

# MiVoice Business

Troubleshooting Guide

RELEASE 9.3

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](mailto: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

<b>Chapter: 1</b>	<b>Introduction . . . . .</b>	<b>1</b>
	About this Guide . . . . .	1
	What's new . . . . .	1
	Supporting Documentation . . . . .	2
	Accessing Mitel Documentation . . . . .	2
	Mitel Product Documentation . . . . .	2
	Product Bulletins . . . . .	2
	Mitel Knowledge Base Articles . . . . .	2
	Resolving Technical Issues . . . . .	2
	TSN Your Technical Support Network . . . . .	6
	What Services are Available . . . . .	7
	What Products are Supported . . . . .	8
	Registering for Services . . . . .	8
	Self Help Solutions . . . . .	9
	Checking the Knowledge Base . . . . .	9
	Using the Online Service Desk OSD . . . . .	9
	Checking for Fixes in Software Patches . . . . .	9
	Fixed in Latest Software Patch? . . . . .	10
	Fixed in Previous Software Patch? . . . . .	10
	Fixed in Software Update? . . . . .	10
	Accessing Product Support . . . . .	11
	Before You Call . . . . .	11
	Making a Support Call . . . . .	16
	What are Normal Business Hours? . . . . .	16
	What are After-Hours Calls? . . . . .	16
	Returning Faulty Hardware . . . . .	17
 <b>Chapter: 2</b>	 <b>Initial Setup . . . . .</b>	 <b>18</b>
	Initial Setup Troubleshooting Tips . . . . .	18
	Licensing . . . . .	21
 <b>Chapter: 3</b>	 <b>Hardware . . . . .</b>	 <b>24</b>

---

Hardware Troubleshooting Tips . . . . .	.24
Hardware Alarms . . . . .	.25
Controllers . . . . .	.28
MXe III/MXe III-L Controller . . . . .	.28
3300 ICP Controllers . . . . .	.30
Service Units . . . . .	.34
Embedded Modules . . . . .	.35
Phones . . . . .	.38
General Phone Issues . . . . .	.38
Issues with Specific Models . . . . .	.47
IP Phone Power . . . . .	.56
IP Phone Registration . . . . .	.58
Phone Connection . . . . .	.66
Phone Audio Quality . . . . .	.69
5550 IP Console . . . . .	.74

## Chapter: 4

## Software . . . . . 76

Software Troubleshooting Tips . . . . .	.76
---	-----

System Software . . . . .	.76
---------------------------	-----

Unable to boot the MiVoice Business System on 3300 ICP Controller . . . . .	.81
---	-----

Overview . . . . .	.81
--------------------	-----

Recover the system through the Server Manager . . . . .	.82
---	-----

Recover the System through SSH . . . . .	.82
--	-----

Overview . . . . .	.82
--------------------	-----

Procedure . . . . .	.82
---------------------	-----

Recover the System through the Maintenance Port . . . . .	.83
---	-----

Overview . . . . .	.83
--------------------	-----

Before you begin . . . . .	.83
----------------------------	-----

Procedure . . . . .	.83
---------------------	-----

Password Recovery for 3300 ICP Controller . . . . .	.85
---	-----

Overview . . . . .	.85
--------------------	-----

Before you Begin . . . . .	.85
----------------------------	-----

Procedure . . . . .	.85
---------------------	-----

Unable to Recover the MiVoice Business System from Active and Inactive . . . . .	
--	--

Partitions . . . . .	.86
----------------------	-----

Reset the VoiceAdmin Password . . . . .	.86
---	-----

Overview . . . . .	.86
--------------------	-----

Procedure . . . . .	.86
---------------------	-----

Reset the System Admin Password . . . . .	.87
---	-----

Overview . . . . .	.87
--------------------	-----

Procedure . . . . .	.87
---------------------	-----

Backups and Restores . . . . .	.87
--------------------------------	-----

Determine whether there is enough space for backup . . . . .	.91
--	-----

Migration . . . . .	.92
---------------------	-----

Reverse Migration . . . . .	.92
-----------------------------	-----

Reverse Migration of an AX Controller if the 16 GB CF is Unavailable or . . . . .	
---	--

---

	Corrupt . . . . .	92
	U-Boot based E2T card in MxIII cannot boot E2T8260 Image after Reverse Migration . . . . .	93
Migration . . . . .	U-Boot based E2T card in MxIII cannot boot E2T8260 Image after Reverse Migration . . . . .	95
<b>Chapter: 5</b>	<b>System Features . . . . .</b>	<b>97</b>
	System Features Troubleshooting Tips . . . . .	97
	Features A to B . . . . .	97
	Features C . . . . .	100
	Features D to G . . . . .	106
	Features H to K . . . . .	110
	Features L to O . . . . .	112
	Features P to R . . . . .	115
	Features S to V . . . . .	116
<b>Chapter: 6</b>	<b>Trunking . . . . .</b>	<b>118</b>
	Trunk Troubleshooting Tips . . . . .	118
	Analog Trunks . . . . .	118
	Digital Trunks . . . . .	121
	MSDN DPNSS Links . . . . .	130
	Direct IP RoutingDirect IP RoutingTroubleshooting Symptom Probable Cause Corrective ActionIncoming calls failFaulty configuration of trunk Forms.Ensure that the Direct IP Route used to provision IP trunks between MiVoice Business system is configured correctly.Verify the IP Networking Programming using the Direct IP Route method. For more detail see System Administration Tool Online Help. 133	
	IP Trunking (IP Networking) . . . . .	139
	SIP Trunking . . . . .	140
<b>Chapter: 7</b>	<b>Tools and Embedded Applications . . . . .</b>	<b>141</b>
	System Management Tools . . . . .	141
	Automatic Call Distribution . . . . .	151
	Hot Desking . . . . .	151
	Emergency Call E911 Support . . . . .	153
	Troubleshooting MiVB Next Generation 911 (NG911) with Red Sky 153	
	Dialing 911 Does Not Work . . . . .	154
	PSAP Does Not Receive Accurate Information . . . . .	154
	Gathering Information . . . . .	155
	Next Steps . . . . .	155
	Embedded Voice Mail . . . . .	156
	Networked Voice Mail . . . . .	163
	Station Message Detail Recording . . . . .	165
<b>Chapter: 8</b>	<b>Voice Networking . . . . .</b>	<b>167</b>

---



---

Setting the Phone Mode . . . . .	218
Using Tools and Features . . . . .	218
IEEE 802.1X Authentication for IP Phones . . . . .	220
Configuring an Authentication Username and Password . . . . .	220
Erasing an Authentication Username and Password . . . . .	221
Enabling or Disabling 802 1X Authentication . . . . .	221
IP Phone Boot Sequence . . . . .	222
Checking the IP Phone Resiliency Progress Display . . . . .	226
Diagnosing SIP Device Issues . . . . .	227
Dialing from Aastra SIP DECT handsets . . . . .	228
Trunks . . . . .	228
Diagnosing Digital Trunk Issues . . . . .	228
Hardware . . . . .	230
Using LEDs to Diagnose Faults . . . . .	230
Reading E2T Card Statistics . . . . .	230
Diagnosing DSP Module Related Issues . . . . .	233
Diagnosing MSDN DPNSS Link Problems . . . . .	233
Loopback Testing on Digital Trunks . . . . .	233
Resiliency . . . . .	234
Locating Resilient Devices . . . . .	234
Locate Extension . . . . .	235
Locate Feature . . . . .	236
Locate Remote . . . . .	237
Locating Resilient Hunt Groups . . . . .	238
Identifying the Status of a Resilient Device . . . . .	239
State Extension . . . . .	239
State XNET ICP . . . . .	240
Obtaining the Status of Resilient Trunks . . . . .	240
Controlling the Failover and Failback of Resilient Trunks . . . . .	240
Identifying the Current ICP . . . . .	240
Checking T1/E1 Resiliency Alarms . . . . .	241
Checking the T1/E1 Combo MMC Indicators . . . . .	241

## Chapter: 11

<b>Using Logs . . . . .</b>	<b>244</b>
Logs . . . . .	244
Software Logs for System Features . . . . .	244
Hot Desking Error Logs . . . . .	245
Voice Mail System Logs . . . . .	246

---

# Introduction

## About this Guide

This guide provides troubleshooting information for the Mitel® 3300 IP Communications Platform (ICP). This guide is intended for use by Mitel certified 3300 ICP technicians.

The troubleshooting information has been grouped by topic (Initial Setup, System Features, Devices, and so forth) and then organized into tables using the following structure:

- Symptom,
- Probable Cause, and
- Corrective Action.

To locate help on a specific problem

- Use the Adobe Acrobat search functionality to search for key words associated with the problem symptoms, or
- Go to the table that contains troubleshooting information related to the problem and scan the symptoms column for a possible match.

**NOTE:** The AX controller will be supported in MiVoice Business Release 9.1 and later versions.

## What's new

**Table 1.1:** Issue 1.0

Feature/Enhancement	Description	Location
General updates	Updated: The flowchart for resolving technical issues. <ul style="list-style-type: none"><li>• Steps for accessing MiACCESS.</li><li>• The TSIS ID to MiACCESS ID.</li><li>• Technical Support contact number.</li></ul> Removed: <ul style="list-style-type: none"><li>• Details about credit check.</li><li>• E-mail notification of new and updated TBs and RNs.</li></ul>	



# Supporting Documentation

This guide references other documents that are available on Document Center.

## Accessing Mitel Documentation

### Mitel Product Documentation

To access the product documentation:

1. Go to <https://www.mitel.com/document-center>.
2. Click **BUSINESS PHONE SYSTEMS > MIVOICE BUSINESS**.

### Product Bulletins

To access Mitel Product Bulletins:

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

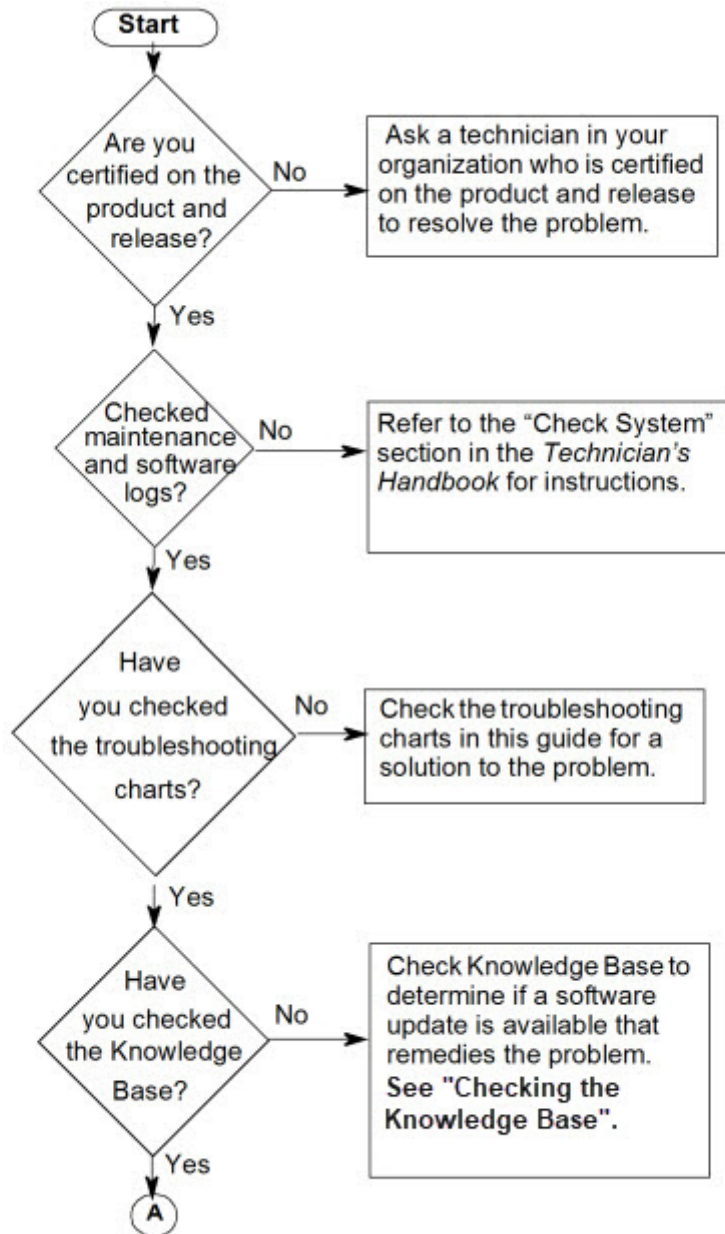
### Mitel Knowledge Base Articles

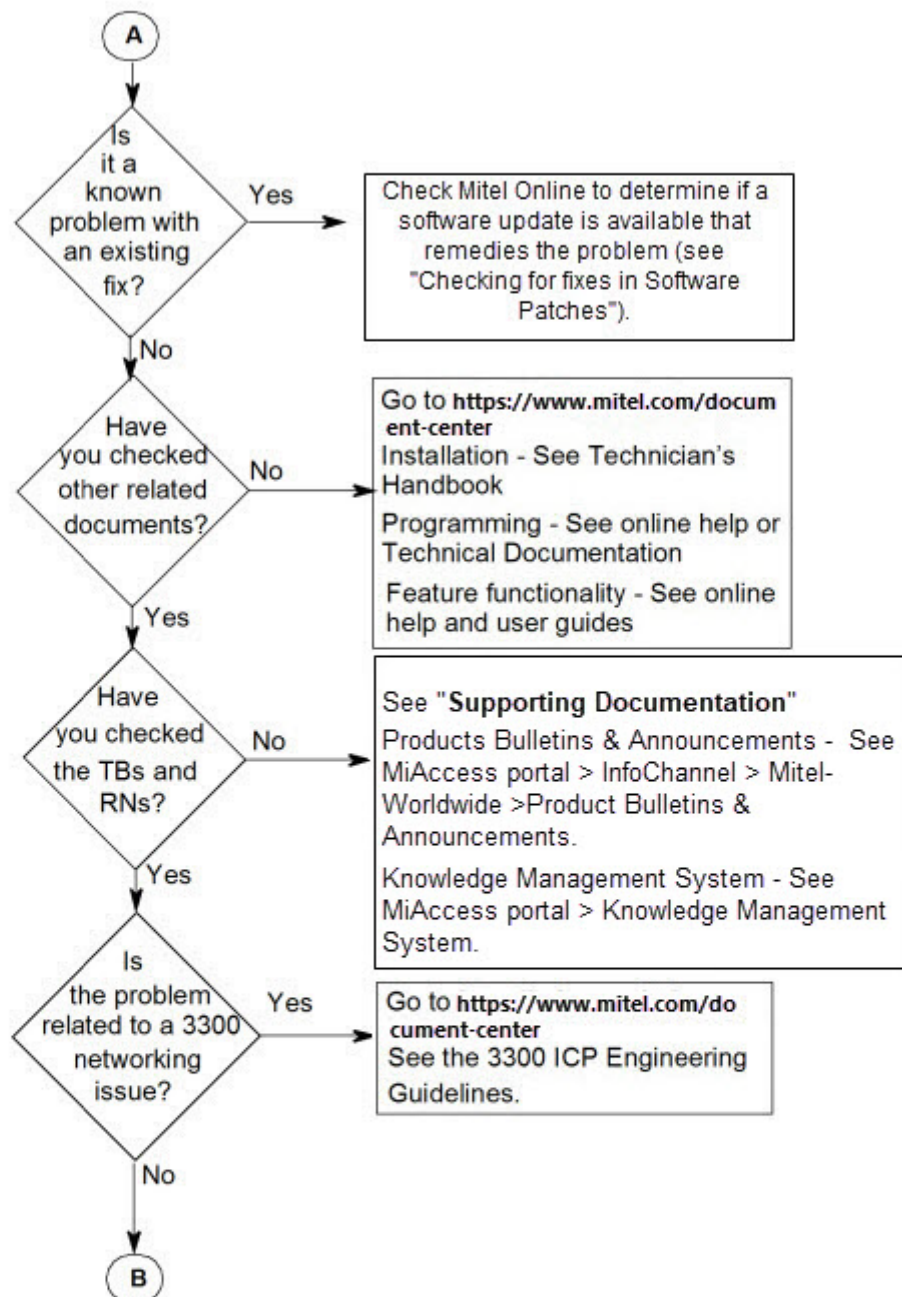
To access Mitel Knowledge Base Article:

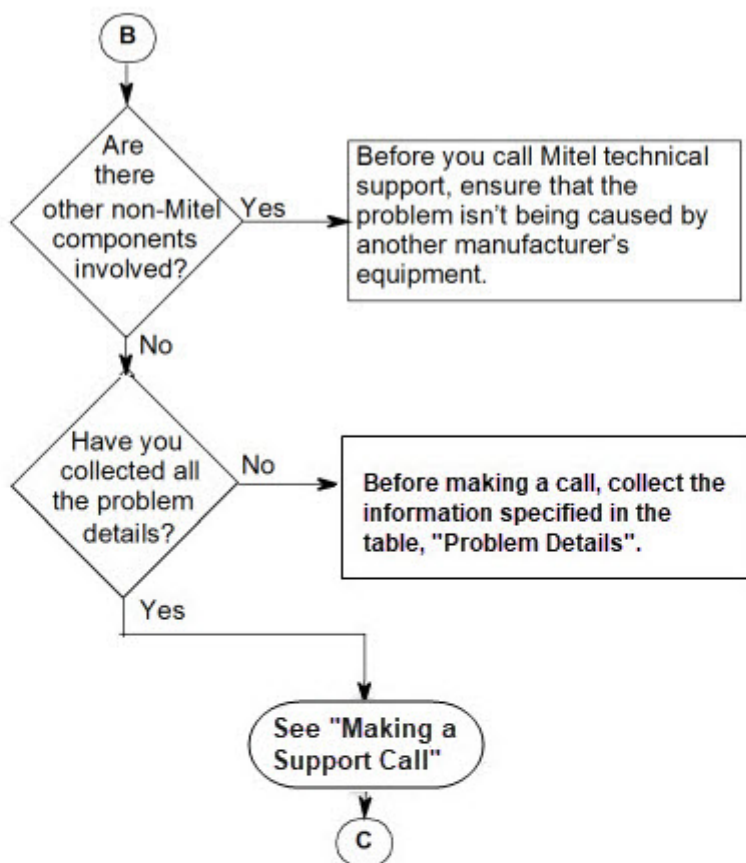
1. Log on to [MiACCESS](#) Portal.
2. In the left pane, click **Knowledge Management System**.

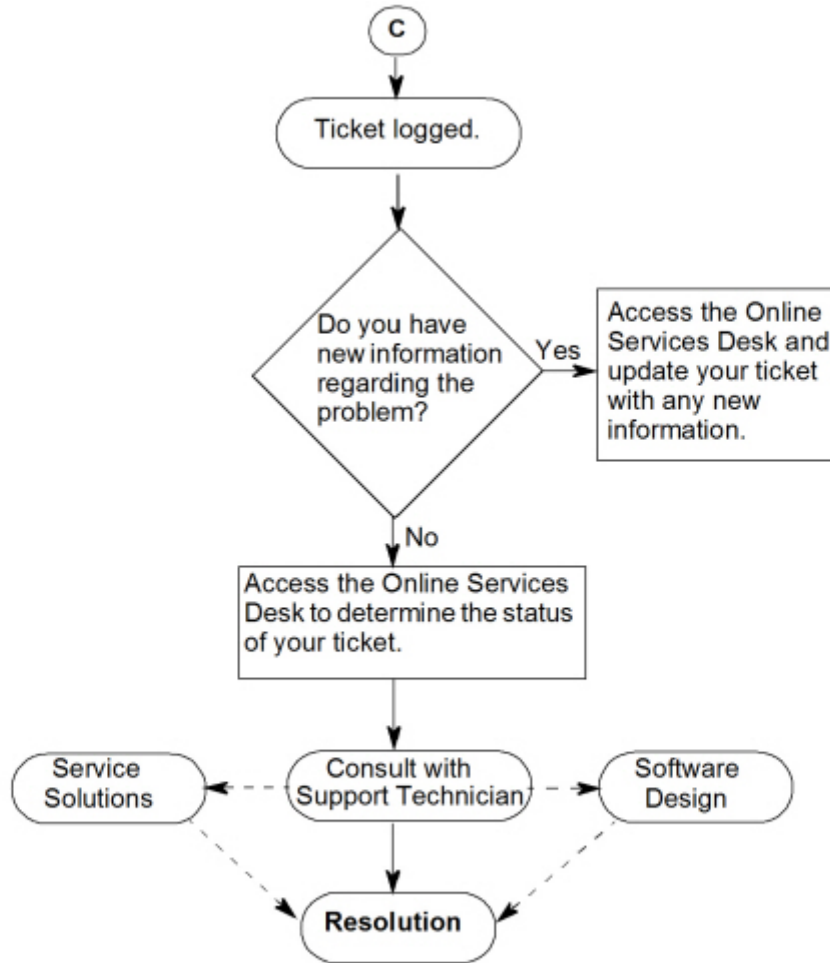
## Resolving Technical Issues

Use the following flowchart to resolve technical issues:









## TSN Your Technical Support Network

The Mitel Technical Support Network (TSN) provides authorized channel partners with the following services:

- access through the Mitel OnLine website to
  - up-to-date customer documentation
  - the Mitel Knowledge Base
  - the Online Service Desk (OSD) allowing you to view and update your Technical Support Tickets
- standard telephone support with current product releases during normal business hours
- after-hours emergency telephone support
- e-mail notification of new and updated technical documentation.

Before you can become a registered user, you must purchase a minimum of five technical consultation credits. Your technical consultation credits can be used to purchase telephone support (standard and emergency).

**NOTE:** If you have questions about the Technical Support Network Program or your access to Technical Support, please call 1-800-722-1301, option 5-0 or e-mail your question to [tsn@mitel.com](mailto:tsn@mitel.com).

**NOTE:** Online Service Desk (OSD) response time is three business days. The OSD should not be used to obtain emergency support services.

## What Services are Available

- **Mitel Knowledge Base:** provides access through the Mitel Online website to the latest product information. The Knowledge base provides
  - *Technical Bulletins (TBs):* Provide information on the installation and service of Mitel products. TBs are issued to introduce new software support tools, provide support information on discontinued products, identify product issues and describe TSN program policies. TBs are published when required.
  - *How to Articles:* Provide information on proper programming of features and applications
  - *Troubleshooting Articles:* Provide troubleshooting procedures to help identify and solve issues.
  - *Known Product Issues:* Describe product issues that are known by Mitel and are in the process of being resolved.
  - *Release Notes (RNs):* Provide software upgrade procedures, describe documentation and hardware requirements, summarize the new enhancements in a release, identify improvements that have been made in the product in response to customer reported issues, and include last-minute product changes that are not described in the latest documentation. RNs are published for each new software release.
- **Standard telephone support:** Allows certified channel partner technicians to consult Mitel Network's Technical Support Specialists on current products during normal business hours. For details see [Making a Support Call](#).
- **After-hours emergency telephone support:** Outside of normal business hours, certified technicians can consult with a Technical Support Specialist or a Support Manager for assistance with resolving an emergency situation or with restoring service for an essential services site. See [What are After-Hours Calls?](#) for details.
- **Online Service Desk (OSD):** Allows you to view the status of your active Technical Support Tickets and your technical credit statement. Whenever changes are submitted against your account, you will be sent a confirmation email. To register for OSD notification updates, log into Mitel OnLine, click Technical, and then click **Register/Cancel Email Notifications**.
- **Password Resets:** If you lose your password or if your password is not available, follow the below steps:
  - a. Login to [MiACCESS](#).
  - b. Navigate to **InfoChannel** from the left panel. A new tab is displayed.
  - c. Select **Mitel - Worldwide** from the drop-down options.
  - d. Scroll down and navigate to **Services and Support > Support Services > Technical Support**. A list of Technical Support documents will be displayed on the screen.
  - e. Click **System Password Resets** to reset the password.
- **Software Releases:** You can download the latest product software releases from Mitel Online. To access the available software downloads on Mitel Online, login to [MiACCESS](#) and then click on **Software Download Center**.

- **Software Patches:** Between major releases, you can download major system software patches from Mitel OnLine that include fixes for field-found problems (see [Checking for Fixes in Software Patches](#)). Note that minor software patches are only available from Technical Support via a Mitel FTP site.
- **Replacement of failed (out-of-box) system:** If a system fails within the first 72 hours of service it will be replaced by Mitel. Direct requests for replacement of failed systems to Mitel Customer Service Group. Replacements of defective software, complete systems, or three or more components of a system must be authorized by Mitel Technical Support.

## What Products are Supported

For an up-to-date list of the products that are supported, follow the below steps:

1. Login to [MiACCESS](#).
2. Navigate to **InfoChannel** from the left panel. A new tab is displayed.
3. Select **Mitel - Worldwide** from the drop-down options.
4. Scroll down and navigate to **Services and Support > Support Services > Technical Support** A list of Technical Support documents will be displayed on screen.
5. Click **Technical Support (TS) Guide and Quick Reference Guides**.

Telephone support falls into one of the following categories:

**Current Products:** Telephone support is provided at no charge during normal business hours to Mitel certified technicians for the currently supported products.

**Manufactured Discontinued - Supported:** Telephone support is chargeable for the manufacture discontinued products.

**Manufactured Discontinued - Unsupported:** Telephone support is not available for manufactured discontinued products. Access to all existing technical support bulletins for these products remains available through Mitel Online.

## Registering for Services

To register for access to TSN services

1. Complete a Technical Consultation Order form and fax the form to Mitel Customer Services at 613-591-2308.
2. After the Mitel Customer Services receives your purchase order, we will fax a MiAccess ID to the fax number that you included with your order form.
3. Distribute the MiAccess ID to staff who require access to TSN services, including staff that may need to call Mitel Technical Support.

**NOTE:** Change your MiAccess ID whenever you experience staff turnovers. You can change your MiAccess ID at any time by contacting the Mitel TSN Coordinator: Phone: 1-800-722-1301, option 5-0 E-mail: [tsn@mitel.com](mailto:tsn@mitel.com)

4. Instruct your staff to obtain a Mitel OnLine username and password by submitting a request online. All requests are confirmed with the designated channel partner. After a request is confirmed, a username and password is e-mailed to the individual.



5. Instruct your staff to register for the Online Service Desk. From Mitel OnLine, click **Technical Support**, then click **Online Service Desk** under Related Links. Complete and submit the form. Registrations will be processed within 2 business days (a return e-mail will confirm activation).

## Self Help Solutions

### Checking the Knowledge Base

The Knowledge Base is your source for product information covering a large range of technical support methods. All new Technical Bulletins (TBs), Release Notes (RNs), How to Guides and Troubleshooting guides will be posted in the Knowledge Base. Access to the Knowledge Base is given with access to MOL.

