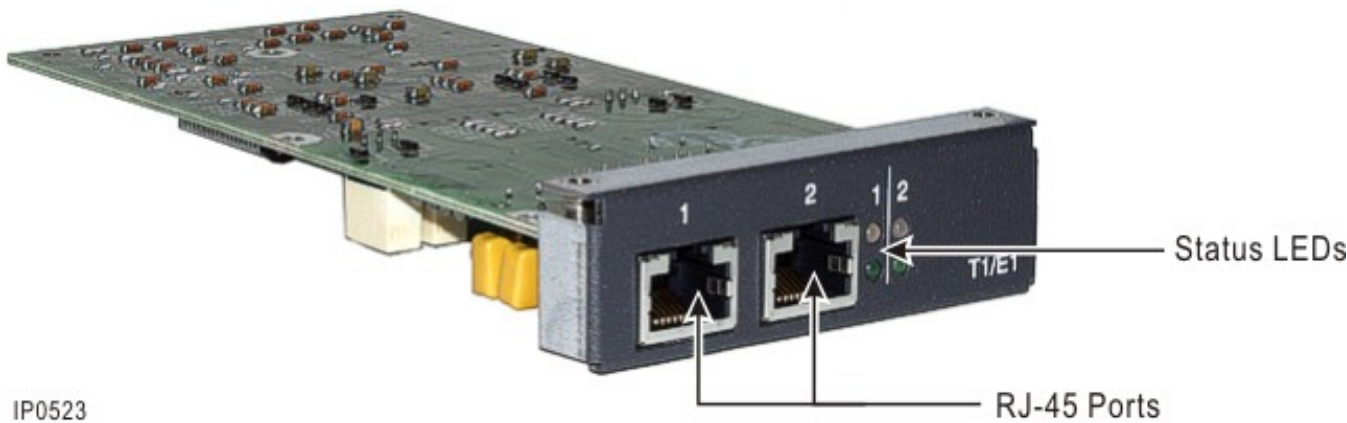


Figure 11.6: Dual T1/E1 Framer Module

Table 11.10: 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 11.7:** Controller T1/E1 Combo Card (3300 R6.0)



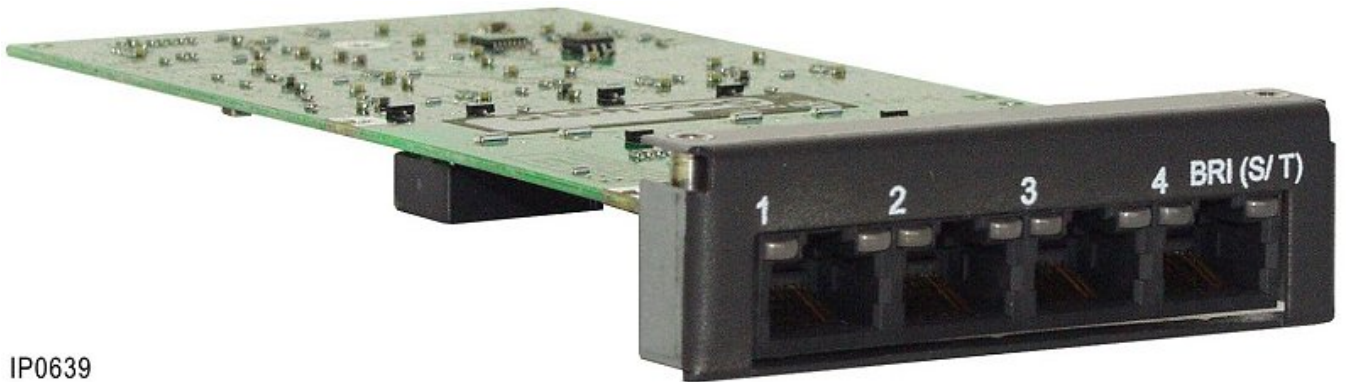
Figure 11.8: Resilient T1/E1 Combo Card (3300 R7.0)

Table 11.11: 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 11.12](#).



IP0639

Figure 11.9: Controller BRI Framer LEDs

Table 11.12: Controller BRI Framer LEDs

LED		Meaning
Alarm	Status	
Red Green	OFF OFF	BRI port not programmed. Link Descriptor is not assigned in the Digital Links 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 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.

Analog Services Unit LEDs

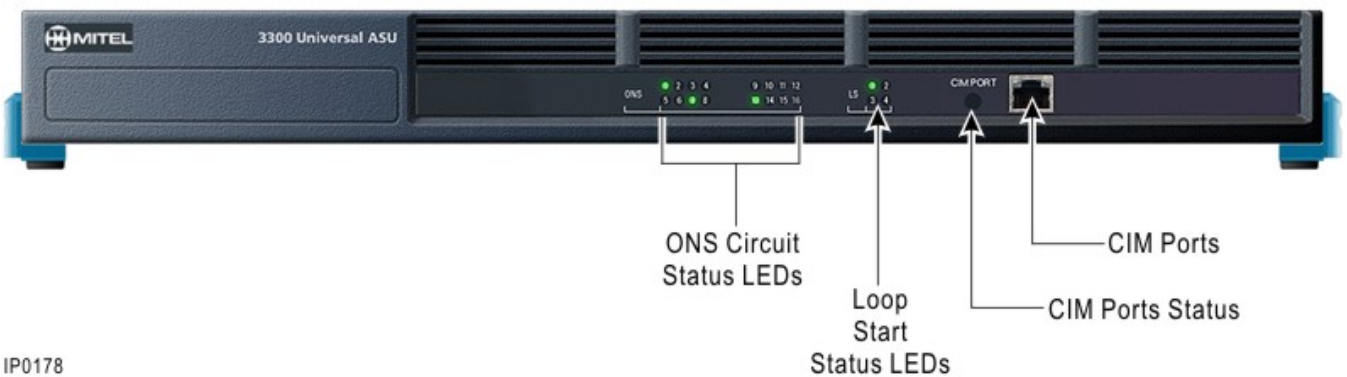


Figure 11.10: Universal ASU LEDs

The Universal ASU has 16 ONS LEDs, 4LS LEDs, and a CIM Status LED.

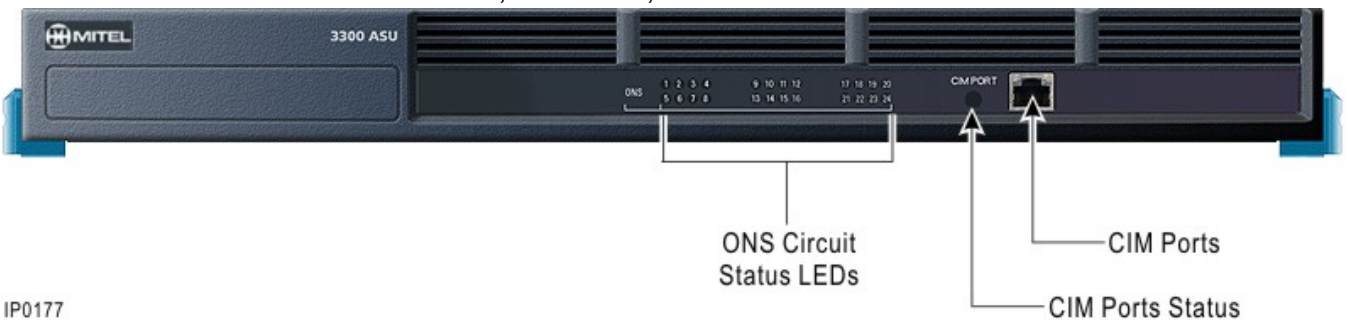


Figure 11.11: ASU LEDs

The ASU has 24 ONS LEDs, and a CIM Status LED.

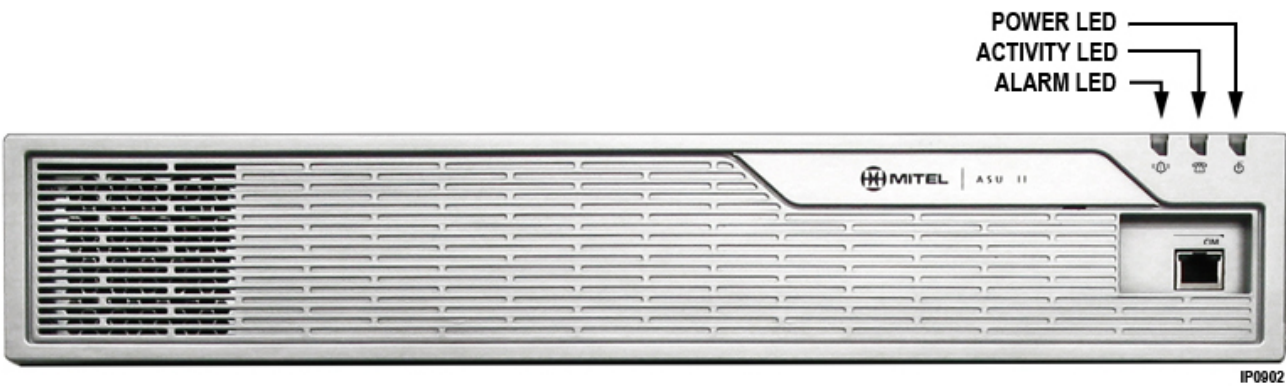


Figure 11.12: ASU II LEDs

The ASU II has an Alarm, Activity, and Power LED.

Table 11.13: CIM LED (Sheet 1 of 2)

LED Status - RED	Meaning
ON	Communication link synchronized with Controller.

Table 11.13: CIM LED (Continued) (Sheet 2 of 2)

LED Status - RED	Meaning
Flashing	Powered on, BSP running.
OFF	No power.

Universal ASU, ASU, and ASU II CIM Status LEDs

Table 11.14: 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 11.15:ASU II Alarm LED (Red)

LED Status	Meaning
Flashing or ON	System error.
OFF	No error.

Analog Services Unit II Activity LED

Table 11.16: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 11.17:ASU II Card Alarm LED

LED Status	Meaning
Red ON	System error.
Red OFF	No error.

ASU II ONS Card Activity LED

Table 11.18:ASU II ONS Card Activity LED

LED Status	Meaning
Green ON	System error.
Green OFF	No error.

ASU II Combo Card Activity LED

Table 11.19: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.

The table below shows the meaning of the IP Phone, IP Appliance LAN LEDs.

Table 11.20: 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

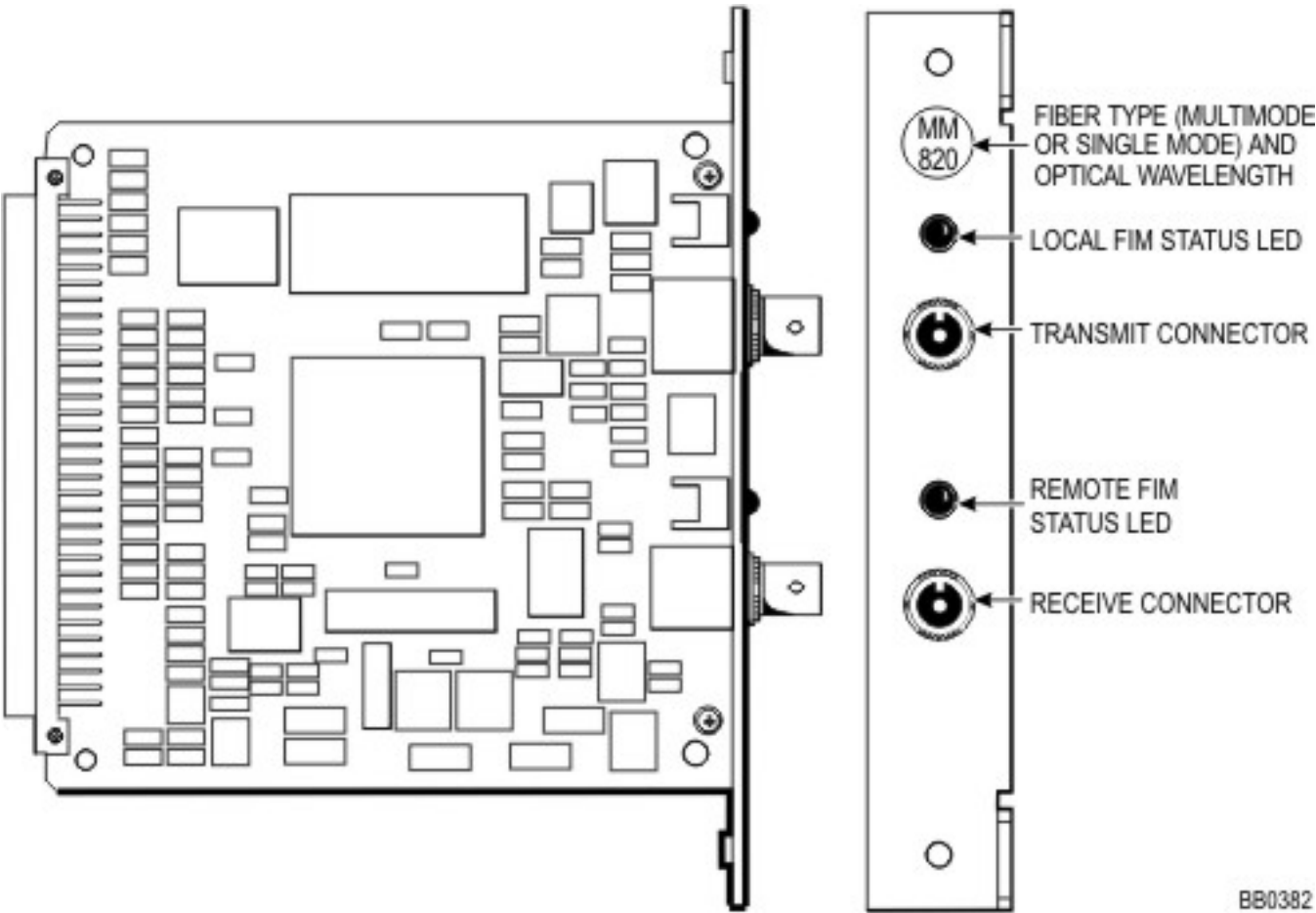


Figure 11.13: Peripheral Cabinet FIM LEDs

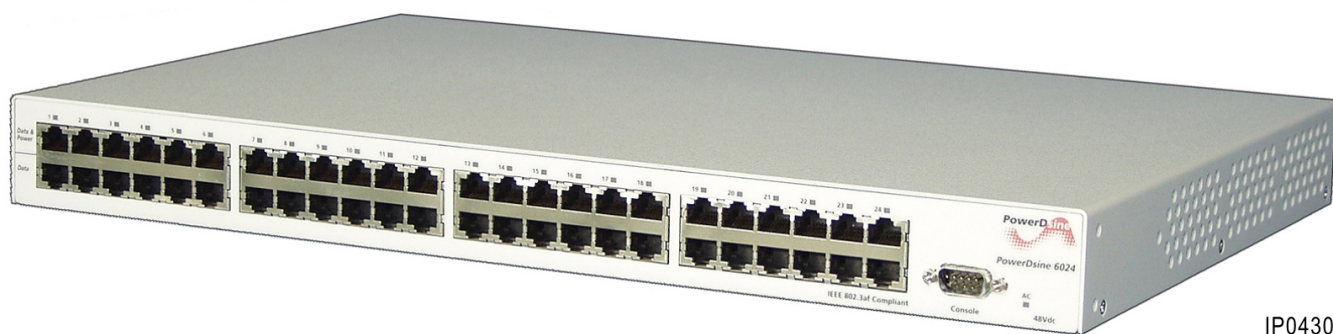
LED Status	Meaning (All LEDs)
ON	In-frame synchronization

LED Status	Meaning (All LEDs)
Flashing	Out of synchronization <i>OR</i> TX and RX fiber optic cables reversed.
OFF	Power off <i>OR</i> held in reset

Table 11.21: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.

In-Line Power Unit LEDs

**Figure 11.14:** In-Line Power Unit LEDs

The In-Line Power Unit LEDs are grouped as follows:

- [AC Power](#)
- [Power Unit Alarm](#)
- [Power Unit Port Status](#)

AC Power

Table 11.22: 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

The table below shows the meaning of the Alarm LED.

Table 11.23: 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 11.24: Power Unit Port Status LEDs (Sheet 1 of 2)

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.

Table 11.24:Power Unit Port Status LEDs (Continued) (Sheet 2 of 2)

LED Status		Meaning	Port Voltage
Green	Orange		
OFF	ON	Overload condition. <i>OR</i> Shorted terminal port. <i>OR</i> 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. <i>OR</i> 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. <i>OR</i> Unplugged load.	No DC voltage present on spare pairs.

Appendix E: FRU Part Numbers

Hardware Part Numbers

Table 12.1: Hardware Part Numbers (Sheet 1 of 3)

Part Number	Description
3300 ICP Controllers and Components	
50006507	AX Controller, i-Button, AC power
50008331	MXe III-L Controller ¹
50001247	3300 - 128 Channel Echo Canceller
50006508	AX Controller Card
50005751	DSP II MMC
50003560	Dual T1/E1 Trunk MMC (AX, MXe III, LX)
50003726	Stratum 3 Clock Module
50004070	3300 Quad BRI Module
50004451	Quad CIM MMC
50005184	Analog Main Board III (CX II/CXi II, MXe III), Version III
50004870	Analog Option Board (CX II/CXi II only), Version II NOTE: This AOB is only compatible with the AMB Version II (PN 50004870) and AMB Version III (PN 50005184).
50004920	3300 Spare i-Button
50006431	MXe III RAID Controller Sub-system
50005104	4 + 12 Port Combo Card (AX and ASU II)
50005731	3300 24 Port ONSP Card (for all markets, excluding Brazil)
50005160	T1/E1 Combo MMC II
50005883	512MB RAM Module (for MXe III only)
50006727	3300 1GB RAM Module Upgrade
50006794	512 MB RAM Module Downgrade (for MXe III III, CX II, and CXI II with 1 GB RAM Module)

Table 12.1: Hardware Part Numbers (Continued) (Sheet 2 of 3)

Part Number	Description
50006729	3300 CX II Controller with 1GB RAM (replaces 5006093)
50006731	3300 Mx III Controller with 1GB RAM
50006730	3300 Mx III Processor Card with 1GB RAM (replaces 50006432)
50006727	3300 CXi II and Mx III 1GB RAM Module Upgrade
50006794	3300 CXi II and Mx III 512MB RAM Module Upgrade
52002581	3300 Mx III Expansion Kit
50005761	3300 Mx Rack Mount Brackets
50006162	Music On Hold Input Adaptor
Services Units	
50005105	3300 Analog Services Unit II with AC Power Supply
Power Units	
50005611	Power Cord single - Euro (replaces Euro 3 Pack -2952)
50005612	Power Cord single - UK (replaces UK 3 Pack - 2977)
50005084	Mx III AC Power Supply
50005091	ASU II AC Power Supply
50005182	AX AC Power Supply
50005471	AX Fan Assembly
50006510	3300 CX(i) II Fan Kit
50005683	Mx Fans FRU
51000582	C7 Power Cord with UK Plug
51004990	C7 Power Cord with Euro Plug
51005172	C7 Power Cord with NA Plug
Consoles	
50005811	5540 IP Console

Table 12.1: Hardware Part Numbers (Continued) (Sheet 3 of 3)

Part Number	Description
¹ The MXe III-L controller will be available in Q1, 2020 only for the following regions: North America, UK, Middle East, Africa, Australia, and New Zealand.	

Software Part Numbers

Table 12.2: Software Part Numbers

Part Number	Description
50006266	3300 CXi II Controller SATA SSD (16 GB, 32 GB & 128 GB SATA SSD). See Note at the end of the table.
50006268	3300 MXe III Controller SATA SSD (60 GB, 64 GB & 128 GB SATA SSD). See Note at the end of the table.
50006965	3300 MXe III SATA SSD 2pk (Cntr-Server).
50008286	3300 AX 16GB Compact Flash (CF).
50008286XX	16GB Compact Flash (for AX only) (for all markets excluding Americas)
50006509	3300 AX 2G & 4G Flash SSD
50005441	3300 AX 4G VM Flash SSD
50006511	SX-200 AX SW 4G SSD
50006266XX	3300 CX II Controller SATA SSD INT
50006965XX	3300 MXeIII SATA SSD 2pk (Cntr-Svr) INTL
50006509XX	3300 AX 2G & 4G Flash SSD INTL
NOTE: This is the current drive size shipped under this part number; however, this size can be different than listed - depending on the inventory.	

Appendix F: System Capacity and Parameters

Port Usage

Table 13.1:Port Usage (Sheet 1 of 2)

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
PDA, Application communication	3998
UDP/TCP for SIP	5060
TLS (transport layer security) for SIP	5061
E2T to RTC (SSL)	6000
Set to ICP (Unsecured)	6800
Set to ICP (SSL)	6801
Set to ICP (Secure Minet)	6802
5550 TKB to IP Console PC (Secure Minet)	6902, 10002
PMS for voice mail port	6830
E2T voice UDP ports (prior to 3300 R6.0)	RTP/UDP 5000 to 5512
E2T voice UDP ports (post 3300 R6.0)	RTP/UDP 50000 to 50255
E2T voice UDP ports (post 3300 R8.0)	RTP/UDP 50000 to 50511
RTC	TCP 6800
IP Sets	TCP 6900
System Data Synchronization	7050
IP Sets - Voice B1/B2, Rx	RTP/UDP 50000/50511

Table 13.1:Port Usage (Continued) (Sheet 2 of 2)

Function	Port/Socket Number
IP Sets - Voice B1/B2, Tx	RTP/UDP 50000/50511
ACD Real Time Event	15373
IP PMS (3300 R6.0)	15374
5550 Console Keypad to Console PC (See Note)	6800 (PC must allow inbound TCP sessions to port 10000)
Console PC to ICP (See Note)	6800, 7011, 1606
NOTE: These TCP ports must not be blocked or conflict with other applications running on the console PC.	

For a more complete list, refer to the *MiVoice Business Engineering Guidelines*.

Encryption Support

Signaling encryption is device dependent and used whenever supported. Voice stream encryption is optional and used if both endpoints support it. Calls initiated on a 3300 ICP or a legacy IP set which does not support encryption (pre- 3300 R6.0) are supported, but will not be encrypted. The encryption scheme used for voice (AES or Cast) is negotiated by the endpoints during call setup.