To access the Knowledge Base:

1. Log into [MiACCESS](#).
2. Navigate to **Knowledge Management System** from the left panel.
3. Enter the name, ID or any key word of the document you are searching for in the search field and click on the search icon.

### Using the Online Service Desk OSD

The Online Service Desk provides up-to-date information on your Support Notifications and Technical Credit balance. This portal lets you view the status of your open tickets, update Support Notifications with new information for our technical support team, and check your technical credit usage. Once the issue has been resolved your ticket will be updated. OSD will automatically display all active support notifications when you log in.

To access the Online Service Desk:

1. Log into [MiACCESS](#).
2. Navigate to **TechCentral Tracker** from the left panel.
3. When you log in for the first time, you will be asked for your MiAccess ID.
4. Choose your channel partner location.
5. View your open and closed tickets.
6. Update your open tickets with any new information and the Mitel technical support specialist will be notified of your updates by e-mail.

**NOTE:** Online Service Desk (OSD) response time is three business days. The OSD should not be used to obtain emergency support services.

7. Display a summary of your technical credits (depending on your access privileges).

### Checking for Fixes in Software Patches

Before calling technical support with a problem, check to see if there is a software update available on Mitel Online that includes a fix for the problem.

- Major software patches are provided on Mitel Online.



- Minor software updates are available from Technical Support via a Mitel FTP site. The Known Product Issue (KPI) fixes that are contained in minor software updates are listed in the “KPI fixed lists” articles. The “KPI fixed lists” are Mitel Knowledge Base articles.

If an update is available with the required fix, you can download the software patch or update and install it on the system.

### Fixed in Latest Software Patch?

To determine if a fix for your problem is available in the latest software patch:

1. Log into MiACCESS PORTAL.
2. Click **Software Downloads**.
3. Click the product name (for example, 3300 Integrated Communications Platform).
4. Click the latest software update.
5. Open the Release Notes (RN).
6. In the RN, review the list of problems that are resolved in this software update. If your required fix is listed, read the RN carefully to ensure that the update is appropriate, download the update, and then install it on the system. See the *Technician's Handbook* for software installation instructions.

### Fixed in Previous Software Patch?

If the software version on your system is a few releases old, the fix may have been provided in a previous software patch. To check the problems that have been fixed in previous software patches

1. Log into Mitel OnLine.
2. From Mitel OnLine, click **Technical**, and then click **Knowledge Base**.
3. Select the product name (for example, 3300 Integrated Communications Platform).
4. Set the Article Type to Release Notes (RN) and then click **Start Search**.
5. Open the RNs that have been issued since the release of your system's current software and check the list of problems that have been fixed.
6. If you find a fix to your problem, download and install the latest software patch. See the *Technician's Handbook* for software installation instructions.

### Fixed in Software Update?

To determine if a problem has been fixed in a minor software update:

1. Log into Mitel OnLine.
2. From Mitel OnLine, click **Technical**, and then click **Knowledge Base**.
3. Select the product name (for example, 3300 Integrated Communications Platform).
4. Enter “KPI” and then click **Start Search**.
5. Open and review the Known Product Issues (KPI) fixed lists.
6. If you find a fix to your problem, contact Technical Support to obtain the software update.

# Accessing Product Support

## Before You Call

1. Are you certified on the product in question?
2. Have you searched the tables in this Troubleshooting Guide for a solution?
3. Have you checked the Mitel Customer Documentation site, Knowledge Base and training materials for a solution to the issue?
4. Is the product supported (see [What Products are Supported?](#))?
5. Do you have your valid MiAccess ID at hand?
6. Are you calling within normal business hours or after hours? See [What are Normal Business Hours?](#) and [What are After-Hours Calls?](#)
7. Is it an emergency call? See Emergency Calls are Not Charged.
8. Have you collected the following information?

**Table 1.2:** Problem Details (Sheet 1 of 3)

Required Information	Details
Site information	Name, address, and phone number of end-user site
Product	What system or application is exhibiting the problem? What is the system or application variant (for example: 3300 ICP MxIII or MiVoice Business Virtual)?
Country variant	What country variant is selected for the controller?
Software version	What software version is the system running (for example, MCD Release 4.2 (10.2.2.10))?
System Identifier or Hardware Identifier	SysID code of system, and the ARID.
Serial number(s)	Serial numbers of the hardware and software.
System platform	If the problem involves a Mitel application that runs on a PC or server, what is the platform operating system, and what service packs, security software, firewall software, and browser version are installed?
Grounding	What grounding schemes are being employed for all Mitel equipment?

**Table 1.2:** Problem Details (Continued) (Sheet 2 of 3)

Required Information	Details
Problem symptoms	<p>Detailed description of the problem symptoms. What is the problem? When did the problem first appear? Have you made any changes to the system programming, hardware configuration or network setup that coincide with the appearance of the problem? Does the problem occur sporadically or only under specific conditions?</p> <p>Try to narrow the scope of the problem down as much as possible. For example, if the system is dropping calls, are only IP Phone to IP Phone calls affected? TDM to TDM calls? IP to TDM calls? or TDM to trunk calls?</p>
Troubleshooting steps	<p>What troubleshooting steps have you taken? Have you been able to eliminate any possible causes of the problem?</p>
Call scenarios	<p>Is the problem occurring between IP to IP devices, IP and remote IP devices, remote IP to IP devices, IP to TDM devices, and so forth?</p>
Network configuration	<p>Do you have a network diagram available?</p> <ul style="list-style-type: none"> <li>• What is the DHCP configuration and settings in the network?</li> <li>• IP Addressing scheme?</li> <li>• VLAN configuration and settings?</li> <li>• Layer 2 switch configuration and settings</li> <li>• Layer 2 switch port statistics for FCS, collision, and duplex mismatch</li> <li>• Router configuration and settings. Is there a common denominator (router, only one side of subnet, etc.)?</li> </ul>
LED status	<p>If hardware, for example a controller or NSU, is affected, what is the status of the LEDs?</p>

**Table 1.2:** Problem Details (Continued) (Sheet 3 of 3)

Required Information	Details
Maintenance and software logs	<p>Collect the logs associated with the problem. For example, collect errors on the maintenance port of the NSU.</p> <p>Collect the Alarm log details.</p> <p>On 3300 ICP systems, generate the system diagnostic report. (The PSTSWLOG and XRTC logs are included.)</p> <p>See MKB article 04-1000-00011 for instructions. The Mitel Knowledge Base article explains how to collect specific logs if ESM cannot be accessed.</p>
Phone types	<p>What type of phones are on the system? Is there a specific phone type that is exhibiting the problem? What is the firmware version?</p>
Trunking	<p>What types of trunks (PRI, BRI, LS, DID, XNET/IP, and so forth) are on the system?</p> <p>How are trunk groups set up?</p> <p>How are the LS trunk descriptors programmed?</p>
FAX Support	<p>What type of fax machines are installed? What is their make and model number?</p> <p>Are you using T.38 for faxing? Do the fax calls go over any IP connection, IP trunks or SIP?</p>
Contact telephone number and e-mail address	<p>Be prepared to provide the Mitel Technical Support technician with a telephone number and e-mail address so that the technician can contact you or provide your contact number to other support specialists. If your call concerns an emergency problem, ensure that you can be reached at the telephone number at any time. Don't provide a number that will forward the technician to voice mail. Don't provide a cell phone number that is likely to be unreachable (out-of-range).</p>

9. If the problem is with an IP Phone, have you collected the following information?

**Table 1.3:** IP Phone Information (Sheet 1 of 3)

Question	Answer	Comment
Is there a PC attached to the IP Phone?		If yes, please have the Network Interface Card (NIC) settings of the PC ready. It is recommended that NO power saving options and NO flow control options be enabled.
Have there been broadcast storms?		You can observe a broadcast storm using a packet analyzer (sniffer). A packet analyzer intercepts and logs packet traffic passing over a network.
Is your cabling CAT 5 or better?		CAT 5 or better is recommended for Ethernet connections. Cat 5e is required for 1Gig connections.
Do your L2 or L3 switch statistics show any issues such as Runts, etc.?		Runs/Collision/Frame error may indicate an issue with NIC or a duplex mismatch.
What is the L2 port setting for IP phone and controller?		For IP phones, we recommend access ports that can handle both tagged and untagged packets to and from specific VLANs.
How is the IP phone powered? Power over Ethernet (PoE) or from a power adaptor (transformer) that is plugged into a power outlet.		If powered over Ethernet which L2 PoE switch is being used?
Does your L2 switch have CDP enabled, spanning tree enabled, or Port Fast enabled?		None
What is your speed setting? (10/100, Full/Half, Auto, Fixed?)		None

**Table 1.3:** IP Phone Information (Continued) (Sheet 2 of 3)

Question	Answer	Comment
Do the symptoms improve if the IP phone is set to “auto and lock”?		For controllers, we recommend Access Port. Mitel recommends setting “Auto” on phones. In some unique PC/network, the IP phone may require to hard coding or setting to “auto and lock” mode.
Do the symptoms appear in hands free mode only or do they also occur via the handset?		None
Are you using a headset? What type? What make and model?  Is the problem only seen when using the headset?		
Do you have the assert information from the debug (Configuration) menu?		Assert value is saved in the debug mode and reports the last reason that the phone rebooted.
What type of phones are you using (for example 5330, 5340)? How many display phones are connected to the system? Do any of the phones have PC applications associated with them?		These factors affect system performance.
Is there a pattern? For example, does the problem follow the phone? Can you ping the IP phone?		None.
Have you noted any display information?		None.
Have you tried increasing keepAlives up to 1 minute via the System Administration tool registry entries?		None
Do you have a complex network (for example, multiple nodes and or sites)?		If yes, a network topology diagram is required.

**Table 1.3:** IP Phone Information (Continued) (Sheet 3 of 3)

Question	Answer	Comment
Can you obtain a packet capture via a packet analyzer (sniffer) at the phone level?		Packet capture helps Technical Support to analyze the state of the network and the condition of the phone.
Can you obtain an IP Phone Analysis (IPA) for the phone in question?		IPA provides crucial information about how the phone is reacting.

## Making a Support Call

1. Ensure that you have collected as much information as possible (see [Accessing Product Support](#)).
2. If possible, establish local or remote access to the system (for example, the 3300 System Administration Tool) that you require support for before you call.
3. Call Mitel Technical Support:
  - If you are in North America, you can reach Technical Support at 1800-722-1301 or 1613-592-2122.
  - If you are in any other region, contact your local regional support service. For regional contact information, follow the below steps:
    - i. Login to [MiACCESS](#).
    - ii. Navigate to **InfoChannel** from the left panel. A new tab is displayed.
    - iii. Select **Mitel - Worldwide** from the drop-down options.
    - iv. Scroll down and navigate to **Services and Support > Support Services > Technical Support**. A list of Technical Support documents will be displayed on the screen.
    - v. Click **Contacting Mitel Technical Support**.
4. Describe the nature of the problem to the technician.
5. Record your problem ticket information.

## What are Normal Business Hours?

- 8:30 am EST to 5:00 pm LOCAL time (local to North American customer site), Monday to Friday, excluding public holidays.

## What are After-Hours Calls?

- Calls originating outside normal business hours (See the TSN Guide for details).
- For example, for customers in the Eastern Time Zone, “after-hours” is defined as 5:00 pm to 8:30 am Monday to Friday, and all day Saturday and Sunday.
  - CAUTION:** Mitel Technical Support will not provide password resets or changes to system options during after-hours support.
  - NOTE:** After hours calls are charged at a higher rate.

## Returning Faulty Hardware

Any Field Replaceable Unit (FRU) that is found to be faulty must be returned with a repair tag containing the following information:

- The date the device is returned
- The site where the unit was installed
- The company name
- The product name
- The system serial number
- The software revision
- The assembly part number of the item being returned
- The assembly serial number of the item being returned (this is a white sticker located on the card itself)
- Any pertinent alarm/error displays. This may include circuit alarm LEDs, console or main-tenance error messages, or maintenance log messages.
- A brief description of the symptoms of the problem.
- Indicate whether the fault occurred during installation, or while the system was in service.
- Any further information that may be useful should be included on the rear of the repair tag.



# Initial Setup

## Initial Setup Troubleshooting Tips

- Refer to the Technician's Handbook for instructions on how to install and set up a 3300 ICP controller.
- For hardware related issues, also see [Controllers](#).

**Table 2.1:** General Controller Setup Troubleshooting (Sheet 1 of 4)

Symptom	Possible Cause	Corrective Action
Unable to access the console screen.	You are replacing an existing 3300 ICP controller with another controller, and trying to use the same system IP address for the new controller from a PC on a different subnet.	Initially, you can only connect to the controller from the local subnet. Before you can connect to the new controller from other subnets, you must manually clear the router ARP cache or wait until the router ARP cache is automatically updated. Refer to the latest 3300 ICP Release Notes for instructions.
Controller not powering up.	Power cable is not securely plugged into the controller and/or power source.	Ensure power cable connections are secure.
	The power switch or both power switches on a redundant power supply controller are not on.	Ensure power switch or both power switches on a redundant power supply controller are turned on.

**Table 2.1:** General Controller Setup Troubleshooting (Continued) (Sheet 2 of 4)

Symptom	Possible Cause	Corrective Action
Unable to establish communication with controller via maintenance PC	Controller has not finished starting up.	The controller can take up to 15 minutes to start up.
	PC communication application (for example VT 100 emulator program) serial port settings incorrect.	See “Connect to PC” in the “Initial Setup” chapter of the <i>Technician’s Handbook</i> for correct settings.
	Crossover Ethernet cable used to PC to controller.	Use a straight-through Ethernet cable.
	PC Network Interface Card IP address not programmed.	Program the PC’s NIC with the following settings: <ul style="list-style-type: none"> <li>IP Address: <b>192.168.1.n</b> (where n is a value between 30 and 254)</li> <li>Subnet Mask: <b>255.255.255.0</b></li> </ul>
	Maintenance PC on different subnet.	Configure maintenance PC on same the same subnet as controller.
	IP address and subnet mask for RTC entered incorrectly.	Enter IP addresses without leading zeros. For example, 192.168.1.2; not 192.168.001.002

**Table 2.1:** General Controller Setup Troubleshooting (Continued) (Sheet 3 of 4)

Symptom	Possible Cause	Corrective Action
E2T does not come up even though the network settings have been programmed.	E2T was hard coded with an IP address and then later changed to request an IP address from the DHCP server. This change is made by changing the <b>flags (f)</b> parameter in the bootline of the E2T from <b>0x0</b> (hardcode) to <b>0x40</b> (DHCP). If <b>any</b> IP addresses remain on the E2T (at “inet on ethernet”, “host inet” or “gateway inet”), the E2T will use them and will obtain the rest of its parameters from the DHCP server.	When changing the flag from 0x0 to 0x40 on E2T, ensure that you blank out ALL IP addresses in the bootline of E2T. Refer to “Programming the E2T via a Debug Cable or Secure Telnet” in the Technician’s Handbook.
	RTC is set up with a different virtual LAN (vlan).	For 9.0 releases, on the Linux shell enter: <b>mcdDebug vlan_off</b> Then log into ESM, <b>System Administration Tool &gt; Lan/WAN Configuration &gt; L2 Switch</b> On this form set VLAN ID to 1. For 9.1 releases and onward, on the Linux shell enter: <b>mcdDebug vlan_reset</b> The E2T VLAN is reset when, the system restarted. If the E2T still fails to boot, on the Linux shell enter: <b>e2tcardConsoleStart</b> The E2T VLAN is reset when the system is restarted. If the E2T still fails to boot, on the Linux shell enter: <b>e2tCardConsoleStart</b> Log into the E2T card as root and then set the VLAN to the proper value by performing one of the following two methods. If the E2T card cannot boot, enter the following command in U-boot: <b>setenv vlan x saveenv</b> If the E2T card does boot, but cannot load E2TLX, enter the following command from the Linux shell: <b>fw_setenv vlan x.</b>

**Table 2.1:** General Controller Setup Troubleshooting (Continued) (Sheet 4 of 4)

Symptom	Possible Cause	Corrective Action
After a new install, the internal DHCP server is not supplying addresses to IP devices.	Internal DHCP server is not activated.	The internal DHCP server is not activated by default. If your system relies on the internal DHCP server, you must enable the DHCP server using the DHCP form in the Server Manager.

## Licensing

For general AMC troubleshooting, also see the AMC Troubleshooting Guide. Refer to Mitel Knowledge Base Article HO1318.

**Table 2.2:** Troubleshooting Licensing and Optioning (Sheet 1 of 3)

Symptom	Possible Cause	Corrective Action
License and Option Selection error.	The System ID or i-Button has not been installed.	<p>Install the SysID module or I-Button. Verify that the I-Button can read. The I-Button hardware ID value is found in the System Administration Tool. Click <b>Licenses &gt; License and Option Selection</b> and look at the hardware ID. If the hardware ID is blank, there is a problem reading the I-Button. If you still can't fix the problem, call Technical Support. Make sure you have the following information on hand before calling:</p> <ul style="list-style-type: none"> <li>The error message(s) in the PostSoftware Logs and/or the journalctl logs.</li> </ul>

**Table 2.2:** Troubleshooting Licensing and Optioning (Continued) (Sheet 2 of 3)

Symptom	Possible Cause	Corrective Action
Unable to communicate with the Application Management Center (AMC).	<ul style="list-style-type: none"> <li>Inability to communicate with the AMC because unable to find the AMC servers via a DNS lookup.</li> <li>Inability to communicate with the AMC because of network/system configuration.</li> <li>Inability to communicate with the AMC using specific protocols or ports due to router or firewall configuration</li> </ul>	Refer to Mitel Knowledge Base Article HO1318.
Cannot move licenses after manual upgrade.	There is a specific procedure that you must follow to move licenses after a manual upgrade.	Refer to Mitel Knowledge Base Article 06-9999-00013.
The system is generating "Warning" license violation messages in maintenance logs and the ESM System Administration Tool (pop-ups and banner status messages).	<p>One of the following warning-level license violation events has occurred:</p> <ul style="list-style-type: none"> <li>Over Allocation</li> <li>Missing DLM</li> <li>Missing Application Group Member</li> <li>Core Package capability exceeded</li> <li>License Keys cannot be validated</li> <li>System ID mismatch</li> <li>SDS is off</li> <li>Duplicate System</li> <li>Multiple DLMs</li> <li>Failure of timely synchronization with AMC</li> <li>Application Group is in license violation mode</li> <li>"licensekeys" or "licensecert" file is corrupt or has been tampered with</li> </ul>	Correct the license violation event.

**Table 2.2:** Troubleshooting Licensing and Optioning (Continued) (Sheet 3 of 3)

Symptom	Possible Cause	Corrective Action
The system is generating “Minor” license violation messages in maintenance logs, alarms, and the ESM interface (pop-ups on multiple forms and banner status messages).	The “Warning” level license violation escalation timer has expired (2 days after the original event).	Correct the license violation event.
The system is generating “Major” license violation messages in maintenance logs, alarms, and the ESM interface (pop-ups on multiple forms and banner status messages).	The “Minor” level license violation escalation timer has expired (7 days after the original event) OR An attempt has been made to over-allocate a license that cannot be over-allocate (e.g. an ACD Active Agent license).	Correct the license violation event.
The system is generating “Critical” license violation messages in maintenance logs, alarms, the ESM interface (pop-ups on multiple forms and banner status messages), the Desktop Tool, and device displays.	The “Major” level license violation escalation timer has expired (14 days after the original event).	Correct the license violation event.
The system has reached “System Lock” license violation level and is generating a variety of error messages and alarms. In addition, the Desktop Tool is disabled and all sets except attendant consoles are placed in restricted service mode. Users can place emergency and attendant calls, and receive calls, but they cannot place regular outgoing calls.	The system is locked when an over-allocation violation is left uncorrected. For this to happen, the “Critical” level license violation escalation time must expire (36 days after the original event) provided either: <ul style="list-style-type: none"> <li>a number of licenses that have been over-allocated must exceed 5% of all purchased licenses.</li> <li>the system is a Virtual Controller that has not synchronized with the AMC for more than six months.</li> </ul>	Correct the license violation event.

# Hardware

## Hardware Troubleshooting Tips

- Only change one setting at a time (either a hardware or software setting).
- Observe carefully and document all observations (for example, feature programming, call states, time of day, problem symptoms and so forth).
- If all the functionality supported by a module or card is out of service, it is likely defective. If possible, swap the module or card with a known working module or card to confirm.
- Check the Alarm logs in the System Administration tool for hardware alarms.
- Check the LEDs on the hardware. Refer to “Appendix D: Status LEDs” in the *Technician’s Handbook* for LED state information.
- Verify that the IP addresses reserved for the hardware units are not used elsewhere on the system. See the “Installation Planner” chapter in the *Technician’s Handbook* for a list of the IP addresses that are reserved for the Analog Main Board (AMB), ASU and ASU IIs.
- For phone related issues, is the problem occurring
  - on a single phone?
  - on a group of phones of a specific type (for example IP Phones only)?
  - on a group of phones within a specific Class of Service only (indicates a potential programming conflict in COS Options form)?
  - during local-to-local calls only or local-to-external calls only?
- For phone or trunk related issues, if you don’t find the solution in this chapter, you should also check the troubleshooting tables in
  - Chapter 5: [System Features](#)
  - Chapter 6: [Trunking](#)
- Use the IP Phone Analyzer Tool to help you troubleshoot IP phone problems
- In the System Administration Tool use the following Maintenance and Diagnostic forms:
  - *Hardware Compute* form: displays details of the Real Time Controller (RTC) card and Ethernet-to-TDM (E2T) card
  - *Hardware Modules* form: displays the Mitel Mezzanine Card (MMC) modules that are installed in the system.
  - *IP Telephone* form: displays all IP phones in the system and their status.
- For help with *diagnosing* hardware problems, see [Hardware](#).
- For help with *diagnosing* phone hardware problems, see [Phones](#).

# Hardware Alarms

**Table 3.1:** Hardware Alarms Troubleshooting (Sheet 1 of 3)

Alarm	Probable Cause	Corrective Action
ICP Comms	E2T card has no IP address.	<p><b>If you are using the controller's internal DHCP server for the E2T:</b> ensure you assigned a static IP address to the E2T using the correct MAC address (see "Configure the Layer 2 Switch" in the "Initial Setup" chapter or the <i>Technician's Handbook</i> for instructions).</p> <p><b>If you are using an external DHCP server for the system:</b> verify that options are programmed correctly (see "Configuring External DHCP Settings for E2T" in the "Installation Planner" chapter of the <i>Technician's Handbook</i> for instructions).</p>
	Incorrectly programmed E2T IP address or incorrect setup of debug cable.	Verify that E2T parameters are correct (see "Programming E2T via Debug Cable or Secure Telnet" section of the <i>Technician's Handbook</i> for instructions).
	RTC is set up with a different virtual LAN (vlan).	<p>For 9.0 releases, on the Linux shell enter: <b>mcdDebug vlan_off</b> Then log into ESM, <b>System Administration Tool &gt; Lan/WAN Configuration &gt; L2 Switch</b>. On this form set VLAN ID to 1. For 9.1 releases and onward, on the Linux shell enter: <b>mcdDebug vlan_reset</b> The E2T VLAN is reset when the system is restarted. If the E2T still fails to boot, on the Linux shell enter: <b>e2tCardConsoleStart</b> Log into the E2T card as root and then set the VLAN to the proper value by performing one of the following two methods. If the E2T card cannot boot, enter the following command in U-boot: <b>setenv vlan x saveenv</b> If the E2T card does boot, but cannot load E2TLX, enter the following command from the Linux shell: <b>fw_setenv vlan x</b>.</p>



**Table 3.1:** Hardware Alarms Troubleshooting (Continued) (Sheet 2 of 3)

Alarm	Probable Cause	Corrective Action
	E2T card is defective.	Attempt to access the E2T serial port using the following procedure <i>Determine Bootloader of the E2T card</i> in <i>Technician's Manual</i> . The default baud rate should be 9600, but a card may have a baud rate of 115200. If nothing appears, then the E2T card is either not seated correctly or is defective.
DSP Status	A percentage of DSP resources are unavailable. The failure of one or more, but not all, DSPs results in a Minor alarm. Critical alarm indicates that all DSPs have failed. In the event of an alarm, reset the system as soon as possible. If the DSP continues to fail, replace the module.	Use the Show Status DSP maintenance command to identify status of DSPs in the controller. Install required DSP modules. See “Increasing DSP Resources” in the “Installation Planner” chapter of the Technician’s Handbook for instructions.
	DSP licenses are enabled but not enough DSP resources are available to support compression requirements	Install required DSP modules. See “Increasing DSP Resources” in the Installation Planner chapter of the Technician’s Handbook for instructions.
	Faulty circuit on DSP module	Replace DSP module.
DSP Card Status	DSP card is defective.	For a defective DSP module, ensure that the module is seated securely. For an embedded DSP failure, replace the controller. Use Show Status DSP to identify the location of the defective module.
Fan	Fan is defective	Replace the fan (see Note below).
One PSU	Power supply unit is defective (AX/MXe III).	Replace the PSU (see Note below).
Two PSU	Power supply unit is defective (AX/MXe III).	Replace the PSU (see Note below).

**Table 3.1:** Hardware Alarms Troubleshooting (Continued) (Sheet 3 of 3)

Alarm	Probable Cause	Corrective Action
RAID Hard Disk	Hard disk has a fault (MXe III).	If the alarm occurs on the primary drive, replace the hard disk (see Note below). Refer to Mitel Knowledge Base article HO1715. If the alarm occurs on the secondary drive, check the primary drive for faults. (In some cases, the primary drive has a sector error while the secondary drive is fault free.)
TDM Clock	Stratum 3 clock module in controller has failed.	Replace Stratum 3 clock module.
Temperature	Temperature in the system is getting too high.	System has overheated. Cool down system to clear alarm.
SFT Zones	System Fail Transfer zones have switched into SFT mode.	Determine cause for switch to SFT mode.
SYSID Mismatch	The System Identification module or i-button is not installed or is incorrect.	Install or replace System Identification module or i-button.

**NOTE:** Enter the **Show Status Redundant** maintenance command to identify the failed component. A minor Fan, Power Supply, or RAID alarm in the MXe III means that only one of the components has failed. A major alarm means that more than one component has failed. See the *Technician's Handbook* for hardware replacement procedures.

# Controllers

## MXe III/MXe III-L Controller

**Table 3.2:** MXe III Controller Troubleshooting (Sheet 1 of 2)

Symptom	Probable Cause	Corrective Action
E2T fails to initialize.	Changing from a hard coded E2T IP address to requesting one from the DHCP server. (If <b>any</b> IP addresses remain on the E2T (at “inet on ethernet”, “host inet”, or “gateway inet”), the E2T will use them and will obtain the rest of its parameters from the DHCP server.)	For information and guidance for correcting this problem, refer to "Programming E2T via Debug Cable or Secure Telnet" in the <i>Technician's Handbook</i> .
	RTC is set up with a different virtual LAN (vlan).	From the RTC shell or the E2T VxWorks shell, remove the vlan using the <b>cv</b> command.
	E2T card defective.	Check the Hardware Compute Cards form in the System Administration Tool. If the IP Address for Slot 2 displays “Not Responding”, replace the E2T card.
Unable to communicate with MXe III (not applicable to the MXe III-L controller)	You are attempting to use port 2 to access the MXe III controller but the Layer 2 IP address is not programmed.	Use port 1 to access the MXe III controller. Then launch the System Administration Tool and program the Layer 2 IP address.

**Table 3.2:** MXe III Controller Troubleshooting (Continued) (Sheet 2 of 2)

Symptom	Probable Cause	Corrective Action
Audio problems from IP to IP or IP to TDM.	E2T is unable to communicate with devices off its subnet.	If the problem is IP -> IP or IP -> TDM: Check the default gateway on all components involved in the call that is having audio problems. For example, you might see this issue when the following pairs are on different subnets: <ul style="list-style-type: none"><li>• E2T to E2T</li><li>• E2T to IP phone</li><li>• IP phone to IP phone</li></ul>

## 3300 ICP Controllers

**Table 3.3:** 3300 ICP Controllers Troubleshooting (Sheet 1 of 4)

Symptom	Probable Cause	Corrective Action
<p>There is no access to either Server Manager or System Administration Tool. If you connect putty to the maintenance port, you would observe the following message every time you press &lt;ENTER&gt; key: Give root password for maintenance (or press Control-D to continue): If you were monitoring the booting process via the maintenance port, you would observe the following message at the same time suggests the recovery actions: <i>The system is in emergency mode!</i> followed by the instructions for the corrective action, followed by <i>Give root password for maintenance (or press Control-D to continue):</i></p>	<p>The system has entered emergency mode. The possible reason for the system to enter the emergency mode are:</p> <ul style="list-style-type: none"> <li>The controller's iButton has its Real Time Clock set to a time behind the file system time.</li> <li>The controller gets flooded with network traffic while attempting to boot.</li> <li>One of the disk partitions has a corrupted file system.</li> <li>Other reasons</li> </ul>	<p><b>1.</b> In the serial console, press the ENTER key one or more times until the system displays the password prompt: Give root password for maintenance (or press Control-D to continue): <b>2.</b> Enter the password for the root user and press ENTER. If you have entered correct password, you shall get the following prompt: sh-4.3# <b>NOTE:</b> If the system is shipped from the factory or after a full manual installation, the default password is root. Pressing <b>CTRL + D</b> does not work. <b>NOTE:</b> If you do not know the password for the root user, then see <a href="#">Password Recovery for 3300 ICP Controller</a> <b>3.</b> Verify whether the iButton's Real Time Clock is in the past compared to the time of file-system timestamp by running the following two commands: date; hwclock -r ls --full-time /   grep sbin If the date and time of the <b>/sbin</b> directory is ahead, then it is most likely the reason that the system has entered the emergency mode. If the date and time are not the issue, proceed to step 4. You can also execute the following command to confirm that this service has failed ("Loaded:loaded" but "Active:failed") with the reason the <b>Superblock last mount time</b> for a partition <b>is in the future</b> compared to the current time: systemctl status --full systemd-fsck* If the current time is in the past, proceed with the next step to correct both the system time and the time in the RTC. If the current time is not in the past, it is possible that one of the disk partitions suffered a file system corruption; in this case contact Product Support for further instructions</p>

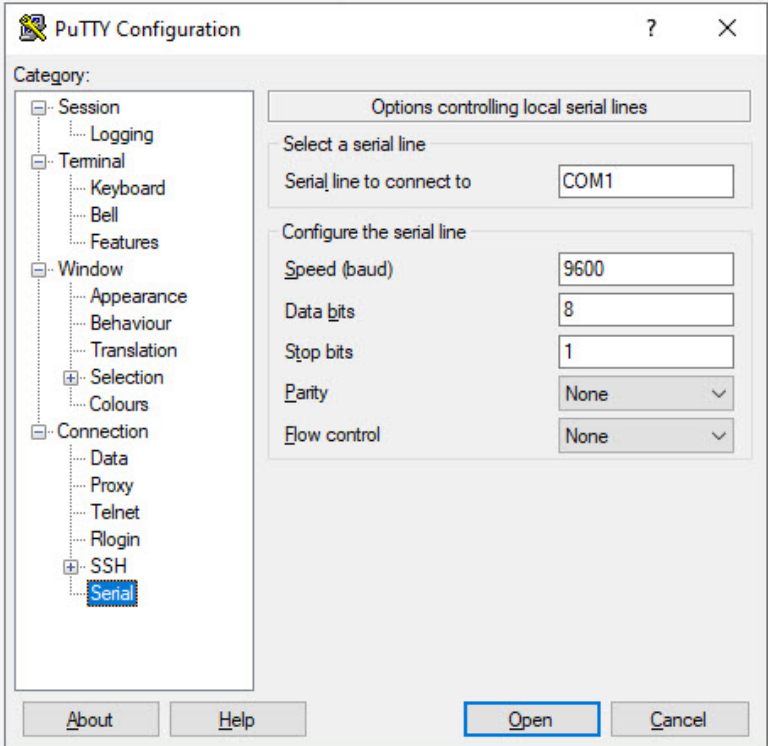
**Table 3.3:** 3300 ICP Controllers Troubleshooting (Continued) (Sheet 2 of 4)

Symptom	Probable Cause	Corrective Action
		<p><b>3.1</b> Run the following system commands from the serial console to set the system time and then transfer the system time to the H/W real time clock:</p> <pre>date -s 'HH:MM Month Date Year'</pre> <pre>hwclock -w</pre> <p>where HH:MM Month Date Year is the current date and time.</p> <p><b>For example:</b></p> <pre>date -s '12:19 April 20 2020'</pre> <pre>Mon Apr 20 12:19:00 UTC 2020</pre> <pre>hwclock -w</pre> <p><b>3.2</b> Verify that the commands were successful by running the following command:</p> <pre>date; hwclock -r</pre> <p><b>For example:</b></p> <pre>date; hwclock -r</pre> <pre>Mon Apr 20 12:19:20 UTC 2020</pre> <pre>Mon Apr 20 12:19:21 2020 0.000000 seconds</pre> <p><b>3.3</b> Reboot the system using the following command:</p> <pre>reboot</pre> <p>If the system now boots properly (or in the case of a fresh install gets you to the EULA screen on the serial port), it means that the issue has been resolved. After you log in to the Server Manager, go to the Date time panel and verify the date time settings and the time-zone. We recommend that you enable the Network Time Server if you have access to one.</p> <p><b>4.</b> Execute the <b>dmesg</b> command and analyze the output. If you see "sched: RT throttling activated" soon after "IP-Config: Complete", it means that the system is experiencing too much network traffic and is using too many CPU cycles to handle the network traffic. As a result, the startup of some system services times out, causing the system to enter emergency mode. For example, on AX platform you will observe messages such as "Timed out waiting for device dev-sda6.device" and/or "Timed out waiting for device dev-ttyCPM1.device". Monitor network traffic in order to identify which device is causing network flooding. Check whether the Synectix's serial to Ethernet adapter is pointing to your system. If it is, configure it such as it does not point to your system while it is booting. Upgrade the MiVB software to a release that has a fix for this issue.</p>

**Table 3.3:** 3300 ICP Controllers Troubleshooting (Continued) (Sheet 3 of 4)

Symptom	Probable Cause	Corrective Action
		<p><b>5.</b> If high network traffic or the iButton's Real Time Clock being in the past are not the issues, the possible cause is a file system corruption on a disc partition; most likely the vmal disc partition. Run the <code>fsck</code> command manually to fix the file system for the vmal disk partition. To do that, execute the following system command:</p> <ul style="list-style-type: none"> <li>if your system is CX(i)-II or MXe-III(-L) execute:  <code>fsck -y /dev/sda5</code></li> <li>if your system is AX, execute:  <code>fsck -y /dev/sda6</code></li> </ul> <p>After running the suggested commands, reboot the system using the following system command:</p> <pre>systemctl reboot</pre> <p>or</p> <pre>reboot</pre> <p>If the system now boots fully (or in the case of a fresh install gets you to the EULA screen on the serial port), it means that the issue has been resolved. After you log in to the Server Manager, go to the Date time panel and verify the date time settings and the time-zone. We recommend that you enable the Network Time Server if you have access to one.</p>

**Table 3.3:** 3300 ICP Controllers Troubleshooting (Continued) (Sheet 4 of 4)

Symptom	Probable Cause	Corrective Action
The serial port on the 3300 ICP controller is unresponsive while trying to access it using a terminal emulator application.	<ul style="list-style-type: none"> <li>Configuration issue with the terminal emulator application.</li> <li>Configuration issue with the terminal server, if the serial port is connected to the terminal server (for example LanTronix-SLC32).</li> <li>Hardware issue.</li> </ul>	<p>1. Ensure that the terminal emulator application connected to the controller's serial port through the DB9 serial cable is configured correctly as shown in the following figure.</p>  <p>2. If you have modified the default baud rate (9600), then set the baud rate to the recommended default value. See <b>Maintenance&gt; Modify Default Baud Rate of the System Console (3300 ICP Controller)</b> in the <i>Technician's Handbook</i>.</p> <p>3. If you are using a terminal server (for example, LANTronix SLC32) to access your controller's serial port remotely over the network, then verify that:</p> <ul style="list-style-type: none"> <li>the terminal emulator application has the correct terminal server's port and protocol configured.</li> <li>the terminal server port is configured correctly.</li> </ul> <p>4. Run the terminal server's configuration command for the terminal server port connected to the controller's serial port with the correct configuration values.</p>



## Service Units

**Table 3.4:** Service Unit Troubleshooting

Symptom	Probable Cause	Corrective Action
<b>Analog Service Unit</b>		
User can hear clicking sound while on a call on an external ASU ONS circuits.	Message Waiting voltage cycling.	Refer to Mitel Knowledge Base article 05-4409-00008.
Voice calls on ASU have an echo.	Faulty programming.	Ensure that the <b>ARS Call Progress Tone Detection form</b> for the analogue trunks is programmed correctly and ensure that the <b>Tone to Detect</b> entry is left blank (i.e. no tone to detect). If the <b>Tone To Detect</b> entry is set to detect a tone, it may cause echo.

## Embedded Modules

**Table 3.5:** Embedded Module Troubleshooting (Sheet 1 of 3)

Hardware	Symptom	Probable Cause	Corrective Action
Embedded PRI Module.	Embedded PRI Module fails to initialize. The LEDs on the embedded PRI (Framer) module are off. The trunks for the module are unassigned.	Module has failed to initialize because the link descriptor is not programmed correctly.	<p>Check the programming for the link descriptor that is assigned to the embedded PRI (Framer) module:</p> <p>For T1 only:</p> <ul style="list-style-type: none"> <li>• B8ZS Zero Code Suppression: Yes</li> <li>• Operation Mode: DSX-1 or CSU</li> <li>• CSU Tx Line Build-Out (dB.): This T1 parameter ensures reliable operation of the network. Select from 0, 7.5, 15, or 22.5 dB. Your carrier can advise you of the correct setting. The default is 0 dB.</li> <li>• DSX-1 Line Length (Ft.): 0-133 feet.</li> <li>• Extended Super Frame: No</li> <li>• Inverted D channel (DPNSS only): Yes</li> </ul> <p>For E1 only:</p> <ul style="list-style-type: none"> <li>• CRC-4 Enabled: “No” in North America; “Yes” in Europe</li> <li>• E1 Line Length (Ft.): 0-133</li> <li>• E1 Impedance (Ohms): 120</li> </ul> <p><b>NOTE:</b> For E1 only, 90% of E1 service providers in Europe require that you set the “CRC-4-Enabled” option to “Yes”. Please consult with your service providers for proper settings.</p> <p><b>NOTE:</b> For DASS/DPNSS (E1), set the “CRC-4 Enabled” option to “No”.</p>

**Table 3.5:** Embedded Module Troubleshooting (Continued) (Sheet 2 of 3)

Hardware	Symptom	Probable Cause	Corrective Action
Dual Framer (T1/E1) Module	After installing a Dual Framer (T1/E) module and programming a Digital Link Descriptor in the Digital Links form, the Framer module LED appears red. If you perform the STAT 7 1 2 maintenance command, the PLID shows “No card installed at requested slot”. (A loopback connector (Pins 1,2 to 4,5) will cause the LED to flash green.)	Protocol type not programmed.	After a digital link has been programmed, you must use the ISDN Protocol form to program the protocol type. System Configuration > Trunks > Digital Trunks > ISDN-PRI > T1 > Protocol Assignment As soon as a protocol is assigned a STAT of the card will show a valid state such as “not seizable”, or “idle”.
DSP card or module	Card fails to come out of reset.	Both PostSoftware and PostMaintenance logs are generated as well as a “DSP Card Status” alarm.	Disconnect controller power and then reconnect. Newer versions of DSPs have been updated to prevent this issue from occurring.

**Table 3.5:** Embedded Module Troubleshooting (Continued) (Sheet 3 of 3)

Hardware	Symptom	Probable Cause	Corrective Action
	DSP Fails to Boot.	No DSP resources. No dial tone on analog devices, embedded voice mail ports don't function, and so forth.	Remove and re-seat the card. Reboot. They should be looking at the connectors for bent pins etc. NOTE: Ensure that the screws are not over tightened! Over tightening of one side can cause the other side of the connector to rise up.
		PostSoftware Log: StartUp (BindId=0) pCOam->coDspBoot failed with: DSP_PROGRAM_ERROR for card: 3 and dsp: 0	If the problem persists, then remove/replace the card completely. This card only needs to be immediately replaced if it is the only card/DSPs being used for Telephony. If it was being used for Telephony, but there are still DSPs left in the system, this is still fine but the user may be traffic limited until it is replaced.
DSP Card or Module	DSP Run-Time Access Fault.	These are mostly exceptions that either produce an XRTC file or simply perform a hard reset on the system. These can occur at any point after the card has been taken out of reset but are considered separate from the Booting Process.	If the system is stuck in a reboot sequence. Remove and re-seat the card. Power on. They should be looking at the connectors for bent pins etc. NOTE: Ensure that the screws are not over tightened! Over tightening of one side can cause the other side of the connector to rise up. Obtain System Diagnostics Reporting output, or at a minimum, the XRTC and PostSoftware logs.
	DSP Overflow Error.	If these occur, the DSP will be taken out of service and a "DSP Status" alarm is raised.	If this happens, and it is a HW problem, it should be repeatable. Remove and re-seat the card. Power on. Look at the connectors for bent pins etc. NOTE: Ensure that the screws are not over tightened! Over tightening of one side can cause the other side of the connector to rise up.

# Phones

**NOTE:** IP phone troubleshooting tips also apply to the 5540 IP Console.

## General Phone Issues

**Table 3.6:** General Phone Troubleshooting (Sheet 1 of 9)

Phone	Symptom	Probable Cause	Corrective Action
Any	No calls are being received.	Programming error.	Check the <ul style="list-style-type: none"> <li>programming to make sure the calls are not forwarded or rerouted elsewhere automatically by the system.</li> <li>Class of Service Options Assignment to make sure the programming allows incoming calls.</li> </ul>
Any	Dial Tone at the set but user is unable to make calls	Programming in Class of Service or Class of Restriction forms are preventing calls	Check the following: <ul style="list-style-type: none"> <li>Establish if the extension being used is the one assigned to the user.</li> <li>Establish the type of calls the user is trying to make.</li> <li>Check the programming on the system for that extension. Look at the Class of Service and Class of Restriction Assignment in particular</li> <li>Check to see if the number dialed is using a route list or plan. If it is then check the Class of Restriction of the routes in the route list or plan.</li> </ul> <p><b>NOTE:</b> Before you change Class of Restriction to enable chargeable calls make sure that you have the authorization of the customer.</p> <p><b>TIP:</b> Use the SMDR records to assist you.</p>

**Table 3.6:** General Phone Troubleshooting (Continued) (Sheet 2 of 9)

Phone	Symptom	Probable Cause	Corrective Action
Any	Calls are being cut off	<ul style="list-style-type: none"> <li>• Trunk programming error</li> <li>• Hardware issue</li> <li>• Wiring fault</li> </ul>	<p>Check for a pattern.</p> <ul style="list-style-type: none"> <li>• Are the calls always being made to the same number?</li> <li>• Is it a cellular phone? If it is it is likely to be a cellular issue.</li> <li>• Is this affecting many users or just one? Build a pattern.</li> <li>• Many Users - Check SMDR records to see if it is a particular trunk or link that is causing the problem.</li> <li>• One User - Ensure that it is not a hardware or wiring issue.</li> </ul>
Any	An internal caller does not get a busy signal when calling a busy internal station.	A busy signal is not returned to the caller when the call is immediately camped onto another internal station that is in the busy state. This can be caused by the Class of Service (COS) option Auto Camp-on Timer being set to 0 (zero).	<p>In the Class of Service Options:</p> <ul style="list-style-type: none"> <li>• Disable the Auto Camp-on Timer option by blanking the option field.</li> </ul> <p>OR</p> <ul style="list-style-type: none"> <li>• Increase the Auto Camp-on Timer to a number larger than zero (e.g. 10 seconds).</li> </ul>

**Table 3.6:** General Phone Troubleshooting (Continued) (Sheet 3 of 9)

Phone	Symptom	Probable Cause	Corrective Action
Any	User reports that they are continually receiving incorrect calls.	System or set programming error	<p>Establish if the calls are always for the same person or if they are for different people. If the calls are always for the same person check the following:</p> <ul style="list-style-type: none"> <li>• Telephone Directory to ensure that the name and extension number are correct.</li> <li>• The users number against that of the person people are looking for. If the numbers are similar then it is possible that people are dialing incorrectly. Changing the users extension number maybe an option.</li> <li>• That the person being called has not call forwarded or rerouted calls to the user (who raised the complaint) in error.</li> </ul> <p>If the calls are for different people try these options:</p> <ul style="list-style-type: none"> <li>• Ask the user to log the calls received in Error.</li> <li>• Check the SMDR logs to establish a pattern.</li> </ul>
Any	Internal caller does not hear busy signal when calling an internal station in busy condition.(Busy signal is not returned to user when call is immediately camped on to another internal station that is in busy condition.)	COS option Camp On Timer is set to 0.	<p>To correct</p> <ul style="list-style-type: none"> <li>• disable Auto Camp on by blanking Camp On Timer in COS, or</li> <li>• delay Auto Camp On by setting COS option- Camp On Timer to a value other than 0 (i.e. 10 seconds). By doing this, the call still Camps On, but only after the timer expires.</li> </ul>

**Table 3.6:** General Phone Troubleshooting (Continued) (Sheet 4 of 9)

Phone	Symptom	Probable Cause	Corrective Action
Any	The volume setting saved on the handset is lost.	The “Handset Volume Adjustment - Saved” parameter is set to “No”	Set the “Handset Volume Adjustment - Saved” parameter to “Yes” in the Class of Service Options form.
		The set is dual mode and the volume was set at its maximum. For hearing safety, dual mode sets are programmed to revert to their default volume setting if they are saved at maximum volume	On a dual mode set, save the volume at least one setting level below maximum to ensure that it will be saved.
Any	Phantom calls are being made to the operator.	When a user hangs up without completing an operation in his or her voice mail box, the embedded voice mail continues to perform its function with whatever portion of the user's input is available, even though the user has hung up, and performs off-hook dialing in attempt to complete the operation. Often, this results in calls to 0, usually the operator.	In the Class of Service Options form, set the Multiline Set On-Hook Dialing option to “No”.
Any	Unable to put DID call on hold.	If you have <b>Record-a-call Save Recording on Hangup</b> enabled, you won't be able to put DID calls on hold.	In the Class of Service Options form: <ul style="list-style-type: none"> <li>• Disable <b>Record-a-call Save Recording on Hangup</b>.</li> </ul>



**Table 3.6:** General Phone Troubleshooting (Continued) (Sheet 5 of 9)

Phone	Symptom	Probable Cause	Corrective Action
ONS Sets	ONS sets not ringing on an AX controller, or ASU II.	Maximum number of ONS supported on an AX controller or ASU II has been exceeded.	Number of ONS sets supported by the AX controller or ASU II has been exceeded. Refer to the Engineering Guidelines for details.
Single-line Analog sets	Message lamp fails to function.	Insufficient voltage. The ASU and ASU II bays only support message lamp activation at 90 volts. Some single-line telephones require 110 volt message light activation.	Some set models will support either 90 volts or 110 volts via dip switch settings, Contact your supplier to determine if the sets support message lamp activation at 90 volts.
Analog Phone	No Dial Tone	Multiple possible causes	See <a href="#">No Dial Tone - Analog or DNI Phone</a> .
Display Phones	Display phone that receives an incoming call transferred from another station does not shown name or number for incoming calls. Instead, the final answer point displays the transferring party information.	Calls which into the system over ISDN using 4ESS protocol do not deliver name or number on the display.	Refer to Mitel Knowledge Base article 06-5104-00034.
IP Phone	No Dial Tone	Multiple possible causes	<b>No Dial Tone IP Phone</b>

**Table 3.6:** General Phone Troubleshooting (Continued) (Sheet 6 of 9)

Phone	Symptom	Probable Cause	Corrective Action
IP Phone	IP Phone fails to boot	Network Connection.	Verify network connection
		No power	Verify power (is there a display?)
		Faulty wiring or connection	Check the wiring and connections
			Check LED on the IP telephone for network activity. <ul style="list-style-type: none"> <li>• A green LED on the bottom of the phone indicates a proper connection</li> <li>• A flashing red LED indicates activity (data flow) on the network.</li> </ul>
IP Phone	IP Phone fails to boot.	Set's IP address cannot be reached.	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.
		DHCP programming.	Ensure that the DHCP server has been programmed with the correct information. If a DHCP server is on the 'other side' of a router from the IP phone, then the router must have DHCP forwarding enabled.

**Table 3.6:** General Phone Troubleshooting (Continued) (Sheet 7 of 9)

Phone	Symptom	Probable Cause	Corrective Action
			<p><b>NOTE:</b> IP sets require a firmware upgrade to support the new DHCP options introduced in 3300 Release 7.0; otherwise, the sets will fail to boot. Such failures can occur, for example, in a resilient cluster of mixed software releases or when sets with old firmware are added to a controller after it was upgraded to Release 7.0. For the sets to boot, DHCP options 128-135 must be present in the DHCP server. After the sets have booted, options 128-135 may be removed to avoid future conflicts with standardized or other vendors use of these options. If the IP telephone displays “TFTP LOAD FAILURE” verify that the TFTP Firmware, DSP and Main software loads are available and not corrupted.</p>
		Phone is not registered with the system.	<p>Register phone with system. See Register IP Phones in the Programming book of the System Administration Tool online help. Also see <a href="#">IP Phone Registration Troubleshooting</a>.</p>

**Table 3.6:** General Phone Troubleshooting (Continued) (Sheet 8 of 9)

Phone	Symptom	Probable Cause	Corrective Action
IP Phone	IP Phone stuck at “lock-out” or “pin in memory”.	The PIN registration code and the extension number of the IP phone are saved in the flash memory of the phone. A potential issue evolves when IP phones are moved from one site to another. If the IP phone has been successfully registered with system A, moving this phone to system B will cause it to fail and it will be stuck at “lockout” or “PIN in memory”.	Ensure that the site is using IP clustering before following these steps to clear the memory. <ol style="list-style-type: none"> <li>1. Clear the PIN registration code and the extension from the flash memory of the IP phone, by pressing the * key for a few seconds while powering the IP phone.</li> <li>2. After the flash memory is clear, the IP phone will prompt you to enter the PIN as usual in a new system.</li> </ol>
	Network ICMP Redirect Packets may cause “Exception Errors” in IP Phones which may result in unexpected reset.	Network ICMP Redirect Packets causing “Exception Errors” in IP Phones resulting in unexpected reset.	Refer to Mitel Knowledge Base article 08-5157-00024.
	PC Port not functional	COS option “PC Port On IP Phone - Disable” is set to Yes.	In the Class of Service Options form, change “PC Port On IP Phone - Disable” option to No.
IP Phones	After Cisco firmware upgrade, phones do not respond to 802.1x/EAP request.	Cisco firmware 12.2.5SE2 supports 802.1x/EAP version 3, MiVoice IP Phones do not recognize version 3 requests and ignore them.	Upgrade phones that support 802.1x versions 1 and 2: <ul style="list-style-type: none"> <li>• 53xx phones: Upgrade firmware to 4.0.0.26.</li> <li>• 52xx phones: Upgrade firmware to 2.5.0.5.</li> </ul>

**Table 3.6:** General Phone Troubleshooting (Continued) (Sheet 9 of 9)

Phone	Symptom	Probable Cause	Corrective Action
IP Phones (Dual Mode)	Dual Mode phone fails to boot up.	Dual mode phones may fail to boot up for two different reasons: <ol style="list-style-type: none"> <li>1. Cisco Discovery Protocol (CDP) is not supported in certain loads.</li> <li>2. You cannot downgrade the Boot Loads in dual mode sets and they are not compatible with the Main Load in 5.0.5.5.</li> </ol>	Refer to Mitel Knowledge Base article 04-5173-00019.
	Dual Mode phone does not retain the increased volume after user hangs up.	Dual mode sets reset to the default volume of level 4 if a user changes the volume to the maximum level of set and then hangs up.	Refer to Mitel Knowledge Base article 06-5173-00037.
SIP Phones	Phone fails to register. Responds with “404 not found” even though SIP extension username/password matches the MiVoice Business generic SIP extension/pin.		Set ARS Maximum Dialed Digits for COR 1 is set to a value equal to or greater than the SP phone DN length.

## Issues with Specific Models

**Table 3.7:** Specific Model Troubleshooting (Sheet 1 of 9)

Phone	Symptom	Probable Cause	Corrective Action
5560 IPT	Only the left handset is functioning. The right handset is not operational.	Directory number is not assigned to the 5560 IPT Slave.	In the 5560 IPT Master/Slave Association form, assign a Slave directory number.
	Unable to log in to a 5560 IPT. Set display shows "Login failed due to an invalid dn".	See <a href="#">Hot Desk Troubleshooting</a> .	
5330, 5340, 5360 IP Phone	A 5330, 5340 or 5360 set loses all applications after the 3300 ICP IP address is changed.	The controller address does not match the ICP/PBX assignment.	<ol style="list-style-type: none"> <li>1. Program Network IP address in the ICP/PBX Networking form to match IP address of the local controller.</li> <li>2. Reboot the controller to make the change effective.</li> </ol>
SUPERSET 4000, YA, and IP Phones	Headset issues.	Attempting to use an unsupported headset.	Refer to Mitel Knowledge Base article 05-6778-00015 for a listing of supported headsets.