For information on application support for encryption, see the *MiVoice Business Engineering Guidelines*.

Table 13.2:E2T/TDM Encryption

Device	Signaling Mode	Voice Streaming Mode
E2T	SSL/Secure Minet	AES/No encryption

Table 13.3:Telephone Encryption

Telephone	Signaling Mode	Voice Streaming Mode
5215DM/5220DM, 5212, 5224, Navigator, 5312, 5320, 5324, 5330, 5340, 5360, 6905, 6910, 6920, 6930, 6940	SSL/Secure MiNet	AES/Cast/No encryption
5001, 5005, 5010, 5015, 5020, 5140, 5201, 5205, 5207, 5215, 5220, 5240	Secure MiNet	AES/No encryption
TeleMatrix 3000IP	Secure MiNet	AES/No encryption

IP Set Features

Table 13.4: IP Set Features (Sheet 1 of 2)

Option	5201 5207	5212 5215 5240 5312 5324	5220 5224	5320 5330 5340 5360	6905 6910 6920 6930 6940	Navi- gator	Tele- Matrix 3000IP 5560 IPT
Compression Support	G.711	G.711 G.729a	G.711 G.729a	G.711 G.729aG .722.1	G.711 G.729aG .722.1	G.711 G.729a	See Note 1
Voice QoS (802.1p/q)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
FCC CLASS B Support	Yes	Yes	Yes	Yes	Yes	Yes	See Note 1
POE using Spare Pair or Signal Pair (802.3af)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AC Power Adapter (24 VDC)	No	No	Yes	No	No	No	Yes
Peripherals (Modules) Support							
PKM	No	Only on 5324	Yes	Only on 5330 & 5340	Yes	No	No
Conference Unit	No	No	Yes	Yes	No	No	No

Table 13.4: IP Set Features (Continued) (Sheet 2 of 2)

Option	5201 5207	5212 5215 5240 5312 5324	5220 5224	5320 5330 5340 5360	6905 6910 6920 6930 6940	Navi- gator	Tele- Matrix 3000IP 5560 IPT
Gigabit Stand	No	Only on 5212, 5215, 5312, 5324	Yes	Yes	See Note 5	No	No
Wireless Stand	No	Yes (except 5240)	Yes	Yes	See Note 6	No	No

NOTES:

1. Refer to TeleMatrix 3000IP Technical documentation for details.
2. The 5550 IP Console requires only an external AC power adaptor.
3. For the conference unit using a side control unit, an external AC power adaptor is required.
4. Any Cisco switch that is non-compliant with 802.3af requires a Cisco power dongle.
5. The 6905 IP Phone does not support Gigabit Ethernet. The 6910, 6920, 6930 and 6940 IP Phones support built-in Gigabit Ethernet, and do not require a Gigabit Ethernet stand.
6. The Mitel Wireless LAN Adapter is the Wireless Stand equivalent for 69xx sets. For 6905 and 6910 IP Phones, the Mitel Wireless LAN Adapter must be configured through a web browser, or through Smart Wireless Setup. It cannot be configured through the 6905 or 6910 IP Phones' Settings interface.

Optional Power Adapter for NA: 50002070 - 5x01, 5x05, 5215; 50000690 - 5x10, 5x20 (except 5320), 5x30, 5x40, 5305, 5310, 5485, 5550; 50002070, 50005080; 9132-800-210-NA - 4015IP, 4025IP.

IP Phone Power Consumption

See the *Mitel IP Sets Engineering Guidelines* in the [Document Center](#) for IP Phone power requirements.

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 13.5](#) 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 13.5: 3300 ICP Hardware Capacity (Sheet 1 of 2)

Parameter Name	MXe III, MXe III-L Base/ Expanded	CX II / CXi II	AX
Compression Channels (G.729a)	64/128/192 ²	64	64
DTMF Receivers	128	64+	128
Echo channels/E2T	64/128/ 192 ²	64	128 ⁶
Tone Detector Circuits	32	32	32
Tone Generators	128	128	128
Voice Mail Ports	30	16	20
T1/E1 Modules	4	2	1
Peripheral Cabinet (direct connection)	6	n/a	n/a
Expanded Cabinet	12	n/a	n/a
ASUs	12	3	n/a
Trunks (analog and digital combined)	628	72	108
IP Trunks between controllers ⁷	2000	2000	2000
ACD Agents ¹	350	50	50
IP Trunks per controller	2000	2000	2000
Attendant Consoles	24	8	8
IP Devices	350 / 1500 ⁴	150	100 /300 ⁵
Programmable Key Modules	75	75	75

Table 13.5: 3300 ICP Hardware Capacity (Continued) (Sheet 2 of 2)

Parameter Name	MXe III, MXe III-L Base/ Expanded	CX II / CXi II	AX
NOTES: <ol style="list-style-type: none"> 1. A combination of IP and DNI phones (no DNI in the CX II/CXi II or AX). Refer to <i>MiVoice Business Engineering Guidelines</i> for details. 2. The largest number is available only with the 192 channel PSTN gateway configuration. 3. R2 NSU only. 4. Maximum 300/1400 IP users. 5. The larger number is for light traffic (Hospitality sites) only. 6. The AX controller uses DSP echo cancellers (40 channels in total) in its default configuration, but can use the 128-channel module to increase capacity. When the 128-channel module is installed, the echo canceller channels on the embedded DSPs revert to telecom resource use. 7. 2000 is the maximum number of IP trunks in a cluster, irrespective of the cluster size. 			

System Capacity

Table 13.6: System Capacity (Sheet 1 of 4)

Parameter Name (numbers in brackets are minimum and maximum values with flexible dimensioning)	Maximum Value (default maximum)
IP User Licenses	5600 (1400)
ACD Active Agent Licenses	350, 2100 (MXe III Server, and other server-based platforms only)
SIP Trunk Licenses	2000
Analog Port Licenses	5000
Voice Mail Licenses	750 (including Advanced Voice Mail licenses)
Mailbox Licenses	750
Digital Link Licenses	16
ACDII Agent Groups	64, 128 (extended), 999 (MXe III Server, and other server-based platforms only)
ACDII Agents per Group	150, 500 (extended), 700 (MXe III Server, and other server-based platforms only)
ACDII Agent Appearances	8

Table 13.6:System Capacity (Continued) (Sheet 2 of 4)

Parameter Name (numbers in brackets are minimum and maximum values with flexible dimensioning)	Maximum Value (default maximum)
ACDII - Agent IDs	1181, 2100 (MXe III Server, and other server-based platforms only)
ACDII - Agent Paths	999
Attendant Consoles (2-48)	24
Attendant Groups (2-100)	48
Attendant Console Calls Waiting	72
Broadcast Groups (12-16000)	1875 (9000 for 512MB)
- Members per Broadcast Group	32
Busy Lamp Groups (Monitored Devices) (2-5000)	439
- Members per Busy Lamp Group	16
Call Reroute Always (250-1000)	175
Call Reroute 1st Alternates (250-1000)	336
Call Reroute 2nd Alternates (100-1000)	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 (41556 to 100000)	<ul style="list-style-type: none"> • Default is 12056 for all 700 user systems. • Default is 12256 for all 5600 user systems. • Default is 40001 for all 999 Cluster systems.
DTMF Receivers (16-200)	192

Table 13.6:System Capacity (Continued) (Sheet 3 of 4)

Parameter Name (numbers in brackets are minimum and maximum values with flexible dimensioning)	Maximum Value (default maximum)
Hunt Groups (10-3000)	server-based platforms: 2000, 64 (extended) all other platforms: 176, 16 (extended)
- Members per Hunt Group	server-based platforms: 64, 1000 (extended) all other platforms: 64, 250 (extended)
Independent Account Codes (10-40000)	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
MSDN/DPNSS Remote Directory Numbers (130000)	18500/28501/130000
Multi-device User Groups (see Note 3)	AX: 200 CX II: 100 MXe III/MXe III-L: 200 MXe III/MXe III-L (expanded): 933
Multiline Sets (12-6000)	756 or 5665 (Depending on the value of Maximum Configurable IP Users and Devices in the Licenses and Options form of the MiVoice Business System Administration Tool).
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 (10-3000)	200
- Members per Pickup Group	75
PKM Devices (2-700)	75
Routes (10-2400)	200 / 1200 (see note 1)

Table 13.6:System Capacity (Continued) (Sheet 4 of 4)

Parameter Name (numbers in brackets are minimum and maximum values with flexible dimensioning)	Maximum Value (default maximum)
Route Lists (10-1200)	128 / 600 (see note 1)
Single Line Sets (16-5000)	700
Speed Call Digit String (average 12 digits) (32766 max)	2501
Suites - Single (2-2332)	364
Suites - Linked (2-777)	500
SUPERSET Callback Messages per System (48-10000)	500
System Account Codes (10-100)	24
System Digit Strings (196000 max.)	1000 / 30001 / 170000 (see note 1)
System Speed Call (3000-10000)	1000 / 2000 (see note 1)
Telephone Directory Entries (55-130000)	20000 / 30000 / 130000 (see note 1)
Trunk Groups (8-320)	112
Trunks (8-2000)	628
Trunks per Trunk Group	175
Trunk Service Numbers (8-500)	150
NOTES: <ol style="list-style-type: none"> 1. Larger numbers apply when 250 or 999 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 64 channels or eight eight-party conferences for a total of 64 conference channels. 3. The maximum MdUG values are based on the assumption that there are only two devices per user. If there are more than two per user, the number of MdUGs will decrease proportionately. To implement different quantities, consult your Sales Engineering or Professional Services representative. 	

Appendix G: MSPLogClient Installation and Configuration

About the MSPLogClient

MSPLogClient is a LINUX Red Hat service that collects logs from MiVoice Business and sends them to the LINUX syslog server for viewing and analysis.

Installation

The MSPLogClient is available for download from the Software Downloads page on Mitel Online (MOL).

To install the MSPLogClient service on a Linux workstation:

1. Download the MSPLogClient RPM from MOL.
2. Log in as root and transfer the RPM file by FTP or other means to the workstation.
3. Type one of the following commands at a shell prompt:

`rpm -ivp <package name>.rpm` - installs the MSPLogClient.

`yum localinstall <package name>.rpm` - installs the MSPLogClient along with any required dependencies.

Example:

`rpm -ivp mitel-msplogclient-gcc4-10.5.0.5-01.i686.rpm`

4. Proceed with configuration; see the next section.

After the service is installed and configured, use the following commands to manage it:

- `$ sudo service msplogclient start` - starts the service
- `$ sudo service msplogclient stop` - stops the service
- `$ sudo service msplogclient restart` - stops (if running) and then starts the service
- `$ sudo service msplogclient reload` - directs the service to reload its configuration file.
- `$ sudo service msplogclient status` - tells you whether the service is running or stopped.

Other Useful Commands

To run MSPLogClient as a console application, use the `--local` option (`msplogclient --local`)

To display the current MSPLogClient service settings, use the following command as root `chkconfig --list` (`chkconfig --list msplogclient`).

To install the RPM Calling Party Pays, use `cpptool-1.0.0-2.noarch.rpm`.

Installation

The MSPLogClient is available for download from the Software Downloads page on Mitel Online (MOL).

To install the MSPLogClient service on a Linux workstation:

1. Download the MSPLogClient RPM from MOL.
2. Log in as root and transfer the RPM file by FTP or other means to the workstation.
3. Type one of the following commands at a shell prompt:
- 4.

```
rpm -ivp <package name>.rpm - installs the MSPLogClient.
yum localinstall <package name>.rpm - installs the
MSPLogClient along with any required dependencies.
```

Example:

```
rpm -ivp mitel-msplogclient-gcc4-10.5.0.5-01.i686.rpm
```

5. Proceed with configuration; see the next section.

After the service is installed and configured, use the following commands to manage it:

- \$ sudo service msplogclient start - starts the service
- \$ sudo service msplogclient stop - stops the service
- \$ sudo service msplogclient restart - stops (if running) and then starts the service
- \$ sudo service msplogclient reload - directs the service to reload its configuration file.
- \$ sudo service msplogclient status - tells you whether the service is running or stopped.

Configuration

Log collection starts after you add MiVoice Business to the MSPLogClient .conf file.

The logs MiVoice Business sends are the Security Logs which contain logins/logouts and lockout events and the two most important levels of Audit Trail Logs, Low (most important) and Medium. High (least important) are not sent.

To add MiVoice Business to the MSPLogClient .conf file:

1. Navigate to the /etc/msplogclient/msplogclient.conf file on the Linux workstation.
2. Make a copy of the .conf file and set it aside in case you need to revert to it.
3. Open the original .conf file and add LogServer followed by a period, and then the IP address of the MiVoice Business system as shown below. Repeat to add other systems as required.
4. Make a copy of the revised .conf file. You'll need it if you upgrade to a new version of MSPLogClient (which will install its own .conf file)

```
#####
# Define a list of MiVB instances or other
# logging applications
#
```



```
# Lines beginning with # are commented out
#####
LogServer.10.35.124.21
LogServer.10.35.124.229
LogServer.10.35.21.131
#LogServer.10.35.124.69
```

5. Save the file.
6. Enter the `service msplogclient start` command to start the MSPLogClient service and have it use the new configuration.

Log Location and Format

LOCATION

Security logs are posted to syslog using the AUTHPRIV facility code. Other logs are posted using the USER facility.

The system administrator determines where the logs are posted. Typically, the AUTHPRIV logs go to `/var/log/secure` and USER logs to `/var/log/messages`.

IMPORTANT: When a log is posted to syslog it is UTC timestamped by the syslog system. A portion of the log also contains its own local time stamp generated at the source. As such each syslog entry can contain two timestamps. The default configuration omits the source Log timestamp in favour of the syslog time-stamp.

Format

Audit Logs

```
header : Severity ; Username [value] ; SourceIP ;
AppName ; AppContext ; Action Type ; Message
```

Security Logs

```
header : Severity ; -blank- ; SenderIP ; AppName
; Security-Rule ; Outcome ; Message
```

Software Logs

```
header : Severity ; -blank- ; SenderIP ; AppName
; LoggingComponent ; -blank- ; Message
```

Maintenance Logs

```
header : Severity ; -blank- ; SenderIP ; AppName
; LoggingComponent ; Category ; Message
```

Definitions

header	The header syslog adds to the log
Severity	Log severity (Alarm, Error, Warning...)
Username	Username of user triggering the audit event
SourceIP	IP address where username triggered the audit event from.
SenderIP	IP address where the log originated from.
AppName	The application posting the Audit Log.
AppContext	The activity or trigger for an audit log.
Action Type	Specific action within the specified Audit Log Context.
Security-Rule	The activity or trigger for a Security Log.
Outcome	The Outcome or Action taken by the system as a result.
Logging Component	A designer specified component or log source.
Category	Maintenance log category / type of Maintenance log.
Message	Information details around the log event.

Appendix H: Configure New/Used Controllers and Storage Devices

Greenfield Installations

A greenfield installation refers to the installation of the required MiVoice Business software version on a *brand-new* controller with a *brand-new* storage device.

Installation for MxIII, MxIII-L, CX II and CXi II Controllers

Overview

This section describes the initial setup procedure or greenfield software installation of MiVoice Business Release 9.1 or later for MxIII, MxIII-L, CX II and CXi II controllers on the following brand-new components from Mitel:

- Controller
- Hard Disk

NOTE: If you want to install a pre-9.0 MiVoice Business Release (for example, MiVoice Business Release 8.0 SP3) on your new controller and new disk, refer to **Appendix H, Configure New/Used Controllers and Storage Devices > Greenfield Installs** in the MiVoice Business Technician's Handbook, Release 8.0 SP3 document.

NOTE: The MxIII-L controller requires MiVoice Business Release 9.1 or later only.

The controller ordered from Mitel may ship with either U-Boot or Bootrom as the bootloader; you can determine the bootloader only after you physically receive the controller component (see [Determine 3300 ICP Controller Bootloader](#)).

The hard disk ordered from Mitel may ship with either MiVoice Business Release 7.2 SP2 or 9.1 installed; you can determine the software release version of the received hard disk by checking the attached label.

Based on the hard disk software version and controller received, you must follow the appropriate procedure below for the installation of the target MiVoice Business Release 9.1 (or later) software version.

Before you Begin

- Ensure that you have installed the new hard disk into the new controller (see [Disk Drive Installation \(3300 ICP Controller\)](#)).

Procedures

Table 16.1:Greenfield Install Procedures (Sheet 1 of 2)

Bootloader of New Controller	MiVB S/W Version on New Hard Disk	Greenfield Installation Procedure
Bootrom	7.2 SP2	See Install System Software using the Migration Tool .

Table 16.1:Greenfield Install Procedures (Continued) (Sheet 2 of 2)

Bootloader of New Controller	MiVB S/W Version on New Hard Disk	Greenfield Installation Procedure
U-Boot	7.2 SP2	<p>Option 1 -Guided Full Migration: See Install MiVB 9.0 or Later on a 3300 ICP Controller using HDD.</p> <p>Or</p> <p>Option 2 -Manual Full Install: See Install MiVB Software on a 3300 ICP Controller (Manually).</p>
Bootrom	9.1	<p>1) Upgrade the bootloader of the 3300 ICP controller from Bootrom to U-Boot using one of the following two methods depending on the availability of a spare disk with a pre-9.0 MiVoice Business software version:</p> <ul style="list-style-type: none"> • If you have a spare (used) disk with a pre-9.0 MiVoice Business software version and know its active partition number, see Upgrade 3300 ICP Controller's Bootloader using the Migration Tool. • If you do not have a spare (used) disk with a pre-9.0 MiVoice Business software version, see Upgrade 3300 ICP Controller's Bootloader Without Using a Hard Disk. <p>2) Install the new 9.1 HDD into the controller (see Disk Drive Installation (3300 ICP Controller)).</p> <p>3) Set Network Configuration on 3300 ICP Controller with a New HDD.</p> <p>4) Log in to the Server Manager and license the system (see ServiceLink > Status in the <i>Server Manager Help</i>).</p>
U-Boot	9.1	<p>1) Install the new 9.1 HDD into the controller (see Disk Drive Installation (3300 ICP Controller)).</p> <p>2) Set Network Configuration on 3300 ICP Controller with a New HDD.</p> <p>3) Log in to the Server Manager and license the system (see ServiceLink > Status in the <i>Server Manager Help</i>).</p>

Installation for AX Controllers

Overview

This section describes the initial setup procedure or greenfield software installation of MiVoice Business Release 9.1 or later for an AX controller.

Before you Begin

Ensure that you have the following:

- A new AX controller including a brand-new AX Controller Card.
- A new 16 GB Compact Flash (CF) preloaded with MiVoice Business 9.1 or later software.
- Access to the controller's Maintenance port.

Procedure

1. Insert the 16 GB CF in the **Compact Flash 2** slot of the AX controller card.
2. [Access 3300 ICP Controller Through the Maintenance Port](#)
3. Power on the controller.
4. Wait for the system to boot the development image named RTC8260 from partition 1 and display the -> prompt in the communication application.

***NOTE:** It takes around two minutes for the system to boot the development image. Proceed with the next step after you observe the messages: /sysro/ - disk check in progress ...and /sysro/ - Volume is OK.*

5. From the communication application, run the following commands:

```
Upgrade_Xilinx  
Upgrade_Bootrom  
reboot
```

The U-Boot inherits networking parameters from the VXWorks' bootline in FLASH and automatically boots the system software from partition 2.

6. An End User Licence Agreement screen is displayed on the communication application. Read the entire EULA text; if you are in agreement, select **Accept** to proceed with the configuration of the server through the Bootstrap console (see [Set Network Configuration on 3300 ICP Controller with a New HDD](#)).
7. After the MiVoice Business system is up and running, log in to the Server Manager as user *admin* and license the system (**ServiceLink > Status**).
8. Log in to the MiVoice Business System Administration Tool to provision the system.
9. To upgrade the software, log in to Server Manger (**ServiceLink > System upgrade**).

Controller Replacement

See [3300 ICP Controller Replacement](#) for details on 3300 ICP Controller Replacement.

Hard Disk Replacement

Overview

This section describes the procedures for hard disk replacement on your MxIII, MxIII-L, CX II and CXi II controllers. For replacement of the Compact Flash (CF) cards on AX controllers, see

If you are unable to continue using your hard disk with MiVoice Business 9.0 or later (for example, due to a hardware failure) on your 3300 ICP controller with U-Boot, then you must replace your hard disk. The replacement hard disk may either be a brand-new hard disk from Mitel or a used hard disk.

NOTE: This section assumes that you are keeping the old controller and performing replacement of the hard disk, only.

The hard disk ordered from Mitel may ship with either MiVoice Business Release 7.2 SP2 or MiVoice Business Release 9.1; you can determine the software release version of the received hard disk by checking the attached label.

Based on the software version on the hard disk, see the appropriate procedure below to enable continued service with MiVoice Business Release 9.0 or later.

NOTE: If you want to install a **pre-9.0** MiVoice Business Release (such as MiVoice Business 8.0 SP3) on the new hard disk, refer to **Appendix H, Configure New/Used Controllers and Storage Devices > Hard Disk Replacement** in the MiVoice Business Technician's Handbook, Release **8.0 PS3** document.

Before you Begin

- Ensure that you have installed the disk drive into your controller (see [Disk Drive Installation \(3300 ICP Controller\)](#)).

Procedures

Table 16.2:Hard Disk Replacement Procedures (Sheet 1 of 2)

Status of Replacement Hard Disk	MiVB S/W Version on New Hard Disk	Hard Disk Replacement Procedure
Brand-new	7.2 SP2	You can use either of the following methods: Install MiVB Software on a 3300 ICP Controller (Manually) (This procedure requires a TFTP and HTTP server). Or New Replacement Drive with MiVB 7.2 SP2 Software .