**Table 3.7:** Specific Model Troubleshooting (Continued) (Sheet 2 of 9)

Phone	Symptom	Probable Cause	Corrective Action
5702 IP Phone or SpectraLink Wireless Handset	User experiences audio interruption on either of these sets. User is in a conversation on either of these phones and a programmed key becomes active (for example, ringing or receiving calls) and the user experiences a momentary interruption in audio reception.	The 5207 IP Phone has 14 programmable keys; the SpectraLink wireless set has 13 line select keys. If you program Direct Station Select (DSS) or multiline key appearances with audible “ring” type into any of the programmable keys on these phones, users may experience audio interruption during calls. This interruption occurs because the hardware in these phones does not support two speech channels.	Do not program DSS or multiline key appearances with “audible” ring type on 5207 IP Phones or SpectraLink wireless sets. If you need DSS or multiline key appearances on a phone, you should program the key appearances on the 5207 IP Phone or SpectraLink wireless set with “no ring” type, or use an IP Console (Release 5.2 version or later), a 5215 IP Phone, or a 5220 IP Phone instead of the 5207 IP Phone or SpectraLink wireless set.
5140 or 5240 Webset Phones	The following error appears in the display: WEB BROWSER ERROR # 2 Domain Name Service (DNS) Timeout Host Name was not resolved.	DHCP Server setup.	To resolve this problem, you have two options: <b>Option A:</b> <ol style="list-style-type: none"><li>1. In your DHCP server, program Mitel proprietary Option 135 (Proxy Server) as String type and enter a socket value in the format of &lt;ip:port&gt; For example: 192.168.1.4:3128 where 192.168.1.4 is the IP address of the MSL server and 3128 is the http proxy port</li><li>2. Reboot the webset to get the new DHCP option.</li></ol>

**Table 3.7:** Specific Model Troubleshooting (Continued) (Sheet 3 of 9)

Phone	Symptom	Probable Cause	Corrective Action
			<b>Option B:</b> <ol style="list-style-type: none"> <li>1. Program the MSL server to also be your DHCP server. For information on how to configure the MSL server, refer to the Mitel Standard Linux (MSL) Installation and Maintenance Guide available from Mitel Online</li> <li>2. Reboot the webset to get the new DHCP option.</li> </ol>
5x40 IP Phones	5x40 IP Phone will not function.	If you attempted to use the 5x40 phone Visual Voice Mail feature before enabling the COS option "HCI/CTI/Tapi Monitor Allowed", the phones will not function even after you enable the COS option.	Refer to Mitel Knowledge Base article 04-3849-00010.
5224 IP Phone	After reset of phone, phone display stuck at "Upgrade part 3 14% Do Not Power Down".	If you reset a phone during its upgrade process, the phone's flash memory will become corrupted.	Refer to Mitel Knowledge Base article 06-4409-00020.



**Table 3.7:** Specific Model Troubleshooting (Continued) (Sheet 4 of 9)

Phone	Symptom	Probable Cause	Corrective Action
5220 with 5422 PKM	<p>Any of the following:</p> <ul style="list-style-type: none"> <li>• one way audio when using speakerphone (microphone will not transmit)</li> <li>• Dual mode 5220 phones will not boot and will show “INIT ERROR PKM INFO INCOMPATIBLE” error</li> <li>• Dual mode 5220 phones will not boot and will show “NO INIT ERROR PKM CARD INCOMPATIBLE” error</li> </ul>	Unsupported hardware revisions.	Refer to Mitel Knowledge Base article 04-3849-00863 for the minimum required hardware revisions.
5330, 5340, 5360 IP Phone	No audio streaming to the corded handset. 5330/5340 running firmware 1.6.2.4 or higher. 5360 running firmware 3.0.2.10 or higher.	Set not set up for handset operation.	<p>Do either of the following:</p> <ol style="list-style-type: none"> <li>1. Unpair the Cordless Handset (see 5330/5340 User Guide for instructions).</li> <li>or</li> <li>2. Power down the Cordless Handset (simultaneously hold Mute and Volume down on Cordless Handset)</li> </ol>

**Table 3.7:** Specific Model Troubleshooting (Continued) (Sheet 5 of 9)

Phone	Symptom	Probable Cause	Corrective Action
A 5215 Dual Mode, 5220 Dual Mode, 5304, 5312 and 5324 IP	Phone fails to boot up. Set display shows "Port Access Control – Press # to Continue".	802.1X port authentication is enabled in network, but IP phone is not configured with a username and password.	Configure username and password on IP phone. See "Configuring an Authentication Username and Password" . OR Disable 802.1X support in the Layer 2 switch. See "Enabling or Disabling 802.1X Authentication".
A 5215 Dual Mode or 5220 Dual Mode IP Phone	Phone fails to boot up. Set display shows "Port Access Failure – Rebooting".	802.1X port authentication is enabled in network. IP phone is not configured with correct username and password.	Check the username and password of the IP phone in database of the RADIUS server. Configure the correct username and password in the IP phone. See "Configuring an Authentication Username and Password" OR Erase the username and password that is stored in the phone. See "Erasing an Authentication Username and Password" .Reboot the phone in order to re-enter the username and password.
		802.1X port authentication is enabled in network. PC is connected to network through IP Phone, but PC is not configured with correct username and password.	Check the username and password of the PC in database of the RADIUS server. Configure the correct username and password on the PC. OR Disable 802.1X support in the PC if enabled. OR Ensure RADIUS EAP is "EAP-MD5".

**Table 3.7:** Specific Model Troubleshooting (Continued) (Sheet 6 of 9)

Phone	Symptom	Probable Cause	Corrective Action
5330, 5340, or 5360 IP sets	Phone loses all application features and labels after the set is rebooted or after the 3300 ICP IP address is changed.	<p>The controller address does not match the ICP/PBX assignment.</p> <ol style="list-style-type: none"> <li>1. Program Network IP address in the ICP/PBX Networking form to match IP address of the local controller.</li> <li>2. Reboot the controller to make the change effective.</li> </ol>	See Mitel Knowledge Base article 07-4940-00007.
53xx IP Sets	Phones stuck at DHCP discovery after upgrade to MCD 5.0 SP1.	<p>Misconfiguration issue between Layer 2 switch port and DHCP server. Prior to MCD 5.0 SP1, the 53xx IP Phones would accept both untagged and tagged frames even though they send tagged frames with VLAN ID of N (where N is a value from 1 to 4096.)</p>	<p>Reconfigure network on the basis of the following rule of thumb: If VLAN ID and Priority are assigned to DHCP option 125, L2 port is expected to send and receive Tagged frame with VLAN ID ( In Cisco term, L2 port is configured as a Trunk port).</p> <p>Examples and solutions to some of the network misconfiguration:</p> <p><b>Case 1:</b>  <b>L2 port setting (to which 53xx is connected):</b>  Access port (untagged) for VLAN ID of N.  <b>IP phone obtains VLAN ID via:</b></p>

**Table 3.7:** Specific Model Troubleshooting (Continued) (Sheet 7 of 9)

Phone	Symptom	Probable Cause	Corrective Action
		In MCD 5.0 SP1, the firmware for 53xx IP Phones changed to adhere to the industry-standard behavior for VLAN aware devices as follows: when the DHCP server offers option 125 with VLAN ID of N, the IP Phone releases its current IP address and sends VLAN N-tagged DHCP discovery. The DHCP server responds with a DHCP offer tagged with VLAN N. In a typical VLAN aware device, all outgoing/incoming frames are expected to be tagged.	<p>DHCP option 125 is configured with VLAN ID of N, and priority of N.</p> <p><b>Solution:</b></p> <ul style="list-style-type: none"> <li>Remove the VLAN ID from DHCP option 125.</li> </ul> <p>or</p> <ul style="list-style-type: none"> <li>Make the L2 port and access port tagged for VLAN N.</li> </ul> <p><b>Case 2:</b>  <b>L2 port setting (to which 53xx is connected):</b>  Access port (untagged) for VLAN ID of N.  <b>IP phone obtains VLAN ID via:</b>  From the LAN policy of LLDP/CDP.  <b>Solution:</b></p>
			<p>Make the L2 port a trunk port tagged for VLAN N.</p> <p><b>Case 3:</b>  <b>L2 port setting (to which 53xx is connected):</b>  Access port (untagged) for native VLAN.  <b>IP phone obtains VLAN ID via:</b>  DHCP option 125 is configured with native VLAN ID of 1 and priority.  <b>Solution:</b>  Remove VLAN 1 and priority from DHCP option 125.</p>

**Table 3.7:** Specific Model Troubleshooting (Continued) (Sheet 8 of 9)

Phone	Symptom	Probable Cause	Corrective Action
5310 Conference Unit	5310 Conference is not working with 5220 DPLite (Dual Mode IP phone). The symptoms are when a user pushes the side control button, the saucer flashes but does not work.	Side control defective.	Refer to Mitel Knowledge Base article 06-5191-00067.
5505 SIP Phone	The set shows a different time than the time configured on MiVoice Business.	The set is unable to retrieve the configuration file from MiVoice Business due to the missing DNS server's IP address (DHCP option 6 not configured). As a result, the set is unable to resolve the FQDN to IP address when the SIP server or the configuration server is programmed as FQDN.	Configure Option 6 in the "DHCP Options" form with a valid DNS server's IP address. Ensure that the server is configured with MiVoice Business' FQDN and matching IP address.

**Table 3.7:** Specific Model Troubleshooting (Continued) (Sheet 9 of 9)

Phone	Symptom	Probable Cause	Corrective Action
69xx IP Phones	<p>Accessing the corporate directory from the Contacts application fails with the one of the following messages:</p> <ol style="list-style-type: none"> <li>1. Directory Import Failed</li> <li>2. Not Available Please contact your Administrator</li> </ol>	Incorrect configuration in MiVoice Business	<p><b>A)</b> Message = Directory Import Failed In Network Elements form check the following:</p> <ol style="list-style-type: none"> <li>1. LDAP server ip address is correct.</li> <li>2. FQDN address is correct.</li> <li>3. Phones DNS address is correct and able to translate FQDN address.</li> </ol> <p><b>B)</b> Message = Not Available Please contact your Administrator In LDAP Client Configuration form check the following:</p>
			<ol style="list-style-type: none"> <li>1. LDAP Server Port is configured correctly.</li> <li>2. LDAP Base DN is configured correctly.</li> <li>3. Username is configured correctly</li> <li>4. Password is configured correctly.</li> </ol>

## IP Phone Power

**Table 3.8:** IP Phone Power Troubleshooting (Sheet 1 of 3)

Symptom	Probable Cause	Corrective Action
Power unit is plugged in, but does not power up.	No power at outlet. OR faulty power outlet. OR faulty power cord.	<ol style="list-style-type: none"> <li>1. Plug a known functioning device in the power outlet.</li> <li>2. Verify that the power outlet protection circuit has not tripped.</li> <li>3. Verify that the voltage of the power outlet is within specifications.</li> <li>4. Verify that the Power Unit power cord works correctly (including good and solid ground connection).</li> </ol>
	Faulty power connections.	Verify the following: <ul style="list-style-type: none"> <li>• Ensure power is applied to the power unit.</li> <li>• Ensure you are not using crossover Ethernet cables.</li> <li>• Ensure that the input Ethernet cable is connected to the Data In port of the power unit.</li> <li>• Ensure that the output Ethernet cable is connected to the Data and Power Out port of the power unit.</li> <li>• Ensure that the input and output cables of a port pair are used for the same IP Phone.</li> </ul>
IP device does not work, and both Port Status LEDs are OFF (Power unit is not detecting IP device).	Wiring problem OR faulty IP device OR faulty Power Unit.	<ol style="list-style-type: none"> <li>1. Verify you are using a standard UTP Category 5, 6 or 6e cable (with 8 wires—4 pairs).</li> <li>2. Verify that you are not using a crossover cable.</li> <li>3. Verify that the connections for the port pair both correspond to the same IP device, and that the port connections are not reversed.</li> <li>4. Verify that the cables connected to the Data In and Data Out ports correspond to the same IP device.</li> <li>5. Connect the IP device to a different port pair on the Power Unit. If the device works normally, the original port is probably faulty.</li> <li>6. Connect the IP device directly to the Power Unit using a short cable. If the device works normally, the original cable (or one of its connectors) is faulty.</li> <li>7. If possible, connect the IP device to a different Power Unit. If the device works normally, the original Power Unit is probably faulty.</li> </ol>

**Table 3.8:** IP Phone Power Troubleshooting (Continued) (Sheet 2 of 3)

Symptom	Probable Cause	Corrective Action
IP device works, but there is no data link.	Wiring problem OR Faulty IP device OR Faulty Power Unit. OR Missing/faulty local power adapter.	<ol style="list-style-type: none"> <li>1. Verify that the port's Power Active LED is continuously ON.</li> <li>2. Verify that the connections for the port pair both correspond to the same IP device, and that the port connections are not reversed.</li> <li>3. The IP device may require a local power adapter to operate. If an adapter is already in use, replace it with a known working adapter. If this works, replace the faulty adapter.</li> <li>4. Verify you are using a standard UTP Category 5, 6 or 6e cable (with 8 wires—4 pairs).</li> <li>5. Verify that the cable length between the Power Unit and the IP device does not exceed 100 meters.</li> <li>6. Verify that you are not using any crossover cables.</li> <li>7. Verify that the Power Unit is connected to a switch/hub with a good RJ-45 patch cord connection.</li> <li>8. Connect the IP device directly to the Power Unit using a short cable. If the device works normally, the original cable (or one of its connectors) is faulty.</li> <li>9. Try to connect a known working IP device to the same port (test device). If the test device works and the link is established, there is probably a faulty data link in the original IP device.</li> <li>10. Connect the IP device to a different port pair. If the device works, one of the original ports is probably faulty, or there is a bad RJ-45 connection.</li> </ol>



**Table 3.8:** IP Phone Power Troubleshooting (Continued) (Sheet 3 of 3)

Symptom	Probable Cause	Corrective Action
IP device not operating, with Power Inactive LED ON.	Discharged capacitor in IP device OR wiring problem OR missing/Faulty local power adapter OR faulty port.	<ol style="list-style-type: none"> <li>1. Wait 5 to 10 seconds. If the Power Active LED turns ON, there was a discharged capacitor in the IP device.</li> <li>2. Verify that you are not using any crossover cables.</li> <li>3. The IP device may require a local power adapter to operate. If an adapter is already in use, replace it with a known working adapter. If this works, replace the faulty adapter.</li> <li>4. Connect the IP device directly to the Power Unit using a short cable. If the device works normally, the original cable (or one of its connectors) is faulty.</li> <li>5. Connect the IP device to a different port pair. If the device works, one of the original ports is probably faulty, or there is a bad RJ-45 connection.</li> <li>6. Unplug the IP device, and verify that the Power Inactive LED turns OFF. If it does not, the port is probably faulty, or the RJ-45 socket is shorted.</li> </ol>
IP device powered correctly, but Power Active LED is OFF.		Re-connect the IP device to a different port pair. If the new port pair Active Power LED turns ON, there is a fault in the original out put port (probably a faulty LED).
IP device does not work, but Green Port Status LED ON.	Wrong connection OR faulty IP device.	<p>Verify that the IP device is actually connected to that port.</p> <p>Replace the device by a known working IP device (test device). If the test device powers up, the original IP device is probably faulty.</p>

## IP Phone Registration

1. Record the error message on the IP Phone display, then go through .

**TIP:** To rule out DHCP problems, and isolate network-related issues, we recommend that you program the IP Phone with a static IP Address.

**NOTE:** IP sets require a firmware upgrade to support the new DHCP options introduced in 3300 Release 7.0; otherwise, the sets will fail to boot. Such failures can occur, for example, in a resilient cluster of mixed software releases or when sets with old firmware are added to a controller after it was upgraded to Release 7.0. For the sets to boot, DHCP options 128-133 must be present in the DHCP server. After the sets have booted, options 128-133 may be removed to avoid future conflicts with standardized or other vendors' use of these options.

2. If you still can't fix the problem collect the following information and then call Mitel Technical Support:

- Is the problem with the local or remote subnet?
- DHCP server(s) settings
- Layer 2 switch configuration and settings
- Router configuration and settings
- Network Diagram
- IP addressing scheme
- VLAN configuration and settings

**TIP:** Use the debug option on display IP phones to view Version, Network, Telephony/DSP, Connection Browser Config, and memory Stats details (see debug option).

**NOTE:** If a 3300 system is enabled with the MLPP feature, the IP phones that register to this controller are in an enhanced security mode. You will be unable to access the full phone debug menu because the IP phone is locked down from a security perspective. To bring the IP phone out of lock down mode, you must register the IP phone to a 3300 controller that does not have MLPP enabled. You must redirect the IP phone with DHCP options (that is, change DHCP Server option (option 125) so that IP phone will register to a 3300 controller that is not running MLPP mode). After the IP phone is successfully registered to a 3300 controller that is not in MLPP mode and after the phone has been up and running for approximately 20 seconds, you will be able to access the full debug menu.

**Table 3.9:** IP Phone Registration Troubleshooting (Sheet 1 of 8)

Error Message on Display	Possible Cause	Corrective Action
Invalid VLAN ID	DHCP Option 43 or 125 on 3300 Release 7.0 or later systems or 132 and/or 133 for earlier releases not set correctly.	<ol style="list-style-type: none"> <li>1. Identify the location of DHCP server and which DHCP server is assigned the IP address for the corresponding subnet (see “Network Configuration Examples” in the “Typical Network Configurations” chapter of the <i>Technician’s Handbook</i> for examples).</li> <li>2. For an external Microsoft DHCP server (NT server, etc.), make sure that the option type is set to LONG.</li> <li>3. For a Cisco® Router DHCP server, make sure that the option type is set to hex, and padded with 0s (for example, 0x00000002 for VLAN 2).</li> <li>4. For the controller internal DHCP server, set the option type to numeric.</li> </ol>

**Table 3.9:** IP Phone Registration Troubleshooting (Continued) (Sheet 2 of 8)

Error Message on Display	Possible Cause	Corrective Action
Duplicated IP address	Existing data device owns the IP address.	<ol style="list-style-type: none"> <li>1. Check the IP address on the phone display.</li> <li>2. Disconnect the IP Phone.</li> <li>3. From a PC on the same subnet, ping the suspected IP Phone. If there is a response, identify the data device, and resolve the conflict.</li> </ol>
	Corrupted DHCP server.	<ol style="list-style-type: none"> <li>1. On the suspected DHCP server, disable then recreate the scope.</li> <li>2. If this is a Microsoft DHCP server, reboot the server.</li> </ol>
DHCP discovery OR DHCP OFFER X REJ	DHCP option 43 or 125 on 3300 Release 7.0 or later systems or option 130 (MITEL IP PHONE) for earlier Releases is not programmed.	Identify the location of DHCP server and set to Option 130 as String type with value of "MITEL IP PHONE".
	DHCP server does not have enough IP addresses.	Create a larger scope with more IP addresses on the DHCP server.
	DHCP server cannot assign IP addresses for the corresponding subnet, even though there are enough IP addresses.	<ol style="list-style-type: none"> <li>1. For a Microsoft DHCP server, reboot the server.</li> <li>2. For the controller internal DHCP server, disable DHCP and rebuild the scope.</li> </ol>
	L2 switch port is shut down or not configured properly.	<ol style="list-style-type: none"> <li>1. Check the L2 switch, and ensure that the port is not shut down.</li> <li>2. Ensure that this port can access the DHCP server subnet (that is, access the port for the same VLAN, etc.).</li> </ol>
	Your installation is using the controller's internal DHCP server, but DBMS Save is not on.	Enter the DBMS Save command through the Maintenance Commands form.

**Table 3.9:** IP Phone Registration Troubleshooting (Continued) (Sheet 3 of 8)

Error Message on Display	Possible Cause	Corrective Action
DHCP Discovery OR DHCP OFFER X REJ (VLAN) (after releasing the first IP from the native DHCP server)	DHCP Option 43 or 125 on 3300 Release 7.0 or later systems or Option 30 (MITEL IP PHONE) for earlier Releases is not programmed on the second scope of the DHCP server (or on the second DHCP server). OR VLAN ID is not assigned properly.	<ol style="list-style-type: none"> <li>1. Identify if there is one DHCP server for both VLANs, or if there is one DHCP server per VLAN (see “Network Configuration Examples” in the “Typical Network Configurations” chapter of the <i>Technician’s Handbook</i>).</li> <li>2. For one DHCP server for both VLANs, ensure that option 43 or 125 is properly configured (3300 Release 7.0 and later) or that option 130 is programmed as String type with value of “MITEL IP PHONE” (prior to Release 7.0), in the scope of Voice LAN.</li> <li>3. For one DHCP server per VLAN, ensure that option 43 or 125 (Release 7.0 and later) or 130 (prior to Release 7.0) is defined.</li> <li>4. Verify that the proper VLAN ID is assigned in option 43 or 125 (Release 7.0 and later), or 132 (prior to Release 7.0).</li> </ol>
	One DHCP server for two VLANs network configuration: IP helper address on the router interface is not set up correctly.	<ol style="list-style-type: none"> <li>1. On the router interface (on which DHCP is not residing), enter the IP helper address and specify the IP address of the DHCP server on the other side of the subnet (that is, always set up IP helper address on the DHCP server client side).</li> <li>2. Ensure the second scope is created for the corresponding VLAN (see “Network Configuration Examples” in the “Typical Network Configurations” chapter of the <i>Technician’s Handbook</i>).</li> </ol>

**Table 3.9:** IP Phone Registration Troubleshooting (Continued) (Sheet 4 of 8)

Error Message on Display	Possible Cause	Corrective Action
(Cont'd)	The L2 switch port for the phone interface is shut down or not configured properly.	<ol style="list-style-type: none"> <li>1. Check the L2 switch and ensure that the port is not shut down.</li> <li>2. For a Cisco L2 switch, ensure that this is a trunk port with Dot1q encapsulation, and that this trunk port allows both native and Voice LAN to pass through.</li> <li>3. For an HP L2 switch, ensure that Native Lan is untagged, and that Voice LAN is tagged.</li> <li>4. Verify whether there are two physical interfaces to the router (one per VLAN), or a router on a stick configuration (one physical with virtual sub-interfaces).</li> <li>5. Ensure that the ports on both sides (L2 switch and router) are not shut down (See “Network Configuration Examples” in the “Typical Network Configurations” chapter of the <i>Technician’s Handbook</i>).</li> <li>6. If there is a physical interface on the router for each VLAN, make sure that the L2 switch is set to correctly access port for the corresponding VLAN/ subnet.</li> <li>7. If there is one physical interface on the router for multiple VLANs, ensure that this is a trunk port on the L2 switch, and ensure that this trunk port allows both native and voice LAN to pass through.</li> <li>8. On the router sub-interface, ensure that the proper VLAN is associated to the remote sub-interface.</li> </ol>

**Table 3.9:** IP Phone Registration Troubleshooting (Continued) (Sheet 5 of 8)

Error Message on Display	Possible Cause	Corrective Action
TFTP load failure	DHCP option 43 or 125 on 3300 Release 7.0 or later systems or option 128 for earlier releases is not set up to point to the right TFTP server (Controller).	Check the DHCP server, and confirm that option 43, 125, or 128 is pointing to the right TFTP server.
	No network connectivity between the controller and the phone.	<ol style="list-style-type: none"> <li>1. Confirm that the controller is connected to the network.</li> <li>2. For a Cisco L2 switch: verify that the L2 switch is access port (Voice LAN).</li> <li>3. For an HP L2 switch: verify that the L2 switch is untagged (Voice LAN).</li> <li>4. If the router is involved, make sure that the router's MTU is set to 600 or more.</li> </ol>
	Firmware on controller is missing or corrupted.	<ol style="list-style-type: none"> <li>1. Verify that the firmware ( <b>ipp510bootenc.bin</b>, etc.) is in the <b>sysro/tftp</b> directory (particularly if the user has manually copied the firmware).</li> <li>2. Confirm if TFTP on the controller is corrupted (this can be verified by connecting the IP Phone directly on the controller, or by observing the behavior of other IP Phones).</li> </ol> <p><b>TIP:</b> If you have Option 132/133 programmed on the controller's internal DHCP server, disable them before trying Step 2.</p>
	Your installation is using the controller's internal DHCP server, but internal DHCP server is not enabled.	Using the Server Manager, enable the internal DHCP server using the DHCP form.

**Table 3.9:** IP Phone Registration Troubleshooting (Continued) (Sheet 6 of 8)

Error Message on Display	Possible Cause	Corrective Action
Waiting for link	DHCP option 43 or 125 on 3300 Release 7.0 or later systems or option 129 for earlier Releases is not programmed correctly.	Check Option 43, 125, or 129 on DHCP to confirm that the IP address is programmed correctly. (RTC IP Address of controller)
	Spanning Tree protocol is disabled. It's used to provide location and location information for Emergency Services (E911).	Ensure Spanning Tree protocol is enabled.
	The application server is broadcasting or multicasting on IP Phone port or on PC behind the IP Phone.	Turn off multicasting.
	The PC behind the IP Phone is changing speed 100/10.	Depending on the NIC, you may need to hardcode to 100 MBps instead of auto negotiation.
Waiting for link OR Lost link to Server	IP phone fails to receive Keepalive message in 30 seconds.	Verify if the network or the controller is down.
	There is electrical interference.	Verify the power source, and change the location of the power source.