Table 16.2: Hard Disk Replacement Procedures (Continued) (Sheet 2 of 2)

Status of Replacement Hard Disk	MiVB S/W Version on New Hard Disk	Hard Disk Replacement Procedure
Brand-new	9.1	<ol style="list-style-type: none"> 1. Access 3300 ICP Controller Through the Maintenance Port. 2. Power on the controller. 3. The U-Boot initiates a boot of the MiVoice Business software. A brand-new hard disk can be booted from either partition because MiVoice Business 9.0 (or later) software load is pre-loaded on both partitions of a brand-new hard disk. 4. Set Network Configuration on 3300 ICP Controller with a New HDD. 5. After the MiVoice Business system boots successfully, license the system (ServiceLink > Status in the <i>Server Manager Help</i>).
Used	Pre-9.0	<p>You can use either of the following methods: Install MiVB Software on a 3300 ICP Controller (Manually) (This procedure requires a TFTP and HTTP server). Or Used Replacement Drive with Pre-9.0 Software.</p>
Used	9.0 or later	<p>You can use either of the following methods: Install MiVB Software on a 3300 ICP Controller (Manually) (This procedure requires a TFTP and HTTP server). Or Used Replacement Drive with MiVB 9.0 or Later Software.</p>

AX Compact Flash Card Replacement

See [Compact Flash Cards \(AX\)](#) for details on AX Compact Flash Card replacement.

RTC Card Replacement

See [RTC Processor Card \(MXe III/MXe III-L Controller\)](#) for details on RTC Card Replacement.

E2T Card Replacement

See [E2T Processor Card \(MXe III/MXe III-L Controller\)](#) for details on E2T Card Replacement.

Set up an HTTP/HTTPS Server and a Custom Repository

The Server Manager provides an option to store the MiVoice Business software image on a custom repository (HTTP or HTTPS server) that you can use during a system upgrade.

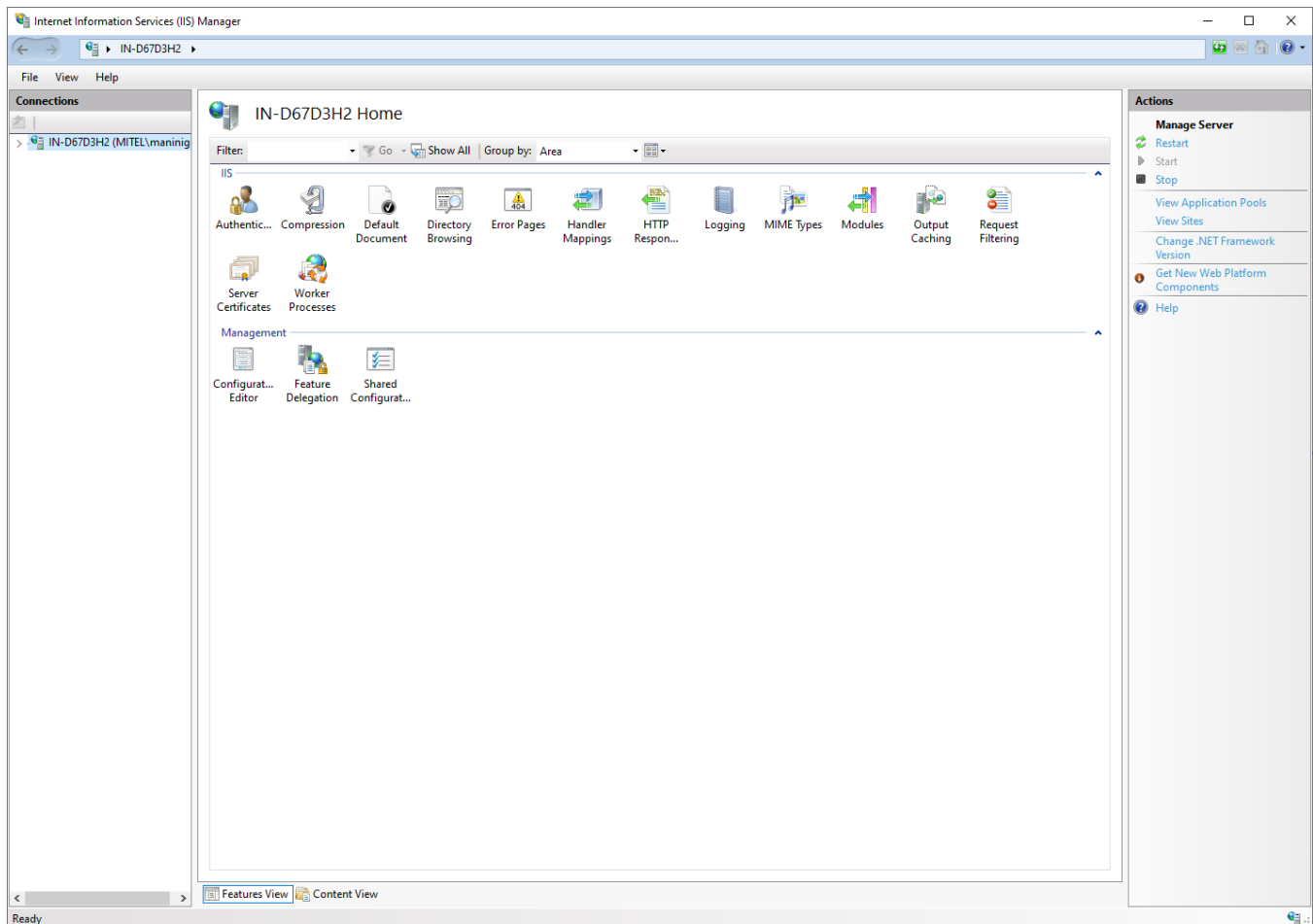
NOTE: If you set up an HTTPS server as a custom repository, then a valid Root CA certificate must be installed through the **Certificate Authority Trust** tab in **Security > Web Server** in the Server Manager.

This section provides instructions for setting up an HTTP service in Microsoft Internet Information Services (IIS). For setting up an HTTPS service in IIS, refer to related Microsoft documentation.

Before you begin

Ensure that:

- Ensure that Microsoft Internet Information Services (IIS) is installed on your PC. To verify whether IIS is installed, click the **Start** button, and type **inetmgr** in the search field. If Internet Information Services (IIS) is installed, then the Internet Information Services (IIS) Manager window is displayed.

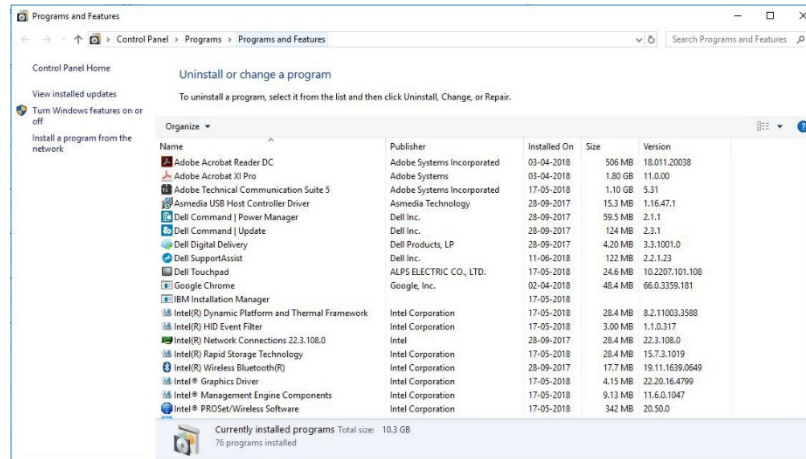


If IIS is not installed, see [Installing IIS](#).

- Ensure that you have downloaded the software zip file (For example, **MiVB_ppc_image_9.1.0.92.zip**) from the **Software Download Center** page on **Mitel MiAccess**.

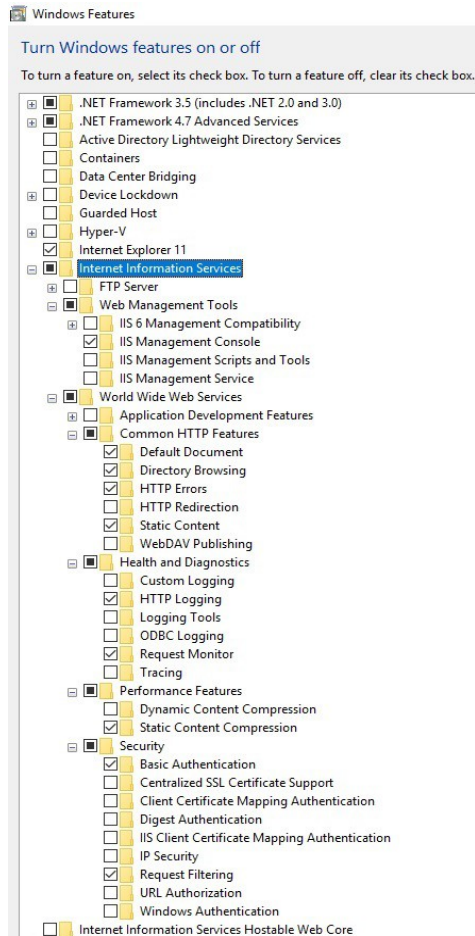
Installing IIS

1. Click the **Start** button on the Taskbar, type **appwiz.cpl** in the search field, and then press ENTER. The **Programs and Features** window is displayed.



2. Click **Turn Windows features on or off**.

The **Windows Features** window is displayed.



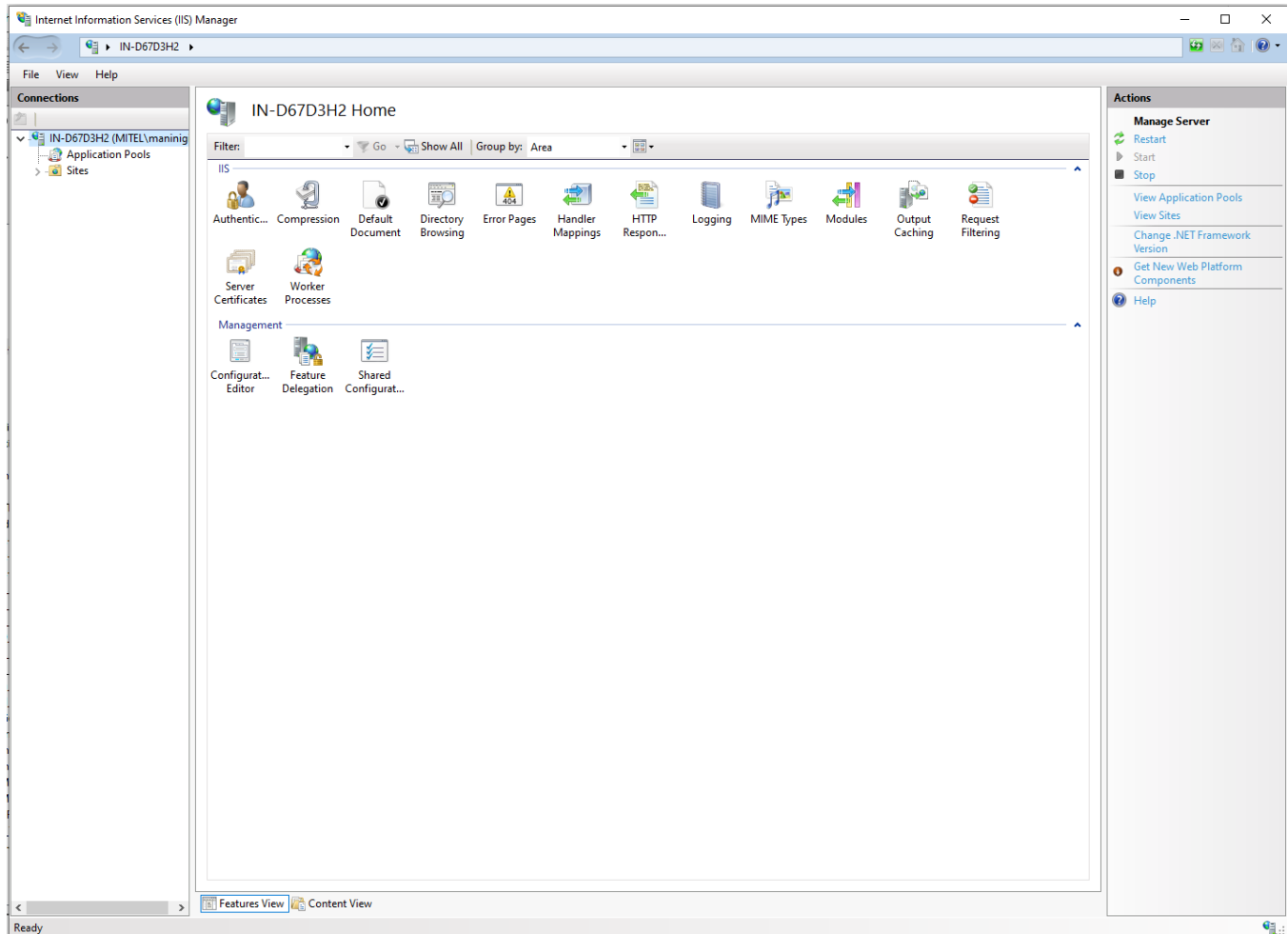
3. Expand Internet Information Services, and select the following check boxes:

- Web Management Tools
 - IIS Management Console
- World Wide Web Services
 - Common HTTP Features
- Default Document
- Directory Browsing
- HTTP Errors
- Static Content
- Health and Diagnostics
 - HTTP Logging
 - Request Monitor
- Performance Features
 - Static Content Compression
- Security
 - Basic Authentication
 - Request Filtering

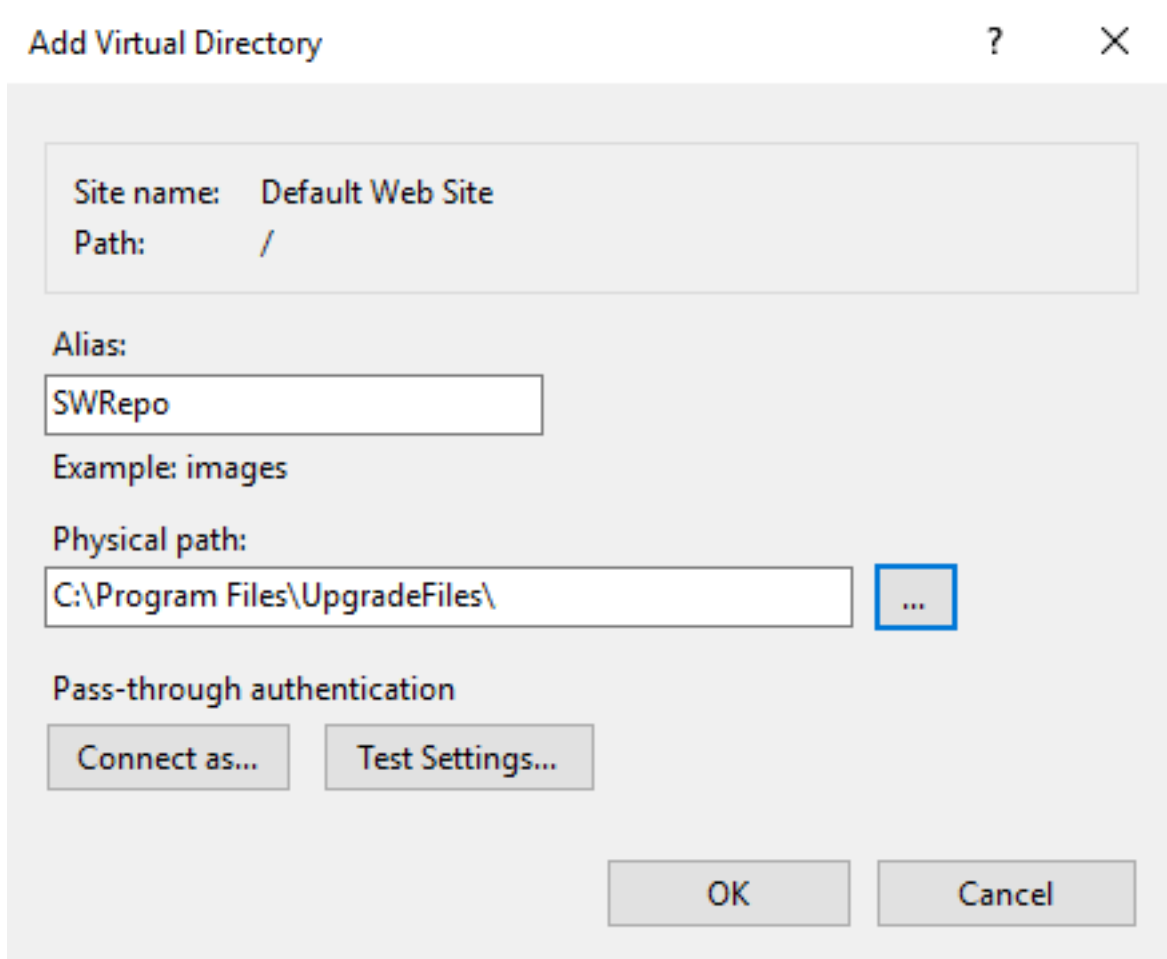
4. Click **OK** to install IIS.

Setting up an HTTP Repository

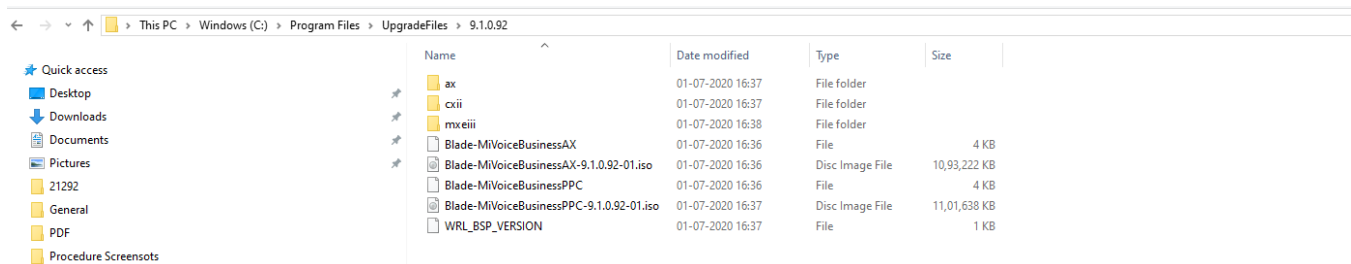
1. Click the **Start** button on the Taskbar, enter **inetmgr** in the search field, and then press ENTER. The Internet Information Services (IIS) Manager window is displayed.
2. In the **Connections** pane, double-click the first entry (usually your PC name).



3. Double-click the **Sites** folder to expand it.
4. Right-click **Default Web Site**, and then click **Add Virtual Directory**. The **Add Virtual Directory** window is displayed.



5. In the **Alias** field, enter a name for the virtual directory (for example, **SWRepo**).
6. In the **Physical path** field, enter the physical path directory that will contain the software (for example, C:\Program Files\UpgradeFiles\).
7. Unzip the software zip file (For example, **MiVB_ppc_image_9.1.0.92.zip**) to the folder specified in the **Physical path** field.



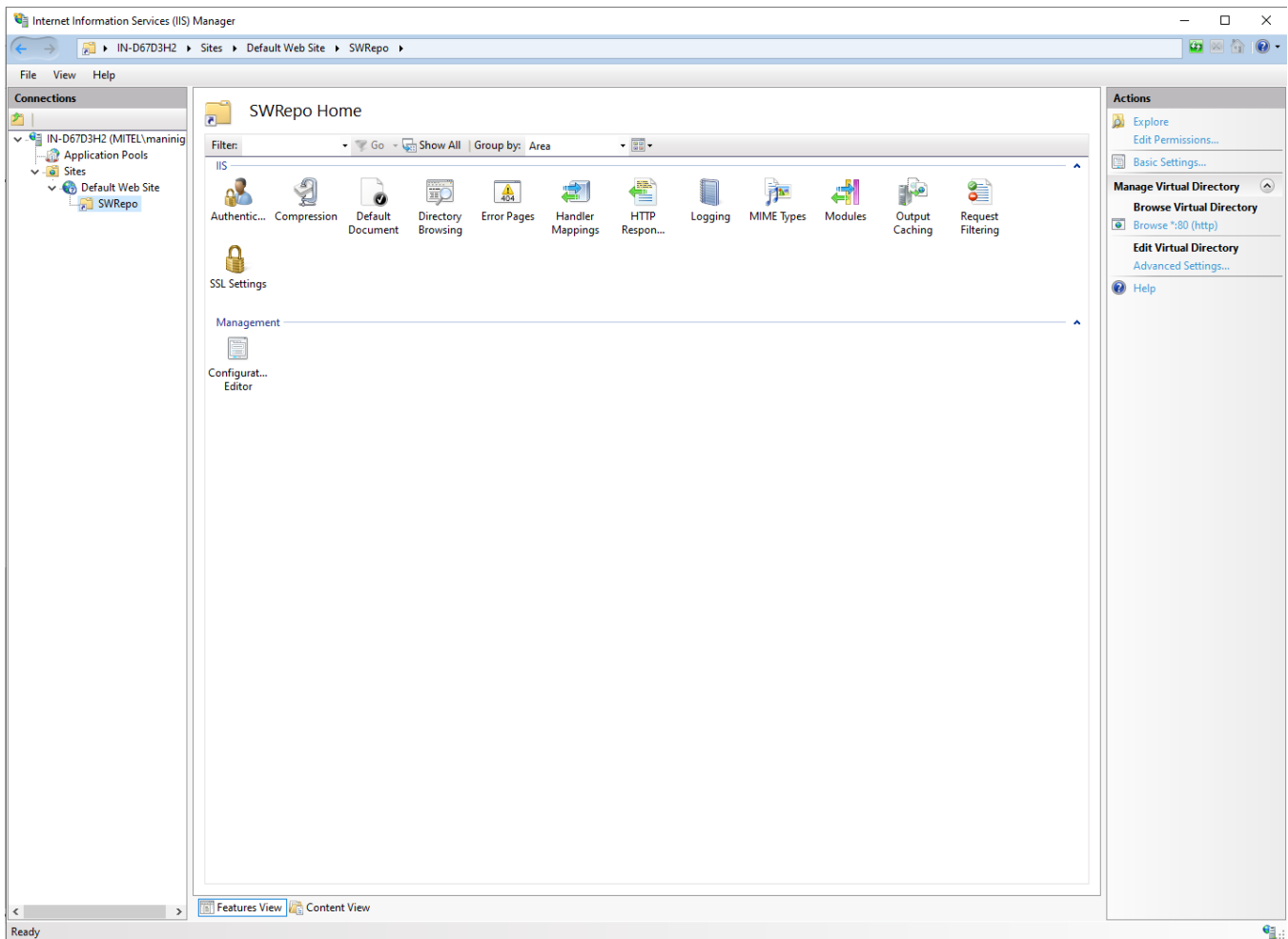
NOTE: Unzipping the software zip file causes extraction of the software to a folder named **X.X.X.XXX** (where X.X.X.XXX is the software version).