**Table 3.9:** IP Phone Registration Troubleshooting (Continued) (Sheet 7 of 8)

Error Message on Display	Possible Cause	Corrective Action
<p>Unable to register IP phones due to regproc trap. Other symptoms once a regproc trap has occurred are as follows:</p> <ul style="list-style-type: none"><li>• Can't reregister a phone that was already registered.</li><li>• Can't log in hot desk users.</li><li>• Phone stays up after deleting a MAC.</li></ul>	<p>IP Phone has tried to register more than 10 times in succession without success.</p>	<p>Refer to Mitel Knowledge Base article 06-9999-00024.</p>



**Table 3.9:** IP Phone Registration Troubleshooting (Continued) (Sheet 8 of 8)

Error Message on Display	Possible Cause	Corrective Action
TFTP Fail ( Remote IP phone with statically programmed IP address cannot access MN3300 across WAN).	The Layer 2 switch port for the phone interface is shut down or not configured properly.	<ol style="list-style-type: none"> <li>1. Check the Layer 2 switch and ensure that the port is not shut down (see “Network Configuration Examples” in the “Typical Network Configurations” chapter of the <i>Technician’s Handbook</i> for more information).</li> <li>2. For a Cisco Layer 2 switch: verify that this is a trunk port with Dot1q encapsulation, and ensure this trunk port allows both native and voice LAN to pass through.</li> <li>3. For an HP Layer 2 switch: verify that Native Lan is untagged and Voice Lan is tagged.</li> </ol>
	The Layer 2 switch port for router interface is shut down or not configured properly.	<ol style="list-style-type: none"> <li>1. Verify which configuration you have (see “Network Configuration Examples” in the “Typical Network Configurations” chapter of the <i>Technician’s Handbook</i> for more information).</li> <li>2. Ensure the port(s) on both sides (Layer 2 switch and router) are not shut down.</li> <li>3. If there is physical interface on the router for each VLAN, make sure that the Layer 2 switch is set to access the port for the corresponding VLAN/subnet correctly; OR If this is a router on a switch, verify that this is a trunk port on L2 switch, and ensure this trunk port allows both native and voice LAN to pass through.</li> <li>4. On the router's sub-interface, verify that the proper VLAN is associated to the sub-interface (see “Network Configuration Examples” in the “Typical Network Configurations” chapter of the <i>Technician’s Handbook</i> for more information).</li> </ol>
(Cont'd)	Typo in IP address, VLAN ID, gateway.	<ol style="list-style-type: none"> <li>1. Delete and reprogram the static IP address. If there is no VLAN or priority, leave them as blank.</li> <li>2. Verify that the gateway IP address is correct.</li> </ol>

## Phone Connection

**TIP:** On display IP phones use the Configuration (Debug) Menu to view Version, Network, Telephony/DSP, Connection Browser Config, memory Stats details (for more information, see [Viewing Settings and Network Parameters on IP Phones](#)).

**Table 3.10:** Troubleshooting Phone Connection Problems (Sheet 1 of 3)

Symptom	Possible Cause	Corrective Action
Cannot make outgoing calls (except for emergency and attendant calls). "License Violation" displays on idle DNI and IP sets.	The controller is in System Lock license violation mode.	Correct the license violation event by reducing the number of over-allocated licenses.
Cannot make calls externally (display phone may show <b>call barred</b> ).	COR restricted.	<ol style="list-style-type: none"> <li>1. Identify the numbers dialed by the user, then check the route used in ARS.</li> <li>2. Remove the COR number from COR group table in COR assignment used in the route, OR Change the COR group number in the ARS Routes form.</li> </ol>
	COS restricted for PRI or QSIG trunk.	Enable <b>Public network access via DPNSS</b> in the set's COS.
Cannot make call over analog loop trunk (intermittent problem).	PBX is sending the dialing digits too fast for Telco's receiver on the LOOP trunk.	Insert a tone plan in the ARS Digit Modification Plans for the route used by analog loop trunk (tone plan is used to insert one or two seconds delay without any tone detection).
NONE of the sets are responding.	Problem with controller.	Perform a system check on the controller.
Sets cannot receive DID calls.	Non-DID is enabled in Station Attributes form.	Disable non-DID in the set's COS.

**Table 3.10:** Troubleshooting Phone Connection Problems (Continued) (Sheet 2 of 3)

Symptom	Possible Cause	Corrective Action
No dial tone on set.	Set is not programmed.	In System Administration Tool, program the extension accordingly.
	Wrong wiring.	Check the wiring between the phone jack and the ASU, ASU II, AMB, or AOB.
	Faulty handset wire.	<ol style="list-style-type: none"> <li>1. Replace the handset cord.</li> <li>2. Replace the handset.</li> <li>3. Replace the set.</li> </ol>
	Circuit is busy.	<ol style="list-style-type: none"> <li>1. Enter the Maintenance command STATE &lt;plid of the circuit&gt;.</li> <li>2. Enter the Maintenance command RTS &lt;plid&gt;.</li> </ol>
	Circuit is locked out.	Verify the wiring between the phone and the patch panel.
Sets take 10-12 seconds to receive incoming calls. Dialing digit conflict.	ANI/DNIS number delivery trunk option is enabled in T1 trunk's COS.	Disable the ANI/DNIS number delivery in the trunk's COS. <b>TIP:</b> You can assign an unused COS to verify if this is the problem.
	Dialing digit conflict.	Check the following forms for any potential dialing conflict: <ul style="list-style-type: none"> <li>- Station Service Assignment</li> <li>- Miscellaneous Assignment</li> <li>- Feature Access Code</li> <li>- Agent ID Assignment</li> <li>- System Option Assignment</li> </ul>

**Table 3.10:** Troubleshooting Phone Connection Problems (Continued) (Sheet 3 of 3)

Symptom	Possible Cause	Corrective Action
IP to IP calls OK, but not IP to TDM calls (ring back heard once, then call drops).	E2T not loaded.	<ol style="list-style-type: none"> <li>1. Verify that the E2T IP address is programmed correctly.</li> <li>2. Verify that the E2T IP address is not used elsewhere on the network.</li> <li>3. If the E2T IP address was hard coded with a debug cable, verify its settings (see “DHCP Configuration Settings” in the “Installation Planner:” chapter of the <i>Technician’s Handbook</i>).</li> </ol>

**NOTE:** For IP Phone connection issues related to Resiliency, see [IP Device Resiliency](#).

## Phone Audio Quality

**NOTE:** Use the Configuration (Debug) Menu on display IP phones to view Version, Network, Telephony/DSP, Connection Browser Config, memory Stats details (for more information, see [Viewing Settings and Network Parameters on IP Phones](#)).

**Table 3.11:** Audio Quality Troubleshooting (Sheet 1 of 5)

Symptom	Possible Cause	Corrective Action
One-way audio between Remote IP to TDM (VM)	No gateway IP address programmed on E2T.	<ol style="list-style-type: none"> <li>1. If E2T gets IP address from DHCP server, make sure that Option 03 (Router) is assigned to the scope with the proper IP address for the subnet.</li> <li>2. If E2T is hard coded with a static IP address, make sure that the gateway IP address is programmed properly in u-boot environment variables.</li> </ol>
Broken Audio, intermittent	Handsfree on the far end.	Ensure that neither device is using handsfree. Some handsfree phones only operate at half duplex.

**Table 3.11:**Audio Quality Troubleshooting (Continued) (Sheet 2 of 5)

Symptom	Possible Cause	Corrective Action
	Packet loss, jitter via network.	<ol style="list-style-type: none"> <li>1. Identify the speech path between the two end points, including router, switch WAN in the audio stream.</li> <li>2. The network administrator needs to apply QOS/TOS to minimize jitter over slow speed interface (T1, Frame Relay, etc.), and give voice traffic priority over data.</li> </ol>
	Limited bandwidth and too many calls across router, or combination data and voice.	<ol style="list-style-type: none"> <li>1. Limit the number of calls to remote subnets.</li> <li>2. The network administrator needs to apply QOS/TOS to give voice traffic priority over data.</li> </ol>
	Physical port error (CRC, faulty cable, duplex mismatch, HUB).	<ol style="list-style-type: none"> <li>1. Identify the speech path between the two end points, including router, switch WAN in the audio stream.</li> <li>2. Verify that there is no duplex mismatch in each port settings, or faulty cable, or faulty port.</li> <li>3. Make sure that the IP Phone is not plugged into a HUB.</li> </ol>
	Compression zone enabled.	Compression will save bandwidth, but may cause noticeable clipping. If not sure, disable compression to see if it makes a difference.
	Router's CPU is exhausted or congested.	Router may be running excessive filtering. The network administrator may need to monitor the performance of the router.

**Table 3.11:**Audio Quality Troubleshooting (Continued) (Sheet 3 of 5)

Symptom	Possible Cause	Corrective Action
Broken Audio, intermittent	Layer 2 Switch ports configured incorrectly.	<ol style="list-style-type: none"> <li>1. In the Layer 2 Switch form of the System Administration Tool, configure all L2 ports in the voice path with the same settings. The recommended settings for the “Duplex Mode” field and the “Flow Control” field is “Auto”.</li> <li>2. If the network requires fixed settings, use the following: <ul style="list-style-type: none"> <li>– State - Enabled</li> <li>– Speed - 100 Mb</li> <li>– Duplex Mode - Full DX</li> <li>– Flow Control - Enabled</li> <li>– Voice VLAN - Tagged</li> </ul> </li> <li>3. If you change these fields to fixed settings, you must also set the IP phones to use the fixed settings. You change the IP phone settings through the Configuration menu. See Access Configuration Menu on Single-Mode IP Phones.</li> <li>4. In the Configuration menu, select <b>Hardware Config?</b> and then select <b>Modify Port Setting</b> and modify the settings.</li> </ol>
Echo occurring between IP Phones and TDM Phones	Handsfree mode is used.	Check if far end is using handsfree. Switch to handset mode to see if this corrects it, or lower the volume in handsfree mode.
	If echo occurs on calls between IP and TDM phones, the Echo Canceller could be beyond required specifications.	<ol style="list-style-type: none"> <li>1. Identify the path between the two end points, and verify if Trunk is always involved.</li> <li>2. Check with Telco to see if the trunk is within specs. On a typical T1, the input signal should be -15 dB. If it is too high(-5 dB for example), echo may result. If this is the case, keep an echo log to isolate the problem.</li> </ol>
	Network jitter issue.	If the problem only occurs between IP devices, check network jitter issue above.
	Loop Start (LS) Trunk settings	If the problem occurs on phones that are connected via Loop Start (LS) trunks, use the Line Quality Measurement form in the System Administration Tool to test the line quality and to obtain the recommended settings.

**Table 3.11:**Audio Quality Troubleshooting (Continued) (Sheet 4 of 5)

Symptom	Possible Cause	Corrective Action
Echo occurring between IP Phones	Layer 2 switch setting problem.	<ol style="list-style-type: none"> <li>1. Check the L2 switch for duplex mismatch and spanning tree.</li> <li>2. Turn off spanning tree between the L2 switch and the IP Phone if possible (use the PortFast setting).</li> <li>3. In the Layer 2 Switch form of the System Administration Tool, configure all L2 ports in the voice path with the same settings. The recommended settings for the “Duplex Mode” field and the “Flow Control” field is “Auto”.</li> <li>4. If the network requires fixed settings, use the following: <ul style="list-style-type: none"> <li>– State - Enabled</li> <li>– Speed - 100 Mb</li> <li>– Duplex Mode - Full DX</li> <li>– Flow Control - Enabled</li> <li>– Voice VLAN - Tagged</li> </ul> </li> <li>5. If you change these fields to fixed settings, you must also set the IP phones to use the fixed settings. You change the IP phone settings through the Configuration menu (see Access Configuration Menu on Single Mode IP Phones).</li> <li>6. In the Configuration menu, select <b>Hardware Config?</b> and then select <b>Modify Port Setting</b> and modify the settings.</li> </ol>

**Table 3.11:** Audio Quality Troubleshooting (Continued) (Sheet 5 of 5)

Symptom	Possible Cause	Corrective Action
	Far end phone is on handsfree	<p>Check if far end is using handsfree. Switch to handset mode to see if this corrects it, or lower the volume in handsfree mode. For best results when using handsfree mode:</p> <ul style="list-style-type: none"> <li>• ensure that the microphone (on the front edge of the telephone) is unobstructed and not close to a reflecting surface, such as a shelf.</li> <li>• minimize background noise (such as printers, fans, and radios)</li> <li>• sit within reach of the telephone</li> <li>• speak at a normal volume towards the microphone.</li> </ul>
	In conference call, echo is noticed from external trunk	<ol style="list-style-type: none"> <li>1. Identify the path between the two end points, and verify if Trunk is always involved.</li> <li>2. Check with Telco to see if the trunk is within specs. On a typical T1, the input signal should be -15 dB. If it is too high(-5 dB for example), echo may result. Keep a log to isolate the problem.</li> </ol>
	There is an audio path between the users as well as between the phones.	Provide better acoustic shielding between users, e.g. close the door, provide sound-deadening partitions.
Voice quality issues appear after a network upgrade	Cisco IOS is upgraded to IOS 12.2(37), MiVoice IP Phones receive DiffServ (DSCP) value of 0 from LLDP resulting in Voice Quality of Service degradation.	Refer to Mitel Knowledge Base article 08-5191-00104.
Audio issues on SIP, including Music on Hold.	Need to have ENABLE_TX_CHAN_CONN feature enabled.	



## 5550 IP Console

**Table 3.12:** 5550 IP Console Problems Troubleshooting (Sheet 1 of 2)

Symptoms	Probable cause	Corrective Action
5550 IP console fails to register (red LED is lit on TKB).	TKB (keyboard) - does not have a reserved IP address OR does not have the right IP address OR is not communicating with the right controller.	<ol style="list-style-type: none"> <li>1. Check DHCP lease to confirm if an expected IP address is assigned to TKB.</li> <li>2. If not assigned properly, ensure that you enter the MAC address of TKB properly in the Multiline Sets form in System Administration Tool.</li> <li>3. Recycle the power of the TKB to ensure that the TKB is reloaded properly.</li> </ol>
	Console PC does not have the proper IP address.	If the IP address of PC is on different subnet than the TKB, make sure that the router between these two subnets is functional.
	PC NIC has 802.1Q enabled on Data side while L2 switch is not configured to accept tagged frame on Native VLAN.	Disable 802.1Q on PC NIC <b>NOTE:</b> Only use 802.1Q on PC if PC and TKB are on the same VLAN (e.g 2) which L2 switch accepts tagged frame on the specified VLAN.
5550 IP Console fails to launch.	5550 IP Console has been registered and IP console is reinstalled.	Delete the MAC address from IP Consoles form and then re-register using the IP Console Configuration Wizard (Start/MN5550 IP console/Tools).  <b>NOTE:</b> Do not reinstall the IP Console software unless you need to (new installation, corrupted software, etc.). You should always use the Configuration Wizard to register to a different controller.
	User does not have local administration privileges.	Add local administration privileges for the user.

**Table 3.12:** 5550 IP Console Problems Troubleshooting (Continued) (Sheet 2 of 2)

Symptoms	Probable cause	Corrective Action
"Unable to Display Page" Error Message when you launch Internet Explorer.	5550 IP Console is running on Windows 98 operating system on the PC.	Close the 5550 IP Console application and then open Internet Explorer. The 5550 IP Console must be run as a standalone application on Windows 98 (that is, with no other application open while it is running).
5550 IP Console Keypad not operating properly.	Required TCP ports blocked or conflicting with other applications.	Keypad to Console PC: TCP Port 6900, PC Port 10000 Console PC to 3300 ICP: Ports 6800, 7011, and 1606
5550 IP Console stops working due to a pop-up error message that indicates that the console could not be started due to missing configuration settings.	In a resilient configuration the primary controller has failed over to the secondary, but the IP Console has not be configured as resilient (that is, it is not configured on the secondary controller).	You must configure the 5550 IP Console on the secondary controller. <ul style="list-style-type: none"> <li>For clusters that do not support Remote Directory Number Synchronization, you must manually configure the IP Console on the secondary controller. Refer to the <i>MiVoice Business Resiliency Guidelines</i> for instructions.</li> <li>For clusters that support Remote Directory Number Synchronization, configure the IP Console with the secondary controller in the IP Consoles form.</li> </ul>

# Software

## Software Troubleshooting Tips

- Always make a database backup before and after major database changes
- For troubleshooting issues that arise when you are using the MiVoice Business Software Installer Tool, see [Tools and Embedded Applications](#).
- For licensing issues, see [Licensing](#).

## System Software

**NOTE:** In the event of a system failure, collect the system error logs before contacting Product Support. Refer to Mitel Knowledge Base article 04-1000-00011 for instructions.

**Table 4.1:** System Software Troubleshooting (Sheet 1 of 6)

Symptom	Possible Cause	Corrective Action
Loss of system database. After a scheduled reboot of the system, the 3300 ICP system database is blanked out.	If you decrease the IP user or IP device licenses in the License and Option Selection form, the system database is blanked out after the next scheduled reboot.	Perform a Database Restore from a recent system backup. If you reduce the number of IP user licenses or IP device licenses from the License and Option Selection form, always perform a DBMS Save prior to rebooting to prevent the loss of the database
System is not processing calls and appears to be locked up.	Software issue	<b>1. Run System Diagnostics:</b> <b>For MXe-III/MXe III-L controllers only</b> <ul style="list-style-type: none"> <li>• Locate the remote alarm On/Off button next to the alarm relay connector on the front of the 3300 ICP controller.</li> <li>• Press and hold the remote alarm button until all alarm LEDs (critical/major/minor) are ON.</li> <li>• After you release the remote alarm button is released, the system reboots automatically within a short time.</li> </ul>

**Table 4.1:** System Software Troubleshooting (Continued) (Sheet 2 of 6)

Symptom	Possible Cause	Corrective Action
Unable to log in to the EX Controller Web GUI using the <i>mimx</i> user account credentials after it is reset in Server Manager.	Password mismatch. The minimum number of characters the Server Manager accepts for the password is seven. However, if you reset the password to a seven-character password, it is not synchronized with the <i>mimx</i> user account because the <i>mimx</i> and the SNMPv3 passwords require a minimum of eight characters.	<p>Displaying the active <i>mimx</i> password</p> <ol style="list-style-type: none"> <li>1. Start SSH client.</li> <li>2. Log in to the MiVoice Business virtual machine through an SSH session.</li> <li>3. Execute the following command: <code>cd /usr/libexec/mimx</code></li> <li>4. Execute the following commands: <code>./mimx-servermgt.sh -p ./mivbservermgt.sh -p</code></li> </ol> <p>Executing these commands displays the entries in the <i>mimx</i> and MiVoice Business database, including all passwords.</p>
Cannot log in to the System Administration Tool for the 3300 ICP Controller.	Forgot the login credentials	See <a href="#">Reset the System Admin Password</a> .
The MiVoice Business software is unable to boot from the HDD (or SSD).	Partial or complete disk corruption or disk failure	You must recover the MiVoice Business software from the HDD (or SSD). See <a href="#">Unable to boot the MiVoice Business System on 3300 ICP Controller</a> .
MSP430 flash upgrade fails	Some MSP430 instances require a newer BSL patch to perform flash upgrade	<p>Run the following commands:</p> <ol style="list-style-type: none"> <li>1. <code>mcdDebug sys430UseNewBslPatch=1</code></li> <li>2. <code>mcdDebug sys430UseHighBaudrate=1</code></li> <li>3. <code>mcdDebug Upgrade_430</code></li> </ol> <p>For the changes to take effect the system must be restarted.</p>

**Table 4.1:** System Software Troubleshooting (Continued) (Sheet 3 of 6)

Symptom	Possible Cause	Corrective Action
When you attempt to log in as the <i>admin</i> user to the Server Console, the following error message is displayed: ADMIN LOGIN IS BLOCKED UNTIL MIVOICE BUSINESS IS STARTED	MiVoice Business application has not completed the startup. System can unblock access to the Server Console only after MiVoice Business application completes the startup.	<p>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 start up even after 20 minutes (for example, 3300 ICP controller and/or RTC Card replacement scenarios), follow the steps below to recover the system:</p> <ol style="list-style-type: none"> <li>1. Log in as the <i>root</i> user through the Maintenance port (see <b>Ch 6, Maintenance &gt; Access 3300 ICP Controller Through the Maintenance Port</b> in the <i>MiVoice Business Technician's Handbook, Release 9.1</i>), and execute the <b>disablemivb</b> command followed by the <b>reboot</b> command to disable the MiVoice Business application.</li> <li>2. After the system reboots, the MiVoice Business application remains disabled. Log in to the Server Console through the terminal emulator application as the <i>admin</i> user and select the <b>Configure this server</b> option to configure the server (see <b>Ch 6, Maintenance &gt; Configuring the Server using Server Console &gt; Configuring the Console</b> in the <i>MiVoice Business Technician's Handbook, Release 9.1</i>).</li> <li>3. After you make the required configuration changes, the Server Console may force a system reboot to activate the changes. If the Server Console program forces a reboot, wait for the login prompt through the Maintenance port, log in as the <i>root</i> user and execute the <b>enablemivb</b> command followed by the <b>reboot</b> command to enable the application. If the Server Console program does not force a reboot, exit the Server Console, log in as the <i>root</i> user through the Maintenance port and execute the <b>enablemivb</b> command followed by the <b>reboot</b> command.</li> </ol> <p><b>NOTE:</b> The maximum allowed time for the application to complete the startup is 30 minutes. If the application does not complete the startup in 30 minutes, the system automatically initiates a reboot; after 5 unsuccessful application startups, the MiVoice Business application auto-disables (see <a href="#">Unable to boot the MiVoice Business System on 3300 ICP Controller</a>).</p>

**Table 4.1:** System Software Troubleshooting (Continued) (Sheet 4 of 6)

Symptom	Possible Cause	Corrective Action
Visual Voice Mail indicator on the MiCollab client is not displaying correctly. <b>NOTE:</b> <i>The symptom is noticed only with Containers-based MiVoice Business.</i>	User PIN (User and Services Configuration form > Phone Service > Access and Authentication) and Passcode (VM Mailboxes form) are not synchronizing with the MiCollab client	<ol style="list-style-type: none"> <li>1. In the System Administration Tool, navigate to the <b>SDS Form Sharing</b> from, select <b>VM Mailboxes</b>, and set <b>Share Form With</b> <ul style="list-style-type: none"> <li>– as <b>None</b> in case of a non resilient deployment.</li> <li>– as <b>Resilient Pairin</b> in case of resilient deployment.</li> </ul> </li> <li>2. From the MiCollab shell, run the following command to restart sdscc. <pre>sv restart sdscc</pre> </li> <li>3. After the sdscc service has started, from the MiCollab shell, run the following command to restart mom-server. <pre>sv restart mom-server</pre> </li> <li>4. After the mom-server has started (could take approximately one minute), in the System Administration Tool, navigate to the <b>Network Elements Form</b>, and sync the MiCollab client with the System Administration Tool twice.</li> </ol>

**Table 4.1:** System Software Troubleshooting (Continued) (Sheet 5 of 6)

Symptom	Possible Cause	Corrective Action
(Hyper-V) Unable to access the MiVoice Business System Administration Tool through web browser or SSH.	MAC address of the virtual machine has changed.	<p>If power is restored to a virtual machine (Hyper-V) after a prolonged power loss, Hyper-V dynamically assigns a new MAC address to the virtual machine. This prevents access to the System Administration Tool.</p> <p>To resolve the issue:</p> <ol style="list-style-type: none"> <li>1. Access the system through SSH using a communication application, such as PuTTY.</li> <li>2. Log in as user <i>root</i>.</li> <li>3. Run the <code>ip a</code> command to determine the current MAC address.</li> <li>4. Backup the virtual machine.</li> <li>5. Power down the virtual machine.</li> <li>6. In the Hyper-V Manager, select the virtual machine and click Settings.</li> <li>7. In the left pane, expand Network Adapter, and click Advanced Features.</li> <li>8. In the right pane, under MAC Address, select Static and enter the current MAC address.</li> <li>9. Click OK.</li> <li>10. Power on the virtual machine.</li> </ol>

**Table 4.1:** System Software Troubleshooting (Continued) (Sheet 6 of 6)

Symptom	Possible Cause	Corrective Action
<p>The following error output is displayed in the journal logs when you run the <code>calling_party_pays rebuild_tree</code> maintenance command:</p> <pre>Error in extracting the IFT file. Aborting...</pre>	<p>The following shell script is run as <i>root</i> instead of <i>voiceadmin</i>:</p> <pre>/opt/MitelPS/CPPTool/bin/cpptool.sh</pre>	<ol style="list-style-type: none"> <li>1. Access the system through SSH using a communication application, such as PuTTY.</li> <li>2. Log in as <i>root</i>.</li> <li>3. Run the following commands: <ul style="list-style-type: none"> <li>– <code>ls -ald /db/cc/CPPTool</code></li> </ul> <p>Resulting output:</p> <pre>drwxr-xr-x 2 root root 4096 Oct 29 13:14 /db/cc/CPPTool</pre> <li>– <code>ls -al /opt/MitelPS/CPPTool/IFT.zip</code></li> <p>Resulting output:</p> <pre>-rw-r--r-- 1 root root 2029536 Oct 29 13:14 /opt/MitelPS/CPPTool/IFT.zip</pre> <li>4. To delete <code>/db/cc/CPPTool</code> and <code>/opt/MitelPS/CPPTool/IFT.zip</code> files run the following commands: <p><b>NOTE:</b> Delete the above files only if they are owned by <i>root</i>.</p> <ul style="list-style-type: none"> <li>– <code>rmdir /db/cc/CPPTool</code></li> <li>– <code>rm /opt/MitelPS/CPPTool/IFT.zip</code></li> </ul> <li>5. Run the following command to monitor the journal: <pre>journactl -f</pre> <li>6. Log in to the MiVoice Business System Administration Tool, and then run the following maintenance command: <pre>calling_party_pays rebuild_tree</pre> <p>If the issue still persist, contact Mitel Technical Support.</p> </li> </li></li></li></ol>

## Unable to boot the MiVoice Business System on 3300 ICP Controller

### Overview

You must [Recover the system through the Server Manager](#) if:

- the MiVoice Business software is unable to boot from the HDD (or SSD) of your 3300 ICP Controller.



- the MiVoice Business application fails to boot several times. In this case, the error message `Detected several incomplete MiVoice Application reboots. The MiVoice Business services are currently disabled. A manual reboot is required after the root cause is addressed` is displayed.

## Recover the system through the Server Manager

- Log in to the Server Manager.  
If you are unable to access or log in to the Server Manager, see [Recover the System through SSH](#).
- After logging in to the Server Manager, verify whether the following error message is displayed at the top of the page:  
  
`Detected several incomplete MiVoice Application reboots. The MiVoice Business services are currently disabled. A manual reboot is required after the root cause is addressed`  
You may collect the *journal* log file(s) (**Administration > View log files**) to send to Mitel Product Support for analysis.
- Swap the active partition of the controller with its inactive partition (**ServiceLink > System Upgrade > Install and Upgrade > Swap to Inactive**).
- If the system is unable to boot the MiVoice Business software from its HDD after the swap, see [Unable to Recover the MiVoice Business system from Active and Inactive Partitions](#).
- If the system is able to boot the MiVoice Business software after the swap, sync the system licenses with the Application Management Center (AMC) server through the Server Manager (**ServiceLink > Status**).
- After syncing system licenses with the AMC server, upgrade MiVoice Business to the required software version through the Server Manager if needed (**ServiceLink > System Upgrade**).
- Restore the most recent database using the Server Manager (**Administration > Restore**).