8. Click **OK**.

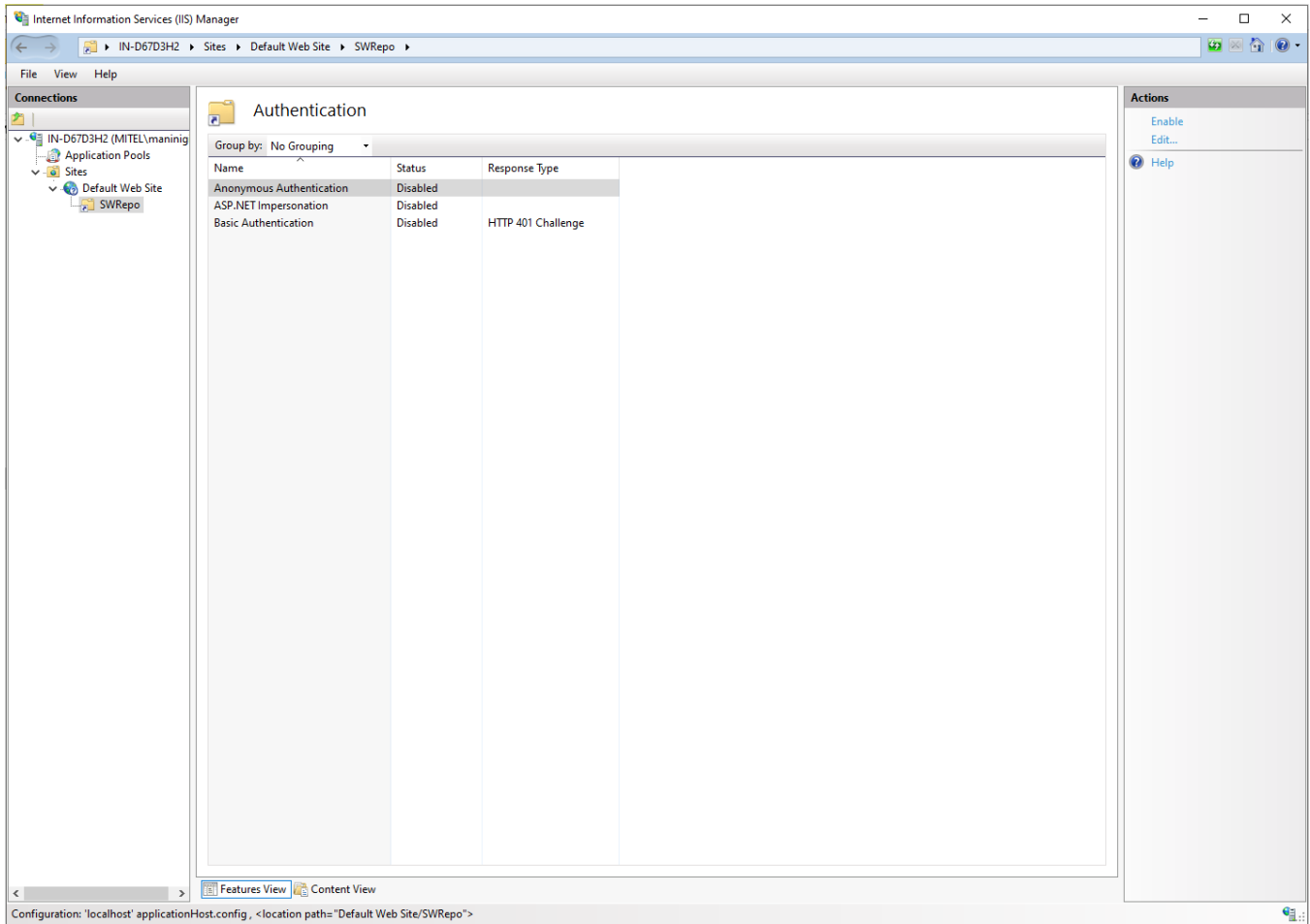
The virtual directory that you created is displayed under **Default Web Site** in the **Connections** panel.

9. Double-click the virtual directory that you created.

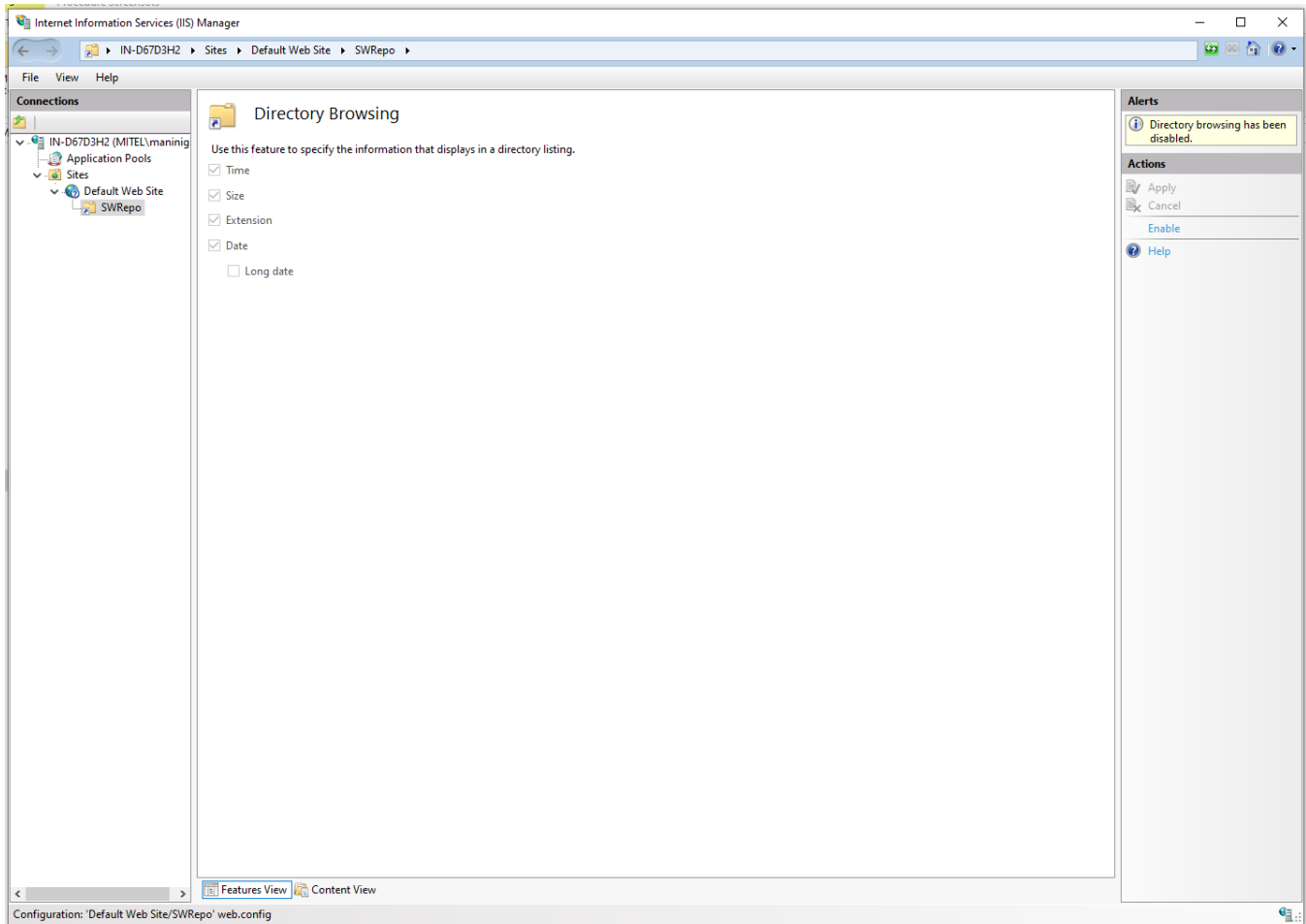
The virtual directory Home is displayed on the main screen of the window.



10. Double-click **Authentication**, select **Anonymous Authentication**, and click **Enable** in the **Actions** pane.



11. In the **Connections** pane, double-click the virtual directory you created. The virtual directory Home is displayed on the main screen of the window.
12. Double-click **Directory Browsing**, and click **Enable** in the **Actions** panel.

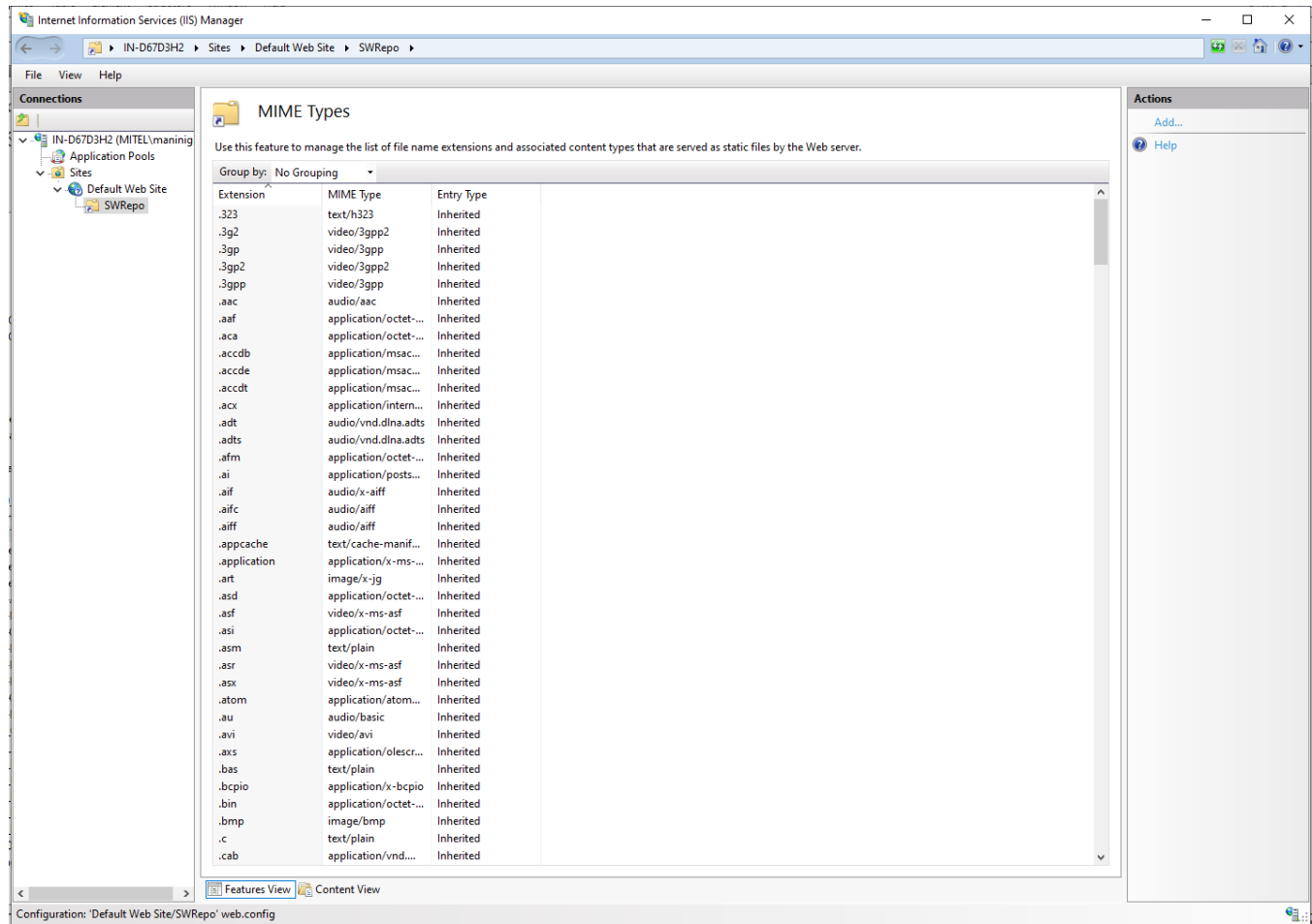


13. In the **Connections** panel, double-click the virtual directory (SWRepo) you created in Step 5.

The virtual directory Home is displayed on the main screen of the window.