## Recover the System through SSH

### Overview

If you are unable to log in to the Server Manager, then connect to the system through SSH as root user (if SSH access is enabled), and use the following procedure to recover the system. Please collect journal logs for product support for analysis.

### Procedure

- Access the system through SSH (for example, through PuTTY) and log in as *root*.  
If you are unable to access or log in to the system, see [Recover the System through the Maintenance Port](#).
- Run the following command to capture the system's journal log into a file, `/root/journal.log`: **journalctl --no-pager > journal.log**. You may send *journal.log* to Mitel Product Support for analysis.
- Run the following command to determine the active partition number of the controller:  
**fw\_printenv ata\_active\_part**
- Run the following command to swap the active partition of the controller with its inactive partition:

**fw\_setenv ata\_active\_part <disk partition>**

Here, <disk partition> is the number beside the current active partition number (output of the command in **Step 3** ) as shown in the table below for the different 3300 ICP controllers

**Table 4.2:** Disk Partition Numbers for 3300 ICP Controllers

3300 ICP Controller	Disk Partition Numbers
MXe III/MXe III-L	1 or 2
CX II	1 or 2
AX	2 or 3

**Example:** The active partition number (output of the command **fw\_printenv ata\_active\_part** in **Step 3**) of an MXe III controller is **1** . Then, to swap the active partition of the MXe III controller with its inactive partition, you must run the following command with the *disk partition* parameter set to **2** :

**fw\_setenv ata\_active\_part 2**

5. Run the following command to reboot the system:

**reboot**

6. If the system is now able to boot the MiVoice Business software from its HDD, sync the system licenses with the AMC server through the Server Manager ( **ServiceLink > Status** ).
7. If the system is unable to boot the MiVoice Business software from its HDD after the swap, see [Unable to Recover the MiVoice Business system from Active and Inactive Partitions](#) .
8. After syncing system licenses with the AMC server, upgrade the MiVoice Business system to the required software version through the Server Manager if needed ( **ServiceLink > System Upgrade** ).
9. Restore the most recent database using the Server Manager ( **Administration > Restore** ).

## Recover the System through the Maintenance Port

### Overview

If you are unable to log in to the system through SSH, then you must access the system console through the controller's Maintenance port.

### Before you begin

Ensure that you have access to the controller's Maintenance port ( RS-232 port ).

### Procedure

1. Connect an RS-232 cable from the controller's Maintenance port ( **RS-232 port** ) to your maintenance PC's serial port.
2. Open a communication application (for example, PuTTY, TeraTerm, ProCom, or Hyperterminal) and enter the connection parameters as follows:
  - **Connection type:** Serial
  - **Port:** Select the COM port that you have connected to; for example, COM1.
  - **Bits Per Second:** 9600

- **Data Bits:** 8
- **Parity:** None
- **Stop Bits:** 1
- **Flow Control:** None

Click on the communication application window and press the ENTER key.

3. If the login prompt is displayed, log in as *root*. If the login prompt is not displayed, verify that you are using the proper connection settings for the PC COM port and that the serial cable is connected properly on both ends. If the settings and connections are correct, power the controller off and power it back on after 30 seconds. You should observe the following reboot sequence:

U-Boot 2015.10 (Oct 25 2018 - 23:03:29 -0400) cxii 1.0.2.3

Reset Status:

CPU: e300c1, MPC8360EA, Rev: 2.1 at 396 MHz, CSB: 264 MHz

Board: Mitel CX-II, U-Boot 2015.10 (Oct 25 2018 - 23:03:29 -0400)

cxii 1.0.2.3

Refresh UBOOTROM

Watchdog enabled

DRAM:

Configuring DDR2 SODIMM using SPD drivers

DDR

Starting POST...

If you do not observe the login prompt after the reboot is complete, see [Password Recovery for 3300 ICP Controller](#).

4. Run the following command to capture the system's journal log into a file, */root/journal.log*: **journalctl --no-pager > journal.log** You may send *journal.log* to Mitel Product Support for analysis.
5. Run the following command to determine the active partition number of the controller:

**fw\_printenv ata\_active\_part**

6. Run the following command to swap the active partition of the controller with its inactive partition:

**fw\_setenv ata\_active\_part <disk partition>**

Here, **<disk partition>** is the number beside the current active partition number (output of the command in **Step 5**) as shown in [Table 4-1](#) for different 3300 ICP controllers.

**Example:** The active partition number (output of the command **fw\_printenv ata\_active\_part** in **Step 5**) of an MXe III controller is 1.

Then, to swap the active partition of the MXe III controller with its inactive partition, you must run the following command with the *disk partition* parameter set to **2**:

**fw\_setenv ata\_active\_part 2**

7. Run the following command to reboot the system:

**reboot**

8. If the system is now able to boot the MiVoice Business software from its HDD, sync the system licenses with the AMC server through the Server Manager (**ServiceLink > Status**).
9. If the system is unable to boot the MiVoice Business software from its HDD after the swap, see [Unable to Recover the MiVoice Business System from Active and Inactive Partitions](#).
10. After syncing system licenses with the AMC server, upgrade the MiVoice Business system to the required software version through the Server Manager if needed (**ServiceLink > System Upgrade**).

11. Restore the most recent database using the Server Manager ( **Administration > Restore**).

## Password Recovery for 3300 ICP Controller

### Overview

If you are unable to log in to the Server Manager or the system (SSH or the Maintenance port), then you must perform a password recovery.

### Before you Begin

Ensure that you do the following:

- Verify that you have access to the Maintenance port ( **RS-232 port**).
- Verify that the controller is powered on.

### Procedure

**NOTE:** The system will be offline for the entire duration of the following procedure.

1. Connect an RS-232 cable from the controller's Maintenance port ( **RS-232 port**) to your maintenance PC's serial port.
2. Open a communication application (for example, PuTTY, TeraTerm, ProCom, or Hyperterminal) and enter the connection parameters as follows:
  - **Connection type:** Serial
  - **Port:** Select the COM port that you have connected to; for example, COM1.
  - **Bits Per Second:** 9600
  - **Data Bits:** 8
  - **Parity:** None
  - **Stop Bits:** 1
  - **Flow Control:** None
3. Reboot the controller by powering it off, and then powering it on. Stop the auto-boot sequence from the serial port (Maintenance port), by pressing the SPACE key three or more times consecutively within 7 seconds at the following message:  
**Press <SPACE> key 3 times within 7 seconds to stop autoboot.**  
The system displays => prompt when the auto-boot sequence stops.
4. At the U-Boot command prompt, run the following command to modify the value of the bootcmd variable:  
**=>set bootcmd run load\_ata\_resetpasswd**
5. Run the following command to check whether the bootcmd variable has been modified successfully:  
**=>print bootcmd**  
The output of the above command should be:  
**bootcmd=run load\_ata\_resetpasswd**
6. Run the following command to boot the system:  
**=>boot**
7. After booting, the system enters in to the rescue mode and the following prompt is displayed:

**sh-4.3#**

8. At the rescue mode prompt, run the following command and then press ENTER to change the root password:

**sh-4.3# passwd**

9. Type a new password, and retype the new password for confirmation:

**Enter new UNIX password:**

**Retype new UNIX password:**

The password should get updated successfully.

10. At the rescue mode prompt, run the following command and then click ENTER to change the admin password:

**sh-4.3# passwd admin**

11. Type a new password, and retype the new password for confirmation:

**Enter new UNIX password:**

**Retype new UNIX password:**

The password should get updated successfully.

12. After changing the passwords, force reboot the system by running the following command:

**sh-4.3# reboot -f**

13. After the reboot is complete, access the Server Manager using the new credentials.

## Unable to Recover the MiVoice Business System from Active and Inactive Partitions

If you are unable to recover the MiVoice Business software from both the active and inactive disk partitions, it might be due to disk corruption or disk failure:

- To resolve a disk corruption issue, see **Software Installation > Software Installation on 3300 ICP Controller > Install System Software Manually on 3300 ICP Controller** in the *MiVoice Business Technician's Handbook*.
- To resolve a disk failure issue, see **Install and Replace Units > Hard Drives** in the *MiVoice Business Technician's Handbook*.

## Reset the VoiceAdmin Password

### Overview

If you are unable to log in to the System Administrator Tool as the voiceadmin user, then you can reset the password for voiceadmin.

### Procedure

1. Log in to the Server Manager as admin user.
2. Under **Administration -> System users**, modify the password for the voiceadmin user.

# Reset the System Admin Password

## Overview

If you are unable to log in to the System Administration Tool as the *system* user, then you can reset the password for *system*.

## Procedure

1. Log in to the system through SSH (for example, through PuTTY) as the *root* user.
2. Run the following command to reset the *system* password:  
**mcdDebug ResetLoginPassword system**
3. Press CTRL + C to exit the mcdDebug shell.
4. Run the following command to log out of the system:  
**logout**

## Backups and Restores

**Table 4.3:** Backup and Restore Troubleshooting (Sheet 1 of 4)

Symptom	Possible Cause	Corrective Action
Backup fails and a Backup Failure alarm generated/ "Backup process has failed" message displayed in Scheduler Event Details.	Database verification has failed, and an Audit Failure alarm was raised. OR An active Audit Failure alarm already exists.	Perform a system restore to clear the Audit Failure alarm. Ensure that you are restoring an uncorrupted database.
	There is not enough disk space - the backup device does not have enough disk space.	If possible, select an alternate backup device or make room on the desired backup device. If there is a hardware issue with the drive, replace the drive.
	Failure to copy files during the backup.	
	Failure to create a .tar file during the backup.	

**Table 4.3:** Backup and Restore Troubleshooting (Continued) (Sheet 2 of 4)

Symptom	Possible Cause	Corrective Action
Backup/restore failure (only fail to FTP files between PC). <b>NOTE:</b> If Java Plug-in console view is enabled, you should see the security warning.	Java version is not correct OR Higher version of Java is installed.	<ol style="list-style-type: none"> <li>1. Verify that the correct version of Java is installed (Mitel supports Java 1.6.0_1 or later).</li> <li>2. If another version is installed, remove it, re-install the correct version, and reboot the PC.</li> </ol>
	Incompatible web browser installed.	<ol style="list-style-type: none"> <li>1. Verify that the correct version of Mozilla Firefox, Google Chrome, or Microsoft Edge is installed. MiVoice Business 9.0 supports Firefox 36.0.4 and above, Chrome 59 and above, and Edge 38 and above.</li> <li>2. If another version is installed, remove it, re-install the correct version, and reboot the PC.</li> </ol>
	Backup/restore applet is not trusted (identitydb.obj not on PC).	<ol style="list-style-type: none"> <li>1. Go to the Backup or Restore forms in System Administration Tool (Maintenance and Diagnostics).</li> <li>2. Click the link to download the <b>identitydb.obj</b> file to the Maintenance PC. Save the file in:   <u>For Windows NT:</u>            WINNT/Profile/ &lt;username&gt;  <u>For Windows 2000:</u>            Documents and Settings/&lt;user-name&gt;         </li> </ol>
	Backup/restore applet is not trusted (identitydb.obj not in right directory).	Verify the file is in the correct <username> profile (the profile used to log onto the PC).
	Backup/restore applet is not trusted (identitydb.obj has wrong extension).	Verify that the extension of the file is .obj (not .obj.obj, or .obj.txt, or anything else). <b>Tip:</b> Disable the Hide file extensions for known file types option to see the complete extension of the file. In the folder window, select: <u>For Windows NT:</u> View/Options/View. <u>For Windows 2000:</u> Tools/Folder Options/View

**Table 4.3:** Backup and Restore Troubleshooting (Continued) (Sheet 3 of 4)

Symptom	Possible Cause	Corrective Action
FTP server responds with "permission denied" when attempting to write the backup file to the target directory.	FTP account missing DELETE permission on target directory.	Assign DELETE (in addition to WRITE) permission to FTP account, then retry backup. See KB article 11-5191-00244 for additional information.
Database backup fails	Lack of free space in the vmail partition.	Delete Voice mails until there is enough space for the backup. To determine whether there is enough space for backup, see <a href="#">Determine whether there is enough space for backup</a> .
During a system database backup or restore you receive the following error message: "RAD group must be a number that will be DATA RESTORED before the pilot number".	The leading digit of the hunt group number is lower than its RAD group number, so the system is unable to back up or restore the RAD group.	Program the leading digits of the hunt group pilot number to be greater than its RAD group numbers. When the system backs up or restores Hunt Groups, it does so in the order of the leading digits of the hunt group pilot number. See Hunt Groups in the System Features book of the System Administration Tool online help.
Unable to restore database	Attempting to restore a database from an AX Controller to a different type of controller.	You must restore an AX Controller database to an AX Controller.
Unable to browse to the backup file from the Restore dialog box	Your computer has does not have the required Java Plug-in version.	Install Java Plug-in version 1.6.0_01 or later. To browse for the backup file and to perform a backup, your current user account on the computer must have Java Plug-in version 1.6.0_01 or later installed.
Unable to perform a Data Restore from the Data Restore dialog box		Install Java Plug-in version 1.6.0_01 or later.
Unable to rename a new folder that you just created within the Backup dialog box or Restore dialog box.		Install Java Plug-in version 1.6.0_03 or later.



**Table 4.3:** Backup and Restore Troubleshooting (Continued) (Sheet 4 of 4)

Symptom	Possible Cause	Corrective Action
You receive the following message when you attempt to restore a database: "RAD group must be a number that will be DATA RESTORED before the pilot number."	The leading digits of the hunt group pilot number are a lower number than its RAD group numbers. When the system backs up or restores Hunt Groups, it does so in the order of the leading digits of the hunt group pilot number. If the leading digit of the hunt group number is lower than its RAD group number, the system will be unable to back up or restore the RAD group data.	In the Hunt Groups form, program the leading digits of the hunt group pilot number to be greater than its RAD group numbers.
You perform a database restore and ACD 2000 agent skill groups are missing from the database after the restore.	If the Extended Agent Group option is enabled and you have more than 128 agent skill groups programmed, when you perform a database backup, only the first 128 groups are saved.	Only the first 128 agent groups were saved to the database backup. Manually reprogram the missing agent groups

If you still can't fix the problem, call Technical Support. Make sure you have the following information on hand before calling:

- Java plug-in version
- Maintenance PC username
- Maintenance PC IP address
- Location of identitydb.obj file on the Maintenance PC
- Postsoftware or journalctl logs

## Determine whether there is enough space for backup

1. On a rough sheet of paper, create a table as shown in the following figure.

Current Voice Mail Size	2xCurent Voice Mail Size	Backup File Size	Available Space	Backup File Size + Available Space

2. To determine the current Voice Mail size, connect to the system using the SSH protocol through a communication application (for example, PuTTY).
3. Log in as root user.
4. At the `root@<system name>:~#` prompt, run the following commands:
 

```
du -hs /vmail/d/vm/grp
```

**Sample System Output:**

```
2.7G /vmail/d/vm/grp
```

In this example, the current Voice Mail size is 2.7 GB. Note down this value under the **Current Voice Mail Size** column.
5. Multiply the current Voice Mail value by 2. For example, 2.7 GB x 2= 5.4 GB. Note down this value under the **2x Current Voice Mail Size** column.
6. To determine the space on last backup file, run the following commands:
 

```
/vmail# du -hs /vmail/temp
```

**Sample System Output:**

```
5.3G /vmail/temp
```

For example, the backup file size is 5.3 GB. Note down this value under the **Backup File Size** column.

**NOTE:** If there is no backup file, then use 0 as the value.
7. To determine the available free space, run the following commands:
 

```
/vmail# df -h /vmail
```

**Sample System Output:**

```
Filesystem Size Used Avail Use% Mounted on
/dev/sda5 15G 8.5G 5.0G 63% /vmail
```

For example, the available space is 5 GB. Note down this value under the **Available Space** column.
8. Add the **Backup File Size** and **Available Space** values.

For example, 5.3 GB + 5 GB = 10.3 GB. Note down this value under the **Backup File Size + Available Space** column.

Current Voice Mail Size	2xCurent Voice Mail Size	Backup File Size	Available Space	Backup File Size + Available Space
2.7 GB	5.4 GB	5.3 GB	5 GB	10.3 GB

9. If the **2x Current Voice Mail Size** value is **greater** than the sum of **Backup File Size** and **Available Space** values, then you must delete Voice Mail messages before you perform a backup.

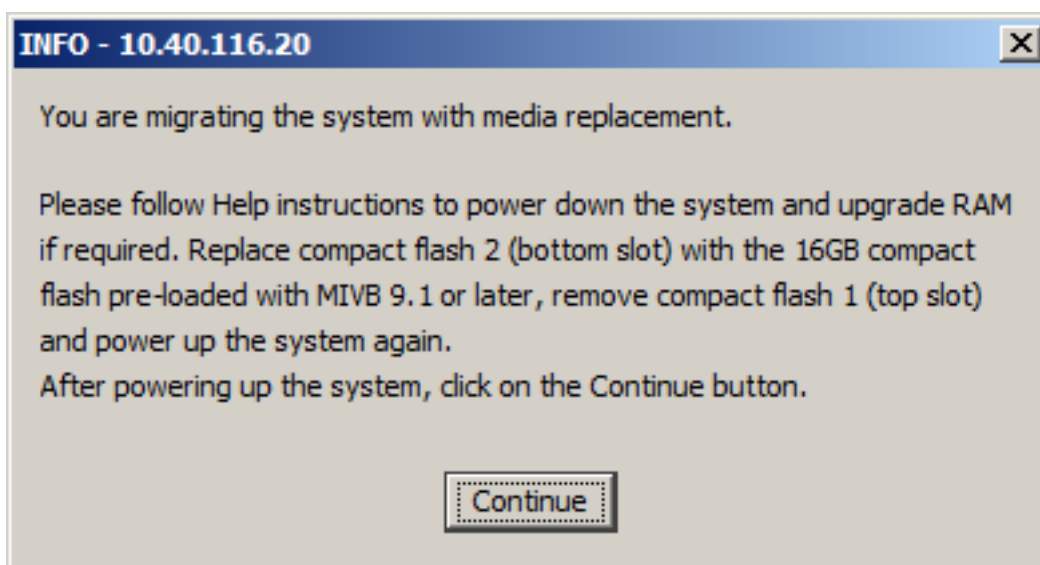
If the **2x Current Voice Mail Size** value is **lesser** than the sum of **Backup File Size** and **Available Space** values, then you can back up Voice Mail messages.

# Migration

## Reverse Migration

### Reverse Migration of an AX Controller if the 16 GB CF is Unavailable or Corrupt

During the migration of an AX controller, the Migration Tool instructs you to replace the current 2 GB/4 GB CF combo with a 16 GB CF:



Follow the reverse migration procedure below if:

- at this time, you do not have a 16 GB CF pre-loaded with MiVoice Business 9.1 software, or
- you have removed the 2 GB/4 GB CF combo and inserted the 16 GB CF into the Compact Flash 2 slot, but the AX controller does not boot (16 GB CF may be corrupt).

**NOTE:** You may also follow the reverse migration procedure below to a pre-MiVoice Business 9.0 Release if the 16 GB CF of your AX controller stopped working /became corrupt during normal operation, and you have the 2 GB/4 GB CF combo that was used at the time of migration of this AX controller to MiVoice Business Release 9.1 or later.

#### Before you begin

Ensure that the 2 GB/4 GB CF are in the slots, Compact Flash 2 and Compact Flash 1 respectively.

**NOTE:** If you had removed the 2 GB and 4 GB CF and installed the 16 GB CF, then re-install the 2 GB/4 GB CF combination by powering down the system, removing the AX controller card, removing the 16 GB CF, re-inserting the 2 GB CF and the 4 GB CF into the slots: Compact Flash 2 and Compact Flash 1 respectively, re-inserting the controller card into the chassis and powering up the system up.

#### Procedure

1. Power the controller down.
2. Access the Maintenance port of the AX controller (See **Ch 6, Maintenance > Access 3300 ICP Controller through the Maintenance Port** in the *MiVoice Business Technician's Handbook*).

3. Power the controller up.
4. 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 => prompt when the auto-boot sequence stops.

5. Run the following commands from the U-Boot command prompt:

```
setenv vxworks_bootfile DEV_RTC8260
setenv vxworks_active_partition 1
fatload ide 0:1 8000000 DEV_RTC8260
```

6. If the fatload command succeeds, skip this step. If the fatload command fails, re-run the last two commands with the partition number set to 4:

```
setenv vxworks_active_partition 4
fatload ide 0:4 8000000 DEV_RTC8260
```

7. After the fatload completes successfully, run the following commands to boot the VxWorks development image:

```
run vxworksargs_ata
bootvx 8000000
```

8. After the VxWorks development image boots, run the following commands to reflash both bootrom and FPGA:

```
Upgrade_Bootrom
Upgrade_Xilinx
```

9. Run the following command to verify and update bootline if needed:

```
bootChange
```

Ensure that the partition number parameter is set to the partition number associated with the successful fatload command in Step 6 (or Step 7), and that the file name is set to RTC8260.

10. Reboot the system:

```
reboot
```

The pre-9.0 MiVoice Business load that was running on the AX Controller before the migration attempt starts booting.

## U-Boot based E2T card in MxIII cannot boot E2T8260 Image after Reverse Migration

This section applies only to MxIII systems featuring an E2T card with U-Boot as the bootloader.

If the E2T card does not come up and connect to the RTC card (running a pre-9.0 MiVoice Business release) after 10 minutes of executing Step 1 of the procedure, **Ch. 6, Appendix A: Reverse Migration > Reverse Migration of an E2T Card** in the *Migration Guidelines* document, first verify that you have indeed copied the **E2T8260** file from `/sysro` to `/sysro/tftp` directory; if you did, you must access E2T card's serial port to attempt the recovery.

**NOTE:** In pre-9.0 MiVoice Business releases, to access the E2T card's serial port from the printer port, you must execute the `redirectPrinter 3` command from the RTC card's shell first. Alternatively, you may access E2T card's serial port via secure telnet to RTC card's IP address, port 2007.

Once you get access to the E2T card's serial port, press ENTER several times to check for any response. If you get no response, reset the E2T card by running the `ToggleCpu 1` command from the RTC shell.

Then, observe the output from the E2T card's serial port and stop the auto-boot by pressing SPACE key three or more time consecutively after you observe the following message on the E2T card console:

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

After you stop the auto-boot, execute run the `ubootprint` command to verify boot parameters of the E2T card. If the `bootcmd` parameter has the value **run loade2t\_dhcp**, then the E2T card was configured to use the DHCP protocol to get its networking configuration and boot image; in this case, `bootcmd` is the only boot parameter that matters on the E2T card.

If the `bootcmd` has value **run loade2t\_static**, then the E2T card was configured to use the static IP configuration; in this case, see **Ch. 6, Maintenance > Configure U-Boot Networking Parameters of the E2T Card > Static IP** in the *Technician's Handbook* to verify whether you've configured the networking parameters correctly.

There are two categories of error conditions:

- The E2T card cannot download the **E2T8260** image from the RTC card
- The E2T card downloads the **E2T8260** image but cannot run it successfully

### E2T card cannot download E2T8260 image from the RTC card

For an error from the first category, you will observe the text: "TFTP error: " followed by an error number. The TFTP error codes are as per **TFTP RFC-1350**. For example:

```
TFTP from server 10.38.72.230; our IP address is 10.38.72.231
Loading: *
TFTP error: '' (1)
Not retrying...
Could not load E2T8260...
```

In the above example, the E2T card with IP address 10.38.72.231 is attempting to TFTP the file, **E2T8260** from the TFTP server 10.38.72.230, and **error (1)** means "File not found" indicating that the file **E2T8260** was not found on the TFTP server 10.38.72.231; this could be because the IP address of the TFTP server is incorrect, or the file is not in the `/sysro/tftp` directory on the RTC card (ensure that you have copied the **E2T8260** image from the `/sysro` directory to the `/sysro/tftp` directory in the right MxI system).

If your E2T card is configured to use DHCP (`bootcmd` parameter is **run loade2t\_dhcp** and the DHCP server is configured to direct the card to the RTC card's IP address to the **E2T8260** image), then the E2T card should be able to download the image from the RTC card.

If your E2T card was configured to use static IP configuration (`bootcmd` parameters is **run loade2t\_static**), and you observe "TFTP error:" message, verify that you have configured E2T card's networking parameters correctly; see **Ch. 6, Maintenance > Configure U-Boot Networking Parameters of the E2T Card > Static IP** in the *Technician's Handbook*.

### E2T card downloads the E2T8260 image but cannot run it successfully

For an error from the second category, the E2T card downloads the **E2T8260** image but encounters difficulty running it.

If the E2T card crashes trying to run **E2T8260**, verify that you have transferred the **E2T8260** file in binary mode rather than the default ASCII (that is, if you've used an FTP app to ftp the file to `/sysro/tftp`).

If you observe the following message on the E2T card's console for more than a minute:

```
## Starting vxWorks at 0x00010000 ...
```

This means that the card's bootloader has downloaded the **E2T8260** image and transferred control to it, but the **E2T8260** image is stuck; this in turn, usually indicates an invalid bootline in FLASH. To recover, you must force bootline update by executing the following procedure:

1. From the RTC card's shell reset the E2T card by executing the `ToggleCpu 1` command.
2. From the E2T card's serial port, stop the autoboot.
3. From the E2T card's shell, execute the following commands:

```
setenv updatebootline yes
saveenv
reset
```

The `reset` command will trigger the reset of the E2T card. The E2T card should now boot successfully and connect to the RTC Card.

## U-Boot based E2T card in MxIII cannot boot E2T8260 Image after Reverse Migration

This section applies only to MxIII systems featuring an E2T card with U-Boot as the bootloader.

If the E2T card does not come up and connect to the RTC card (running a pre-9.0 MiVoice Business release) after 10 minutes of executing Step 1 of the procedure, **Ch. 6, Appendix A: Reverse Migration > Reverse Migration of an E2T Card** in the *Migration Guidelines* document, first verify that you have copied the **E2T8260** file from `/sysro` to `/sysro/ftp` directory; if you did, you must access E2T card's serial port to attempt the recovery.

**NOTE:** In pre-9.0 MiVoice Business releases, to access the E2T card's serial port from the printer port, you must execute the `redirectPrinter 3` command from the RTC card's shell first. Alternatively, you may access E2T card's serial port via secure telnet to RTC card's IP address, port 2007.