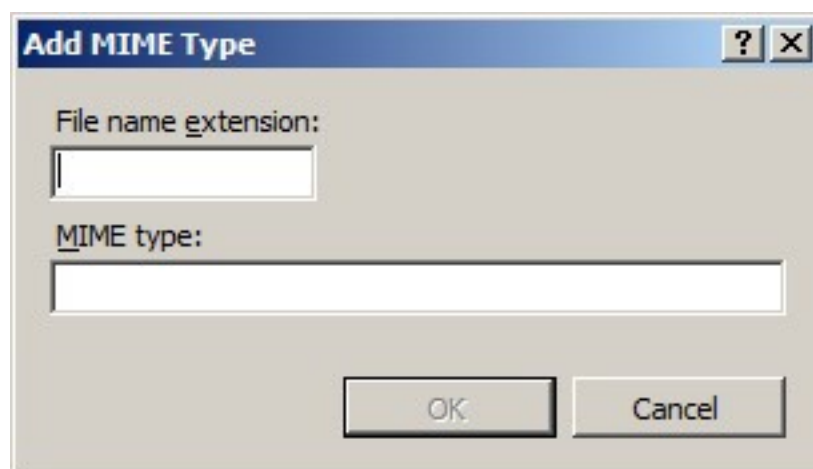
14. Double-click MIME Types on the main screen.

The MIME Types is displayed on the main screen of the window.



15. Click **Add** in the **Actions** panel.

The **Add MIME Type** dialog box is displayed.



16. In the **File name extension** field, type **.md5**.

17. In the **MIME type** field, type **text/plain**.

18. Click **OK**.

The MIME type is added to the list of **MIME Types**.

19. Repeat steps 14 through 17 to add the following MIME types.

Table 17.1:File name extensions for MIME Types

File name extension	MIME type
. (files with no extension)	text/plain
.ax	text/plain
.bz2	application/bz2
.cxii	text/plain
.dtb	application/octet-stream
.iso	application/octet-stream
.map-ax	text/plain
.map-cxii	text/plain
.map-mxeiii	text/plain
.md5	text/plain
.mxeiii	text/plain
.s3	text/plain
.srec	text/plain
.txt	text/plain
.u-boot	application/x-gzip

20. To access the software using a browser, enter **http://<server IP address>/<virtual directory name>** in the address bar of your browser (for example, **http://10.35.83.83/SWRRepo/**).

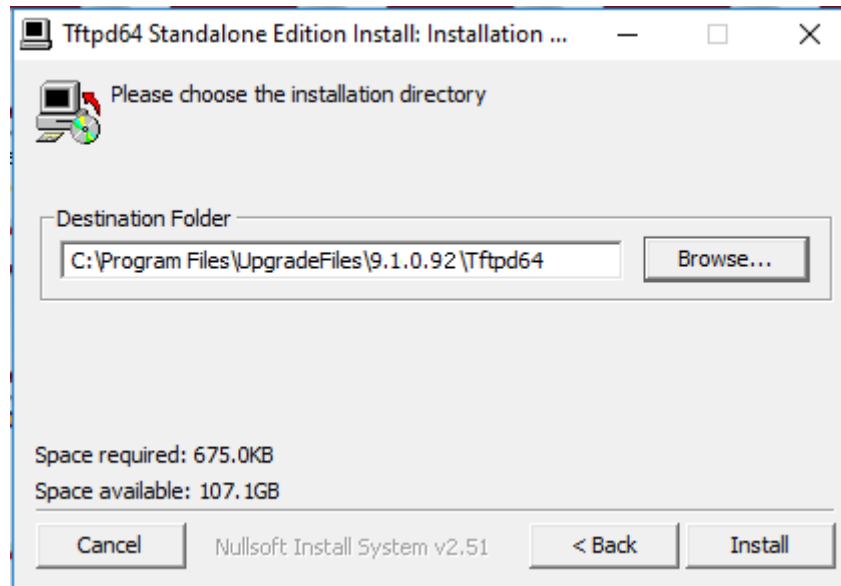


Set up a TFTP server and a custom repository

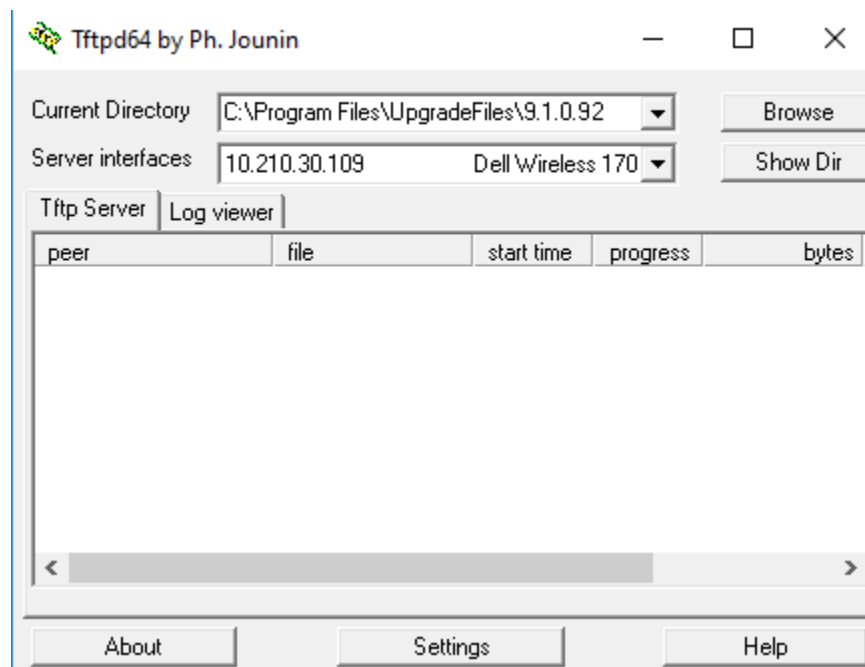
You can set up a TFTP repository on your local computer to host the Mitel's PPC Installer images.

1. Go to http://tftpd32.jounin.net/tftpd32_download.html and download the latest version of the TFTP service (**tftpd64 installer**).
2. Double-click the downloaded file, and double-click **Tftpd64-4.62-setup** to install the TFTP service.

Ensure that the **Destination Folder** is the same as the **Physical path** of the HTTP service you installed earlier (see Step 6 in Set up an HTTP Server and a Custom Repository).



3. After installation is successfully completed, double-click the **tftpd64 application** file in the **Tftpd64** folder to launch the TFTP service.
4. In the **Current Directory** field, enter the folder path of the installed TFTP service; this is also the folder path to the TFTP repository.



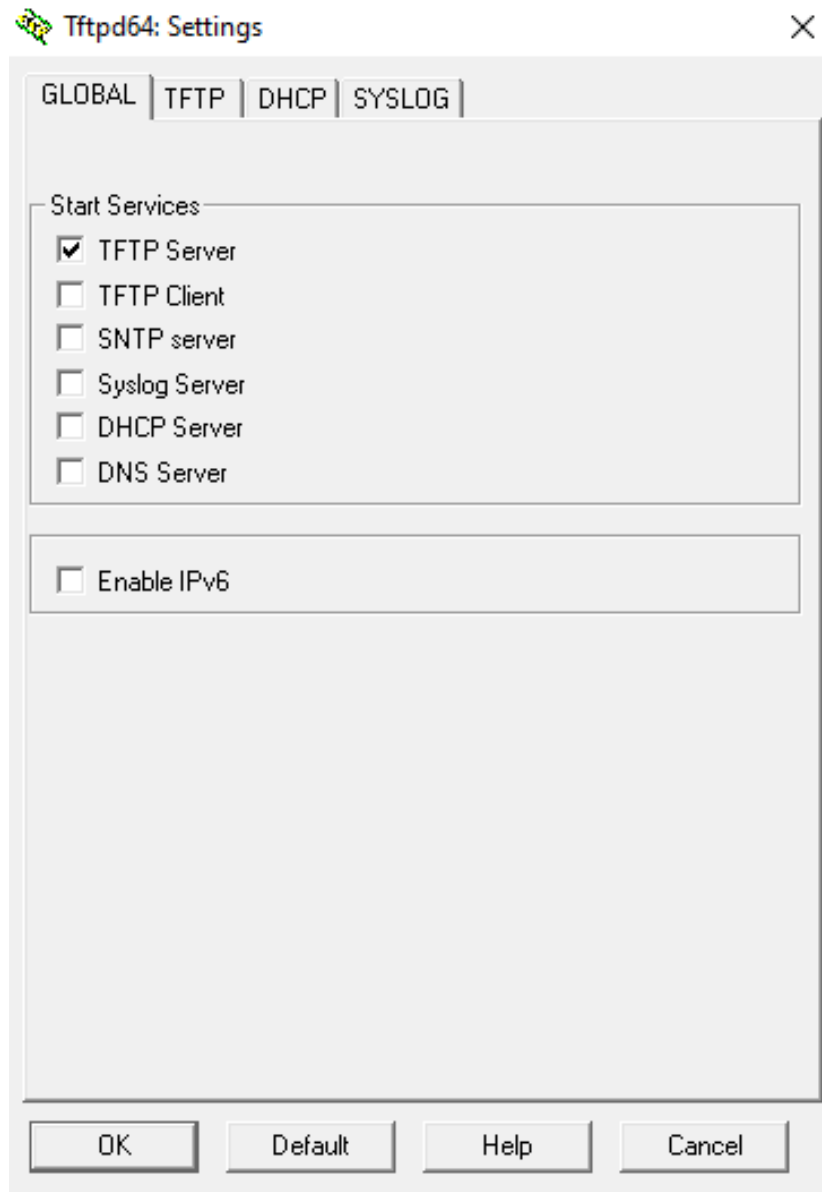
The Server interfaces field automatically fills in the IP address of your computer system, which is also the IP address of the TFTP server.

5. Click the **Settings** button.

The **Tftpd64** window opens.

6. Under the TFTP tab, enter the folder path of the installed TFTP service in the **Base Directory** field.

- Under the **Global** tab, ensure that the **TFTP Server** option is selected in the **Start Services** section.



- Under the **Syslog** tab, enable logging by selecting the **Save syslog messages** option and specifying the location where you want to save the logs.