Once you get access to the E2T card's serial port, press ENTER several times to check for any response. If you get no response, reset the E2T card by running the `ToggleCpu 1` command from the RTC shell. Then, observe the output from the E2T card's serial port and stop the auto-boot by pressing SPACE key three or more time consecutively after you observe the following message on the E2T card console:

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

After you stop the auto-boot, execute run the `ubootprint` command to verify boot parameters of the E2T card. If the `bootcmd` parameter has the value **run loade2t\_dhcp**, then the E2T card was configured to use the DHCP protocol to get its networking configuration and boot image; in this case, `bootcmd` is the only boot parameter that matters on the E2T card.

If the `bootcmd` has value **run loade2t\_static**, then the E2T card was configured to use the static IP configuration; in this case, see **Ch. 6, Maintenance > Configure U-Boot Networking Parameters of the E2T Card > Static IP** in the *Technician's Handbook* to verify whether you've configured the networking parameters correctly.

There are two categories of error conditions:

- The E2T card cannot download the **E2T8260** image from the RTC card
- The E2T card downloads the **E2T8260** image but cannot run it successfully

### E2T card cannot download E2T8260 image from the RTC card

For an error from the first category, you will observe the text: "TFTP error: " followed by an error number. The TFTP error codes are as per **TFTP RFC-1350**. For example:

```
TFTP from server 10.38.72.230; our IP address is 10.38.72.231
Loading: *
TFTP error: '' (1)
Not retrying...
Could not load E2T8260...
```

In the above example, the E2T card with IP address 10.38.72.231 is attempting to TFTP the file, **E2T8260** from the TFTP server 10.38.72.230, and **error (1)** means "File not found" indicating that the file **E2T8260** was not found on the TFTP server 10.38.72.231; this could be because the IP address of the TFTP server is incorrect, or the file is not in the `/sysro/tftp` directory on the RTC card (ensure that you have copied the **E2T8260** image from the `/sysro` directory to the `/sysro/tftp` directory in the right Mx e III system).

If your E2T card is configured to use DHCP ( `bootcmd` parameter is **run loade2t\_dhcp** and the DHCP server is configured to direct the card to the RTC card's IP address to the **E2T8260** image), then the E2T card should be able to download the image from the RTC card.

If your E2T card was configured to use static IP configuration ( `bootcmd` parameters is **run loade2t\_static**), and you observe "TFTP error:" message, verify that you have configured E2T card's networking parameters correctly; see **Ch. 6, Maintenance > Configure U-Boot Networking Parameters of the E2T Card > Static IP** in the *Technician's Handbook*.

### E2T card downloads the E2T8260 image but cannot run it successfully

For an error from the second category, the E2T card downloads the **E2T8260** image but encounters difficulty running it.

If the E2T card crashes trying to run **E2T8260**, verify that you have transferred the **E2T8260** file in binary mode rather than the default ASCII (that is, if you've used an FTP app to ftp the file to `/sysro/tftp`).

If you observe the following message on the E2T card's console for more than a minute:

```
## Starting vxWorks at 0x00010000 ...
```

This means that the card's bootloader has downloaded the **E2T8260** image and transferred control to it, but the **E2T8260** image is stuck; this in turn, usually indicates an invalid bootline in FLASH. To recover, you must force bootline update by executing the following procedure:

1. From the RTC card's shell reset the E2T card by executing the `ToggleCpu 1` command.
2. From the E2T card's serial port, stop the autoboot.
3. From the E2T card's shell, execute the following commands:

```
setenv updatebootline yes
saveenv
reset
```

The `reset` command will trigger the reset of the E2T card. The E2T card should now boot successfully and connect to the RTC Card.



# System Features

## System Features Troubleshooting Tips

If you have programmed a system feature and the feature is not functioning as expected, ensure that:

- the feature is supported for the type of phone. Check the Phone-Feature matrix in the System Administration Tool online help to determine if a feature is supported on a specific phone type.
- you have programmed the feature correctly and reviewed the conditions that apply to the feature. Feature descriptions, conditions, and programming information are provided in the System Features book of the System Administration Tool online help.
- the feature is enabled in the Class of Service (COS) that has been assigned to the phone.
- the Class of Restriction (COR) assigned to the phone is not preventing the feature from operating.
- System timers are set accordingly to allow system to activate feature (for example, Camp-on).
- the feature access code is programmed in the Feature Access Codes form and you have entered the Feature Access Code correctly, if the feature is activated via a feature access code.
- another feature previously enabled on the phone isn't preventing the current feature from functioning. For example, Do Not Disturb could prevent a phone from receiving a call.
- you have enabled the feature on the correct system, if you have multiple systems interconnected in a network.

The tables in the following sections provide specific feature troubleshooting information.

## Features A to B

**Table 5.1:** Troubleshooting Features A to B (Sheet 1 of 3)

Feature	Symptom	Possible Cause	Corrective Action
Add Held	Unable to add a help call.	Record-a-Call is enabled on the phone. The Record-A-Call prompt takes precedence over the Add Held prompt.	Disable Record-a-Call feature in the Class of Service Options form.
	Unable to add a held call to a conference call on hold.	Functionality not supported.	None. Not supported on system.



**Table 5.1:** Troubleshooting Features A to B (Continued) (Sheet 2 of 3)

Feature	Symptom	Possible Cause	Corrective Action
Alpha Tagging	Alpha tagging not present on display phone for incoming calls.	Not supported for trunk type.	Only PSTN calls on the following trunk types support alpha tagging: LS Class, T1/D4, T1 CAS, T1 PRI, T1 QSIG, E1 PRI, E1 R2, E1 QSIG, and E1 BRI.
		Alpha Tagging entries not programmed in Telephone Directory form	Program alpha tagging entry for external telephone number
		Alpha Tagging not enabled in System Options form.	Enable option.
		Incoming signaling indicates that the caller's identity is private.	None. Not supported.
Advice of Charge	Not functioning.	Attempting to implement on non-European site.	None. Not supported in North America. Only supported with the Euro-ISDN (Euro-Standard variant) and Euro-BRI protocols.
		Carrier that provides the ISDN services is not delivering meter pulses for all applicable ISDN links.	Contact carrier.
		The specific variant of Advice of Charge is not supported by the system.	Refer to Advice of Charge in the System Administration Tool online help for a list of the supported variants.

**Table 5.1:** Troubleshooting Features A to B (Continued) (Sheet 3 of 3)

Feature	Symptom	Possible Cause	Corrective Action
Auto Answer	No audio over speakerphone.	Phone is not equipped with a speaker (for example, 5302 IP Phone).	Install a model of phone that has a speaker.
		Not supported for set type (for example, 5560 IPT and SpectraLink Wireless handsets do not support Auto Answer).	Refer to Phone-Feature Matrix in System Administration Tool online help.
		Call received from an incoming trunk where the set is programmed as the trunk's first answer point (e.g., DID or DIL).	None. Not supported.
		Call received from a trunk that is not programmed to provide release supervision.	None. Not supported.

## Features C

**Table 5.2:** Troubleshooting Features (Sheet 1 of 7)

Feature	Symptom	Probable Cause	Corrective Action
Caller Based Routing	Incoming Public Switched Telephone Network (PSTN) calls troubleshooting	The Caller ID of the incoming call does not match the CRS query.  Incorrect destination number.	Verify the caller ID for incoming DID number using the following commands: <ul style="list-style-type: none"> <li>• CRS QUERY ALLOW-LIST</li> <li>• CRS QUERY DENY-LIST</li> </ul>
	Duplicate Allow-list and Deny-list entries causing routing failure.	In some cases, the SDS Synchronization can result in duplicate entries for Allow-list and Deny-list being created, causing Allow-list and Blacklist routing to fail. The unique entry verification is done in the Caller Based Routing Service form rather than the Caller Recognition Service (CRS) form. This might result in conflicting entries.	To remove the conflicting duplicate entries, do the following: <ol style="list-style-type: none"> <li>1. Enable SDS Debug using the <b>SDSDEBUG ON</b> maintenance command.</li> <li>2. Delete the duplicate entries from the Caller Recognition Service form under the SDS Debug branch of the tree.</li> <li>3. Disable SDS Debug using <b>SDSDEGUB OFF</b> maintenance command.</li> </ol>

**Table 5.2:** Troubleshooting Features (Continued) (Sheet 2 of 7)

Feature	Symptom	Probable Cause	Corrective Action
Call Forwarding	Unable to forward call between two internal phones.	Forwarding station and the destination station are not allowed to call each other.	Ensure that the forwarding station and the destination station are permitted to connect to one another in Interconnect Restriction Table.
	Cannot forward calls to a tenant.	One or both tenants do not have permission to call each other (that is, each tenant has granted the other tenant calling permission).	Program both tenants to allow them to call each other. See Tenanting in the System Administration Tool online help information on tenant permissions.
	CFFM or Call Forward - No Answer not behaving as expected.	Set is a member of a Hunt Group. The options for CFFM and Call Forwarding are set differently in the Hunt group COS than the COS of the set.	<p>The Hunt Group COS (or, if no Hunt Group COS is programmed, the COS of the first member of the Hunt Group) is used for the following COS options:</p> <ul style="list-style-type: none"> <li>• Call Reroute after CFFM to busy destination</li> <li>• COV/ONS/E&amp;M Voice Mail Port</li> <li>• ONS/OPS Internal Ring Cadence for External Callers (only if the first member is ONS/OPS)</li> <li>• ANSWER PLUS - Delay To Message Timer</li> <li>• ANSWER PLUS - System Reroute Timer</li> <li>• Call Forward - No Answer Timer</li> </ul>

**Table 5.2:** Troubleshooting Features (Continued) (Sheet 3 of 7)

Feature	Symptom	Probable Cause	Corrective Action
	Call forwarding not functioning on a 5330 5340 or 5360 IP Phone.	User tried to program Call Forwarding using the <b>Superkey</b> .	Use the Call Forwarding application to program call forwarding on the 5320, 5330, 5340 and 5360 IP Phones.
	IP Set is forwarded to other destination for no apparent reason. "Locate Feature Extension" maintenance command from ESM does not show call forwarding active.	Call forwarding set up from associated Your Assistant application via MiTai event. MiVoice Business cannot detect and identify this type of call forwarding features using "Locate" maintenance command.	If the call forwarding is no longer valid or required, disable it for the IP set via YA.

**Table 5.2:** Troubleshooting Features (Continued) (Sheet 4 of 7)

Feature	Symptom	Probable Cause	Corrective Action
Call History	Calls not being logged.	<p>The following calls are not logged by the Call History feature:</p> <ul style="list-style-type: none"> <li>incoming ACD Calls and Personal calls from ACD agents</li> <li>calls to non-prime broadcast groups</li> <li>calls to a device that is forwarded/rerouted to "Always".</li> </ul>	None. Not supported.
	Unable to place calls to external numbers that are stored in your Call History list.	Outgoing prefix is required to dial the external number from Call History.	<p>If you have programmed a specific Call History feature button on the person's phone, you can add the prefix digits using the option "Outgoing External Call Prefix For Applications" in the System Options Assignment form.</p> <p><b>NOTE:</b> This solution does not work if Call History is accessed via one of the following keys:</p> <ul style="list-style-type: none"> <li>a Superkey/Blue button on a 52xx or 53xx phone</li> <li>the redial key on a 69xx phone</li> <li>the call history key on a 69xx phone</li> </ul>
	Caller name not displaying in Call History on 5140/5240 set for calls comes from NI-2 5ESS PRI.	Caller name not in the protocol message required by these sets.	None. Not supported.

**Table 5.2:** Troubleshooting Features (Continued) (Sheet 5 of 7)

Feature	Symptom	Probable Cause	Corrective Action
Call Pickup - Directed	Users cannot pick up calls from a set.	Class of Service option "Call Pickup - Directed: Accept" is not set to "Yes".	Set "Call Pickup - Directed: Accept" to "Yes" in the Class of Service of the ringing set.
	User unable to pick up calls from Attendant Console.	Class of Service option "Allow Directed Call Pickup of Attendant Call" not enabled.	Enable "Allow Directed Call Pickup of Attendant Call" in the Class of Service Options form of the user's set.
Call Pickup - Clustered	Remote elements that host the clustered call pickup group are not updated with a directory number change after an SDS synchronization. An SDS updates error is generated in the System Administration Tool to alert you that the change was not made on the remote elements.	You must remove a member from a clustered pickup group, before you change the member's directory number; otherwise the remote elements that host the clustered call pickup group will not be updated with the change by an SDS synchronization.	Refer to the Call Pickup -Clustered topic in the System Administration Tool online help for instructions.
Camp-on	Unable to camp-on to a group.	Maximum number of allowable camp-ons to a group is exceeded.	Try again at a later time. The maximum number of camp-ons to a group per 3300 ICP is set at 84.
Clear All Features.	Feature not cancelled by code.	<p>"Clear All Features" code does not cancel all features. It will not cancel:</p> <ul style="list-style-type: none"> <li>• Hold (any type)</li> <li>• Account Codes (voice or data)</li> <li>• Rerouting</li> <li>• Callbacks set against your station</li> <li>• Message waiting notifications.</li> </ul>	Ensure that the "Clear all Features" code supports the cancellation of the set feature.

**Table 5.2:** Troubleshooting Features (Continued) (Sheet 6 of 7)

Feature	Symptom	Probable Cause	Corrective Action
Conference	Unable to establish join a conference.	The maximum number of callers in a single conference (maximum of 8) has been reached	Refer to the Conference feature in the System Administration Tool online help for the conference limitations for your 3300 ICP controller.
	Unable to establish a conference.	Maximum number of conferences that you system can support has been reached.	
	Cannot make conference call from single line set.	If COS option Call-Waiting Swap is enabled, user cannot make conference call from single line set. This is because Call-Waiting Swap overrides the conference feature.	Disable Call-Waiting Swap in the COS.
	Cannot create a conference between two external PSTN callers.	Incorrect Calling Line Identification (CLID) is being sent to third party.	Enable "Replace External CLID" in ISDN Protocol form of trunk.
Conference Split	Unable to split a conference call.	Split cannot be activated from a telephone when: <ul style="list-style-type: none"> <li>the attendant is involved in the conference</li> <li>a member of the conference has a party on Consultation Hold</li> </ul>	Ensure call conditions support the Conference Split feature.



**Table 5.2:** Troubleshooting Features (Continued) (Sheet 7 of 7)

Feature	Symptom	Probable Cause	Corrective Action
		<ul style="list-style-type: none"> <li>the conference is on Hold</li> <li>a member of the conference has a party camped-on</li> <li>members of the conference belong to the same Key System Group</li> <li>you are in select features or display mode</li> <li>there are more than three members in the Conference.</li> </ul>	

## Features D to G

**Table 5.3:** Troubleshooting Features D to G (Sheet 1 of 5)

Feature	Symptom	Probable Cause	Corrective Action
DID Service	Incoming calls troubleshooting	<p>Incoming DID number does not match the CRS query.</p> <p>Incorrect destination number.</p>	<p>Enable CCS Trace and verify that incoming DID number matches the one for which CRS query was made. Using CRSQUERY command, verify the destination number for incoming DID number.</p>

**Table 5.3:** Troubleshooting Features D to G (Continued) (Sheet 2 of 5)

Feature	Symptom	Probable Cause	Corrective Action
	Multiple match, partial match, and conflict match in the CRS form	Incorrect or no destination number is assigned to the DID number	Monitor software/audit logs for such scenarios. Use CRS SHOW command to search the CRS database for DID internal DNs to find the matching entries for the specified service type.
Direct Page	Phone user did not receive a Direct Page.	Handsfree Answerback is only available on some phones.	Only phones with a built-in speaker can receive one. See The Phone -Feature Availability matrix in the System Administration Tool online help for more information.
		IP Phone user is on a call on the analog line of the Line Interface Module.	Ensure analog line of Line Interface module is not in use at the time of the page.
		The paged phone has a call on soft hold (i.e. transferring a call).	Ensure paged phone was not on soft hold when page was initiated.
		The paged telephone is engaged in a handsfree call.	Ensure user was not engaged in a handsfree call when the page was made.
		The user of the paged telephone is dialing a number when the Direct Page is received.	Ensure user was not dialing a number when the page was made.
	User hears reorder (busy) tone when attempting a direct page	The IP page group has exceeded the maximum limit of 64 IP devices.	Reduce the number of IP-device members to 64 or less.

**Table 5.3:** Troubleshooting Features D to G (Continued) (Sheet 3 of 5)

Feature	Symptom	Probable Cause	Corrective Action
		One or more IP sets has reset during paging setup.	Ensure that none of the sets that you attempted to page are in the process of being reset.
DSS/BLF key	Cannot program a DSS/BLF key.	You are trying to assign a directory number that does not already exist in the system.	Add the directory number in the Telephone Directory form before you assign the DSS/BLF key.
	In a clustered environment, error logs related to the DSS/BLF keys are being generated at the remote system.	The programming on the remote system is not complete.	Check that the DSS/BLF keys are programmed in the Remote Busy Lamps form on the remote system. If not, complete the DSS/BLF key programming on the remote system. See the Direct Station Select/Busy Lamp Field feature in the System Administration Tool online help for instructions.
	In a clustered environment, the button is not showing the person's status.	The Remote Host Set Directory Number is not listed in the Remote Busy Lamps form on the MiVoice Business system of the monitored extensions.	On the MiVoice Business system hosting the monitored extension, navigate to the Remote Busy Lamps form, and add the Remote Host Set Directory number.
	Phone is not ringing for entire ring cycle when a DSS/BLF key is used to place the call.	DSS/BLF key set to <b>Ring</b> which provides single burst ringing.	In the Multiline Set Keys form, set the DSS/BLF key to <b>Ring Cont</b> .

**Table 5.3:** Troubleshooting Features D to G (Continued) (Sheet 4 of 5)

Feature	Symptom	Probable Cause	Corrective Action
Do Not Disturb	Call rings set when DND enabled.	The calls are incoming external calls. Do Not Disturb (DND) only stops internal calls from ringing a user's telephone and returns busy tone to the caller.	None. Feature functioning correctly.
Embedded Unified Messaging (UM)	Feature not working system-wide.	Programming incomplete. Embedded UM must be provisioned at the user level in the VM Mailboxes form and at the system level in the Embedded UM Settings form.	Complete the required programming.
Feature key	Feature key programmed on set but it doesn't enable the feature.	For a feature key to function, you must complete the required programming for the specified feature. For example, for the DND feature key to function, you must program the DND feature through the System Administration tool forms.	See the System Features book in the System Administration Tool online help for feature programming.

**Table 5.3:** Troubleshooting Features D to G (Continued) (Sheet 5 of 5)

Feature	Symptom	Probable Cause	Corrective Action
Group page	Phone in Page Group does not receive page.	System restrictions prevent the phones from connecting with each other.	Ensure that COR and interconnect restrictions allow the paging and paged parties to connect.
		Number of supported IP Phones in the page group has been exceeded.	Ensure system has adequate resources to support paging requirements. Refer to the Engineering Guidelines for details
		Insufficient E2T resources to support the number of IP Phones.	
Groups - Key System and Multicall	Incoming call to Multicall Group does not ring Multicall line key on 5560 IPT.	The 5560 IP Turret cannot be a member of a Multicall group even though it can be assigned a Multicall line key in the Multiline Set Keys form.	None. Not supported.

## Features H to K

**Table 5.4:** Troubleshooting Features H to K (Sheet 1 of 2)

Feature	Symptom	Probable Cause	Corrective Action
Handset Receiver Volume	Handset receiver volume setting is not retained between calls.	“Handset Volume Adjustment - Saved” option is not enabled for the set.	Enable “Handset Volume Adjustment - Saved” option in the COS of the set.

**Table 5.4:** Troubleshooting Features H to K (Continued) (Sheet 2 of 2)

Feature	Symptom	Probable Cause	Corrective Action
Handsfree Operation	Called party cannot hear you clearly.	Microphone is obstructed.	Ensure that the microphone (on the front edge of the telephone) is unobstructed.
		Background noise	Minimize background noise (such as printers, fans, and radios).
		Too far away from phone	Sit within reach of the telephone.
		Speaking too quietly	Speak at a normal volume towards the microphone.
Hold	User unable to place DID On-Hold.	Users unable to put DID calls on hold when the COS of the set has Record-A-Call - Save Recording on Hang-up enabled.	Disable "Record-A-Call - Save Recording on Hang-up" option in the COS of the set.
Hunt Groups	Calls not ringing sets in expected order.	Incorrect "Hunt Group Mode" specified.	Ensure that the desired Hunt Group Mode (Circular or Terminal) is specified in the Hunt Groups form.
		Hunt group members are programmed in the wrong order in the Hunt Groups form.	Ensure that the member directory numbers are entered (listed) in the Hunt Groups form in the order that you want the calls distributed.

## Features L to O

**Table 5.5:** Troubleshooting Features L to O (Sheet 1 of 3)

Feature	Symptom	Probable Cause	Corrective Action
Loudspeaker Paging	Unable to perform loudspeaker paging	Attempting to perform Loudspeaker Paging feature in handsfree mode.	None. Loudspeaker Paging feature is not supported in handsfree mode.
	Long delay before system connects to loudspeaker equipment.	User is dialing one digit instead of two when paging a zone. Connection to the paging equipment is only made upon expiration of the inter-digit timer in the user's Class of Service. The default timer length is 10 seconds.	Inform user's to dial two digits (00 to 15) when paging a zone.
Message Waiting Indication	The MWI lamps on ONS sets fail to light when a message is left even though the circuit descriptor is configured to provide MWI.	Programming incomplete or incorrect.	<ol style="list-style-type: none"> <li>1. Verify that the circuit is assigned an ONS/OPS Circuit Descriptor that has the Message Waiting Lamp field on set to "Yes"</li> <li>2. Verify that CLASS/CLIP phones have a Class of Service with the ONS CLASS/CLIP Message Waiting field set to "Yes."</li> <li>3. Verify that non-CLASS/CLIP phones have a Class of Service with the ONS CLASS/CLIP Message Waiting field set to "No."</li> </ol>

**Table 5.5:** Troubleshooting Features L to O (Continued) (Sheet 2 of 3)

Feature	Symptom	Probable Cause	Corrective Action
	In a network of PBX platforms, where stations are programmed to have voice mailboxes off of a Message Server or Speech Server application that is centrally located at a main site, the MWI fails to show the presence of new messages at the stations.	After the System Option “Superset Callback Message Cancel Timer” expires, MWI is disabled. This timer is expiring before the message is noticed.	In a network of PBX platforms, where stations are programmed to have voice mailboxes off of a Message Server or Speech Server application which is centrally located at a main site, the System Option, “Superset Callback Message Cancel Timer” must be programmed to “blank” on all remote site PBX platforms. Otherwise, the MWI will be disabled once this timer expires.
Music on Hold	No music	Incorrect file format.	Save file in the following format: WAV, A-law or m-law (G.711), 8 kHz, 8-bit, mono.
		File too large.	See System Audio Files Update in the System Administration Tool online help for the maximum size of the audio files.
		Need to have ENABLE_TX_CHAN_CONN feature enabled.	
	Distortion	WAV file conversion introduced distortion rate.	When extracting a file from a CD (for a example, from your corporate Music on Hold CD) using a “CD ripper” application, choose a sampling rate as close as possible to 8 kHz. This should help prevent audio distortion introduced when converting a WAV file from a high sampling rate to a low sampling rate.



**Table 5.5:** Troubleshooting Features L to O (Continued) (Sheet 3 of 3)

Feature	Symptom	Probable Cause	Corrective Action
	Cannot download Audio Files to the 3300 ICP	The audio file cannot be located.	Verify that the audio file is not corrupted.
		The system greeting audio file is in the wrong language.	Download a file in the correct language using the System Audio File Updates form.
		A system error log is generated.	Verify that you are not attempting to download a file during a backup, restore or upgrade, or while somebody is recording the same greeting from a phone.
	Connection for IP music Source has failed	The directory number (DN) (configured as IP Music Source) is going out of service or not answering, when the MCD re-tries to connect this particular DN. The call drops due to a receiving side or network error.	None. The MCD retries to connect to the IP Music Source every 1 minute. When the MOH source is successfully restored, a log is generated stating "Connection for IP music source is restored".

## Features P to R

**Table 5.6:** Troubleshooting Features P to R

Feature	Symptom	Probable Cause	Corrective Action
Private Line Automatic Ringdown (PLAR)	Feature not functioning.	PLAR is only configured at one end of the connection.	Configure PLAR in the same manner at both ends of the connection.
		One or both systems have pre- 3300 Release 8.0 software.	Support for PLAR on E1 links is limited to systems with Release 8.0 or higher software. Upgrade systems to Release 8.0 or later.
Record a Call	Feature not available.	Advanced Voice Mail option not enabled. Record-A-Call requires the Advanced Voice Mail purchasable option.	Purchase and enable Advance Voice Mail option.
Ring Groups	Calls to group not overflowing to programmed call overflow destination directory number.	The directory number programmed as the overflow destination is invalid (unsupported directory number).	Program the ring group's overflow destination with a directory number from one of the following: <ul style="list-style-type: none"> <li>• station DNs</li> <li>• broadcast group DNs</li> <li>• attendant console DNs</li> <li>• system speed call number</li> <li>• hunt group DN</li> <li>• ring group pilot DN</li> </ul>

## Features S to V

**Table 5.7:** Troubleshooting Features S to V (Sheet 1 of 2)

Feature	Symptom	Probable Cause	Corrective Action
Telephone Directory Support	After exporting data to a Microsoft Excel spreadsheet, you are unable to open the spreadsheet.	PC settings require modification to allow file to be launched.	<p>To launch Excel Spreadsheets</p> <ul style="list-style-type: none"> <li>• Disable the pop-up blocker in your browser.</li> <li>• In Windows Explorer, click <b>Tools &gt; Folder Options</b>.</li> <li>• Click the <b>File Types</b> tab.</li> <li>• In the <b>Registered File Types</b> list, select the XLS Microsoft Excel Worksheet type.</li> <li>• Click the <b>Advanced</b> button.</li> <li>• Clear the <b>Browse in same window</b> box.</li> <li>• Check the <b>Confirm open after download</b> box.</li> <li>• Click <b>OK</b> , and then click <b>Close</b>.</li> </ul>
Transfer	Call cannot be transferred to an internal party.	Interconnect Restrictions prevent the two parties from connecting.	Modify Interconnect Restriction form to allow the two parties to connect.
Trunk Answer from any Station	Station user cannot pick up incoming call ringing at Night Bell directory number.	Interconnect Restrictions preventing station user from accessing incoming trunk.	Ensure that TAFAS stations have access to the incoming trunks in the Interconnect Restriction Table.

**Table 5.7:** Troubleshooting Features S to V (Continued) (Sheet 2 of 2)

Feature	Symptom	Probable Cause	Corrective Action
Speed Call - Pause	Dialing error occurs when using a speed call that is programmed with a pause. The digits proceeding the Pause are processed but the digits after the pause are not processed.	Pause in Speed Call is longer than the Inter-digit Timer.	Shorten the length the pause or increase the Inter-digit Timer in the Class of Service of the trunk.
Speed Call - Personal	User cannot store speed calls against index numbers.	User is trying store speed call number against single digit Index numbers. Index numbers must be two-digit numbers within your assigned range (00 to a maximum of 99).	When storing personal speed calls against index numbers, For numbers 0 to 9, add a leading zero. (For example, 00, 01, 02, 03 and so on).

# Trunking

## Trunk Troubleshooting Tips

- If all the circuits supported by a module or card are out of service, it is likely defective. If possible, swap the module or card with a known working module or card to confirm.
- For help with diagnosing digital trunk problems, see [Trunks](#).
- In the System Administration Tool, use the
  - Line Quality Measurement Tool to test Loop Start Trunks that are connected to the AX Controller Card Chassis, Analog Main Board, Analog Option Board, or ASU II.
  - Voice Quality Statistics form in combination with NetAlly (must be purchased separately) to identify voice quality problems and performance trends for IP phones.

## Analog Trunks

**Table 6.1:** Troubleshooting Analog Trunks (Sheet 1 of 4)

Symptom	Possible Cause	Corrective Action
System not receiving trunk calls.	Analog trunk issues.	Examine that the analog trunk is OK by using individual trunk access and testing on the frame. <b>NOTE:</b> On the EX platform, individual trunk access is not supported as ISDN, T1, and FXO trunks are not assigned trunk numbers when programmed.
	Answer point not programed.	Verify SMDR records to see which trunks have received incoming calls. Verify that the answer point is programmed correctly and is functional.
Outgoing calls are dropping after a couple of minutes into the conversation.	The system is not receiving answer supervision from the central office and is timing out.	If the Central office cannot provide answer supervision on answered calls, go to the CO Trunk Circuit Descriptors form and change the value in the field “fake answer supervision after outpulsing” to yes.

**Table 6.1:** Troubleshooting Analog Trunks (Continued) (Sheet 2 of 4)

Symptom	Possible Cause	Corrective Action
Unable to dial out a trunk.	No dial tone	Ensure dial tone is present from Central Office (CO). You can disable dial tone detection on the trunk to allow users to dial out on the trunk in the absence of dial tone.
Calls are connecting to the far end. Called party can hear caller, but calling party cannot hear party at far end.	The system is not receiving answer supervision immediately from the Central Office.	Go to the CO Trunk Circuit Descriptors form Change the Supervision parameters in the value field "audio inhibit until answer supervision after outpulsing" to No.
Trunks are programmed but are appearing as unassigned with the STAT location ID command.	Card has not had the information downloaded to update the status of the trunks.	Power off and on the information to the ASU at an appropriate time.
Ring is not heard immediately when external phone calls on LS trunk.	An external phone that is connected to the LS trunk rings four times before the receiving phone rings. When the class of service option ANI/DNIS Delivery Trunk is enabled, the system waits for the ANI information before making the phone ring. If this is not provided, the phone will not ring immediately.	In the COS of the LS trunk, disable <b>ANI/DNIS Delivery Trunk</b> .

**Table 6.1:** Troubleshooting Analog Trunks (Continued) (Sheet 3 of 4)

Symptom	Possible Cause	Corrective Action
Poor audio quality on LS trunk.	Incorrect country loss level plan.	In the License and Option Selection form, ensure that the Country field is set correctly for the system. The Country setting determines the default language, dialing plan, tone plan, and loss and level plan for the system. Refer to the Hardware Technical Reference Manual for tables that list the Loss Level Plans. You can also check with the Mitel Regional Sales office to find out the most appropriate setting for your region.
	Incorrect Balanced Network Setting or Trunk Category in the Trunk Circuit Descriptor form for the trunk.	Use the Line Quality Measurement tool in the System Administration Tool to determine the correct settings.
	Inadequate system grounding.	Ensure that the “Protective Ground” on the rear panel of the controller, ASU is connected to a solid ground. Refer to Appendix B in the Hardware Technical Reference Manual for additional grounding information.
Poor audio quality occurring intermittently on LS trunks.	If incoming calls arrive from trunks that are members of a trunk hunt group, an audio quality problem on a trunk in the group will appear as an intermittent problem on the phones.	Use the Line Quality Measurement tool in the System Administration Tool to check the settings of each LS trunk in the hunt group.

**Table 6.1:** Troubleshooting Analog Trunks (Continued) (Sheet 4 of 4)

Symptom	Possible Cause	Corrective Action
	Caller is using a cell phone that does not support the International Telephone Union (ITU-T) recommendation for the Send Loudness Rating (SLR).	If the caller is using a cell phone that has a low SLR, a user on the system will receive low audio. This is an issue with the caller's cell phone.
Poor audio quality on LS Trunk on a UK site.	Incorrect subscriber line has been provided by the carrier.	To ensure that the correct lines are provisioned in the UK, ensure that the Telco (e.g. BT), or carrier, provides 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.

## Digital Trunks

**Table 6.2:** Digital Trunk Troubleshooting (Sheet 1 of 10)

Symptom	Probable Cause	Corrective Action
<b>General</b>		
Excessive Bit Error Rate.	Faulty programming.	Make sure the system is programmed the same as the CO, for B8Zs or AMI.



**Table 6.2:** Digital Trunk Troubleshooting (Continued) (Sheet 2 of 10)

Symptom	Probable Cause	Corrective Action
Excessive Slips.	Faulty programming.	Ensure the Network Synchronization form is programmed and the system is clocking appropriately. Use the Netsync Summary maintenance commands to determine if synchronization is taking place. If not, use Net Set 1 to set off the first clock source or NET SET AUTO to select the best available clock source. After you choose a synchronization clock source always use the NET SET AUTO command to confirm.
System is not Receiving Calls.	The DID trunk digit modification number on the Trunk Attributes form does not have anything programmed in the absorb field. It MUST have a minimum of 0, or no calls will be accepted.	Ensure that there is an entry in the absorb field. It cannot be left Blank.
	Faulty ANI/DNIS programming.	Check ANI/DNIS programming to ensure there has not been confusion with a DID trunk. For ANI/DNIS to work the digit must be received from the Central Office as *ANI*DNIS*. If the digits are not being received in this format, turn off the ANI/DNIS in the Class of service Options.
Outgoing calls are dropping after a couple of minutes into the conversation.	System is not receiving answer supervision from the central office and is timing out.	If the Central office cannot provide answer supervision on answered calls go to the CO Trunk Circuit Descriptor Assignment and change the value in the field "fake answer supervision after outpulsing" to Yes.
Calls are connecting, and the far end can hear us but we cannot hear them.	System is not receiving answer supervision immediately from the Central Office.	In the CO Trunk Circuit Descriptors form, change the Supervision parameters in the value field "audio inhibit until answer supervision after outpulsing" to No.

**Table 6.2:** Digital Trunk Troubleshooting (Continued) (Sheet 3 of 10)

Symptom	Probable Cause	Corrective Action
T1 Trunk unstable or 3300 ICP resets or both.	Improper cable. Cat 5 Ethernet Cable is not approved to use as a standard RJ45/T1 cable.	Use shielded R45-R45 T1 cable for T1, ISDN line and/or DSU/DSU connections. Without proper shielded pairs, the signal integrity on a T1 trunk is not guaranteed. Refer to Mitel Knowledge Base article 08-5191-00123 for additional details.
T1 E&M trunk call cannot be transferred or put on hold.	Release Link Trunk (RLT) setting in the Trunk Attributes form is set to YES. This setting is only intended for T1 integration to centralized attendant. If the RLT field is set to YES for normal operation, it will cause these symptoms.	For normal T1 E&M trunks, set the RLT field in the Trunk Attributes form to NO.
Incoming T1 E&M trunk call limited to 10 digits. (Affects applications such as fax servers trying to dial numbers over 10 digits--e.g., long distance calls).	Trunk COS has "ANI/DNIS/ISDN Number Delivery Trunk" option enabled which limits the maximum number of incoming digits to 10. With option disabled, the trunk can receive more than 10 digits.	Set "ANI/DNIS/ISDN Number Delivery Trunk" option to "No" in the trunk COS.

**Table 6.2:** Digital Trunk Troubleshooting (Continued) (Sheet 4 of 10)

Symptom	Probable Cause	Corrective Action
External forwarding of an incoming PRI call is not successful.	The COS of the incoming PRI does not allow Public-to-Public trunk connection.	In the COS of the incoming PRI trunk, enable “Public Network to Public Network connection allowed”.
	There is a COR restriction against the incoming PRI trunk in the ARS route.	For COR restriction, ensure the COR number of the PRI trunk is not included in the COR group defined for the specified route in the ARS Routes form. See the document “Using CDE to Prevent Toll Fraud on the 3300 ICP” for more information. This document is available in the 3300 ICP System Administration Tool online help.
	Q.Sig Private network access is enabled in PRI link descriptor.	For the link descriptor assignment used by the PRI link, set “Q.Sig Private network access” to NO. (This option should not be enabled for normal PRI. It should only be set if the link is intended for Q.Sig.)
After you install or initially program an embedded E1 module, the DASS II link does not work.	In the Link Descriptor Assignment for the DASS II link, the CRC-4 is set to “Yes”.	In the Link Descriptor Assignment for the DASS link, set the CRC-4 setting to “No” and then reset the controller. If you alter the CRC-4 setting, you MUST reset the controller to enable the new, or changed, setting.
Cannot dial international numbers when connected to DMS500 switch running DMS100 protocol.	System is connected to a DMS500 switch running DMS100 NI1 protocol and the service provider has an NI2 table programmed in the central office. The protocol may set correctly in the central office; however the NI2 table should not be programmed.	Refer to Mitel Knowledge Base article 05-5107-00005.

**Table 6.2:** Digital Trunk Troubleshooting (Continued) (Sheet 5 of 10)

Symptom	Probable Cause	Corrective Action
DID call with number in the name portion fails to access Auto Attendant directly.	Inbound ISDN calls which present numbers in the name portion of the call will not complete. The voice mail which uses screen scrapes are seeing the numbers in the name portion of the caller as choice or extension number, instead of a trunk call. As a result, the DID caller does not hear the auto attendant greeting and may hear other voice mail option or "please enter your mailbox number prompt".	In the voice mail port's class of service, set the following: <ul style="list-style-type: none"> <li>display ani/isdn calling number only YES</li> <li>display ani/dnis/isdn calling/called number YES.</li> </ul>
Outgoing call on PRI E1 trunk (using Euro ISDN protocol) to a busy PSTN (number is dropped instead of receiving busy tone.	Link using Incorrect protocol variant.	<p><b>3300 ICP Release 4.0 - 5.1</b> Upgrade to Rel 5.1.4.8 and set EuroISDN Protocol Variant as explained below</p> <p><b>3300 ICP Release 5.1.4.8 and higher</b> Set Euro ISDN Protocol Variant as explained below</p> <p>For embedded T1/E1, set the Protocol Variant via ESM as follows:</p> <ol style="list-style-type: none"> <li>1. Log into the System Administration Tool</li> <li>2. From the Selection menu (alphabetical view), choose ISDN Protocol.</li> <li>3. Highlight the module required, and change to Telecom Italia under Protocol Variant for Euro ISDN.</li> </ol>
No ANI displayed when call is transferred over Q.SIG from Mitel system to foreign PBX.	ANI missing from the CTCOMPLETE facility message in the Q.SIG signaling.	Add "ctcomplete" to the Comment field in the ISDN Protocol Assignment form in ESM. (Omit the quotation marks.)

**Table 6.2:** Digital Trunk Troubleshooting (Continued) (Sheet 6 of 10)

Symptom	Probable Cause	Corrective Action
<b>Embedded PRI</b>		
Embedded PRI calls fail and all Status LEDs on the Dual T1/E1 Framer are OFF.	Configuration.	<p>Verify that embedded PRI is programmed properly in the following forms (see also Program Embedded PRI/Q.SIG in the Online Help):</p> <ul style="list-style-type: none"> <li>• Controller Module Configuration</li> <li>• Dual T1/E1 Framer Configuration</li> <li>• Link Descriptor Assignment</li> <li>• Digital Link Assignment</li> </ul> <p>After the Digital Links form is completed, the T1/E1 Framer status LEDs should come on. This takes about 15 seconds.</p>
Embedded PRI Links are “not seizable”, Status LEDs show RED alarm.	Configuration or wiring.	<p>Ensure that the ISDN cable is plugged into the correct RJ-45 port on the Dual T1/E1 MMC. Verify that the ISDN cable is correctly wired. Change the “Termination Mode” setting in the Digital Link Descriptors form - either LT or NT. This change takes about 30 seconds to take effect.</p>
Embedded PRI links are “not seizable”, Status LEDs show flashing GREEN.	Configuration.	<p>Verify the “Network Side/QSIG Master” setting in the ISDN Protocol form. Check the “Inverted D-Channel” setting in the Digital Link Descriptors form - normally it is set to “No”. Each of these changes takes approximately 30 seconds.</p>
Embedded DPNSS links are “not seizable”, Green LED is ON	Configuration.	<p>Ensure that the “Address for Message Control” field in the Digital Link Descriptors form is set appropriately (“A” or “B” depending on the far end).</p> <p>If the configuration is correct, wait for about one minute until every circuit has finished negotiation with the far end.</p>

**Table 6.2:** Digital Trunk Troubleshooting (Continued) (Sheet 7 of 10)

Symptom	Probable Cause	Corrective Action
Distorted voice or loud noise over PRI/QSIG call	Voice Encoding is not set properly.	In the Link Descriptor Assignment for the PRI/QSIG trunk, set the "Voice Encoding" to Nil for T1 on NA or E1 on Euro controller.
High number of slips.	Configuration of Network Synchronization form.	Ensure that the synchronization source being selected is to a digital PSTN trunk (like PRI or T1/D4).
Outgoing calls fail with reorder tone.	Configuration error in ARS programming or ISDN Protocol form.	Enter the CCS TRACE maintenance command to ensure that the proper digits are being sent out. Check the Digit Modification with the Per-Call programming for PRI to make sure digits are not being inserted or absorbed unnecessarily. Ensure that the "Protocol" field in the ISDN Protocol form is correct for the PSTN link (not for DPNSS).
Incoming calls fail.	Configuration error in Trunk forms.	Verify in the Trunk Attributes form that there is an Answer Point set up for non-DID trunks for Day and Night services. For dial-in trunks, verify that the "Dial in Trunks Incoming Digit Modification - Absorb" field is set to 0 and that the "Dial In Trunks - Incoming Digit Modification - Insert" field is set appropriately for dial in trunks.
Access denied when calling out on a PRI trunk.	Programming error.	PRI and MSDN trunks are considered to be DPNSS by the system. The Class of Service (COS) option "Public Network Access via DPNSS" of the dialing device must be set to Yes. (The default is No).
When dialing out on a PRI trunk the call is connected, however no audio path is established.	Programming error.	In Trunk Attributes form, ensure that Release Link Trunk is set to No.

**Table 6.2:** Digital Trunk Troubleshooting (Continued) (Sheet 8 of 10)

Symptom	Probable Cause	Corrective Action
Unable to forward an incoming PRI call to an external destination. External forwarding of an incoming PRI call may not be successful for one of the following reasons.	COS of the incoming PRI does not allow Public-to-Public trunk connection.	In the COS of the incoming PRI trunk, enable <b>Public Network to Public Network connection allowed</b> .
	COR restriction against the COR of the incoming PRI trunk in the ARS route.	For COR restriction, ensure the COR number of the PRI trunk is not included in the COR group defined for the specified route in the ARS Routes form. <b>NOTE:</b> You may need to refer to the Toll Fraud control document Knowledge Base Article # 04-1000-00060 "Using CDE to Prevent Toll Fraud on the MN3300 ICP".
	Q.Sig Private network access is enabled in PRI link descriptor.	For the link descriptor assignment used by the PRI link, set <b>Q.sig Private network access</b> to <b>NO</b> . (This option should not be enabled for normal PRI, only if this link is intended for Q.Sig.).
Calls on PRI trunks do not present outbound name.	Not supported by protocol used on the PRI trunks. Outbound name is only supported by PRI trunks that use DMS-100 or QSIG protocols.	Refer to Mitel Knowledge Base article HT4633 for a list of the protocols that support outbound name.
QSIG ISO feature not functioning.	QSIG feature not supported. For unsupported QSIG features, the 3300 will not act as a transit switch.	See Mitel Knowledge Base article 06-5191-00064_1 for a list of the QSIG features supported on the 3300 ICP
<b>Embedded BRI</b>		

**Table 6.2:** Digital Trunk Troubleshooting (Continued) (Sheet 9 of 10)

Symptom	Probable Cause	Corrective Action
Embedded BRI calls fail and all Status LEDs on the Quad BRI Framer are OFF.	Configuration.	<p>Verify embedded BRI is programmed properly in the following forms (see also Program Embedded BRI in the online Help):</p> <ul style="list-style-type: none"> <li>• Controller Module Configuration</li> <li>• Quad BRI Framer Configuration</li> <li>• Link Descriptor Assignment</li> <li>• Digital Link Assignment</li> <li>• Protocol Assignment</li> </ul> <p>After the Digital Links form is completed, the red Quad BRI Framer status LED should come on. This takes about 15 seconds.</p>
Embedded BRI Links are “not seizable”, Status LEDs show RED alarm.	Configuration or wiring.	<p>Ensure that the ISDN cable is plugged into the correct RJ-45 port on the Quad BRI MMC. Verify that the ISDN cable is correctly wired (straight through for trunk interface, crossover for terminal). Note that 3-4 and 5-6 are the relevant pins for the cable.</p> <p>Toggle the “Bus Type” setting in the Protocol Assignment (either S or T). This change takes about 30 seconds to take effect.</p> <p>Ensure that the Manual TEI value is correct (if required).</p>
High number of slips.	Configuration of Network Synchronization form.	<p>Ensure that the synchronization source being selected is not connected to a BRI terminal. If there is a digital E1 trunk, that should be used as the first synchronization choice.</p>
Outgoing calls fail with reorder tone.	Configuration of ARS or configuration of Per Call Capabilities.	<p>Enter the CCS TRACE maintenance command to ensure that the proper digits are being sent out.</p> <p>Check the Digit Modification with the Per-Call programming for BRI to make sure digits are not being inserted or absorbed unnecessarily.</p>



**Table 6.2:** Digital Trunk Troubleshooting (Continued) (Sheet 10 of 10)

Symptom	Probable Cause	Corrective Action
Incoming calls fail.	Configuration of Trunk forms.	Verify in the Trunk Attributes form that there is an Answer Point set up for non-DDI trunks for Day and Night services. For dial-in trunks, verify that the “Dial-in Trunks Incoming Digit Modification - Absorb” field is not left blank and that the “Dial In Trunks - Incoming Digit Modification - Insert” field is set appropriately for dial-in trunks.

## MSDN DPNSS Links

**Table 6.3:** MSDN/DPNSS Link Troubleshooting (Sheet 1 of 4)

Symptom	Probable Cause	Corrective Action
Embedded MSDN/DPNSS calls fail and all status LEDs on the T1/E1 MMC are OFF.	Faulty configuration.	Verify embedded MSDN/DPNSS is programmed properly in the following forms: <ul style="list-style-type: none"> <li>• Controller Module Configuration</li> <li>• Frammer Configuration → T1/E1 Frammer Configuration</li> <li>• Link Descriptor Assignment</li> <li>• Digital Link Assignment</li> </ul> After the Digital Links form is completed, the red T1/E1 MMC status LED should come on. This takes about 15 seconds.

**Table 6.3:** MSDN/DPNSS Link Troubleshooting (Continued) (Sheet 2 of 4)

Symptom	Probable Cause	Corrective Action
Embedded MSDN/DPNSS links are “not seizable” and the red LED is ON.	Faulty configuration or wiring.	Ensure that the T1/E1 cable is plugged into the correct RJ-45 port on the T1/E1 MMC. Verify that the T1/E1 cable is correctly wired. Note that 1&2 and 4&5 are the relevant pins for the cable. Toggle the “Termination Mode” setting in the Link Descriptor Assignment (either NT or LT). This change takes about 15 seconds to take effect.
Embedded MSDN/DPNSS links are “not seizable” and the green LED is ON.	Faulty configuration.	Ensure that the “Address for Message Control” field in the Digital Link Descriptors form is set appropriately (either “A” or “B” depending on the far end). If the configuration is correct, wait for about 1 minute until the every circuit has finished negotiating with the far end.
High number of slips.	Incorrect configuration of Network Synchronization form.	Ensure that the synchronization source being selected is to a digital PSTN trunk (like PRI or T1/D4).

**Table 6.3:** MSDN/DPNSS Link Troubleshooting (Continued) (Sheet 3 of 4)

Symptom	Probable Cause	Corrective Action
User is unable to make an MSDN link call.	Programming error in Trunk Attributes form.	Ensure that the Trunk Attributes form is programmed correctly <b>at both ends</b> of the link. Specifically, dial-in trunks must have an entry in the Absorb column. (Enter '0' if no digits are to be absorbed.) For example, if the Trunk Attributes form of the Local system is programmed correctly but the form in the Remote system is <b>not</b> programmed correctly, MSDN calls will succeed only from Remote to Local. Calls made from Local to Remote will fail.
Outgoing calls links fail with re-order tone.	Faulty configuration in ARS.	Ensure that the proper digits are being sent out – get a “ccs trace” from the maintenance command window in ESM. Also review the routing of the call throughout the PBX network. Verify that the far end is ready to properly accept the call.
Incoming calls fail.	Faulty configuration of trunk Forms.	Verify in the Trunk Attributes form that there is an Answer Point setup for non-DDI trunks for Day and Night services. For dial in trunks, the “Dial In Trunks Incoming Digit Modification – Absorb” is not left blank and that the “Dial In Trunks Incoming Digit Modification – Insert” is set appropriately for dial in trunks.

**Table 6.3: MSDN/DPNSS Link Troubleshooting (Continued) (Sheet 4 of 4)**

Symptom	Probable Cause	Corrective Action
All calls on a link fail.	Faulty cable connections, cable, or card.	Check the status of the link by using the DTSTAT READ PLID maintenance command. Check the cabling and cable connections. Test with a back-to-back cable to prove the card. Replace faulty cable or card.
Only some calls on a link fail.	Configuration errors in programming <ul style="list-style-type: none"> <li>• ARS programming error</li> <li>• Digit conflict</li> <li>• Interconnect Restriction preventing call</li> <li>• Far end fault/programming</li> </ul>	Correct programming through System Administration Tool.
Only calls to the central office fail.	Faulty programming.	Ensure the Class Of Service option of "Public Network Access via DPNSS" is enabled on the extension making the call and the for MSDN trunks.

**Direct IP Routing**  
**Direct IP Routing Troubleshooting**  
**Symptom Probable Cause Corrective Action**  
**Incoming calls fail**  
**Faulty configuration of trunk forms. Ensure that the**  
**Direct IP Route used to provision IP trunks between**  
**MiVoice Business system is configured correctly. Verify the**  
**IP Networking Programming using the Direct IP Route**  
**method. For more detail see System Administration Tool**  
**Online Help.**

XNET

**Table 6.4:** XNET Troubleshooting (Sheet 1 of 5)

Symptom	Probable Cause	Corrective Action
Caller reports reorder tone when calling to another system.	Errors in the XNET ARS programming.	<ul style="list-style-type: none"> <li>• Ensure that the ARS Leading Digit Assignment and ARS Digits Dialed Assignment forms translate the dialed digits to an XNET route. Either the digits do not resolve to a route, or the route does not have the XNET Trunk Group Number field programmed.</li> <li>• Ensure that the PBX Number field in the IP/XNET Trunk Groups form contains a system number which exists in the XNET network.</li> <li>• Ensure that the PBX Number field in the IP/XNET Trunk Groups form contains a PBX number that is correctly programmed on the Remote PBX: <ul style="list-style-type: none"> <li>– The incoming signaling DID number at the Remote PBX may not match the correct local outgoing list.</li> <li>– The incoming voice DID number at the Remote PBX may not match the correct local outgoing list.</li> <li>– Interconnect restrictions may be set up incorrectly in the IP/XNET Trunk Profiles form at the Remote PBX (the remote profile number may not agree with the correct local profile number, or may be the wrong setting for the profile).</li> </ul> </li> </ul>

**Table 6.4:** XNET Troubleshooting (Continued) (Sheet 2 of 5)

Symptom	Probable Cause	Corrective Action
		<ul style="list-style-type: none"> <li>• Ensure that the Direct IP Route used to provision IP trunks between MiVoice Business system is configured correctly.</li> <li>• Verify the IP Networking Programming using the Direct IP Route method. For more detail see <a href="#">System Administration Tool Online Help</a>.</li> <li>• Ensure that the PBX Number field in the IP/XNET Trunk Groups form contains a System number which is programmed correctly on the Local PBX:                         <ul style="list-style-type: none"> <li>– The outgoing signaling DID number at the Local PBX must match the correct remote incoming list.</li> <li>– The outgoing voice DID number at the Local PBX must match the correct remote incoming list.</li> <li>– Interconnect restrictions must be set up incorrectly in the IP/XNET Trunk Profiles form on the Local PBX (the profile number must agree with the correct remote profile number, and must have the correct profile setting).</li> </ul> </li> </ul>

**Table 6.4:** XNET Troubleshooting (Continued) (Sheet 3 of 5)

Symptom	Probable Cause	Corrective Action
Outgoing calls fail with reorder tone (outbound side).	Trunks Out-of-Service	Check trunk status
	Trunk congestion	<ul style="list-style-type: none"> <li>• Check that no trunks are Out-of-Service or MAN-BUSIED.</li> <li>• Ensure you have enough trunks allocated for the expected call rate.</li> <li>• Wait till more trunks become available.</li> </ul>
	Invalid Dialing	Verify that the dialled numbers are routeable.
	Class of Service (COS) settings	If accessing a PUBLIC trunk over XNET, ensure the Trunk COS of the 'Public Network Access via DPNSS' is enabled.
	Insufficient bandwidth to access the necessary resources	Check the bandwidth settings under Voice Network > Bandwidth Management
	The type of end-point being called - for locked IPDO or other "restricted" devices. Restricted devices are: <ul style="list-style-type: none"> <li>• Locked devices</li> <li>• Devices on a system when in License Violation</li> <li>• Phone Locked</li> </ul>	Can only dial an Emergency or an Attendant

**Table 6.4:** XNET Troubleshooting (Continued) (Sheet 4 of 5)

Symptom	Probable Cause	Corrective Action
Outgoing calls fail with reorder tone (inbound side).	Trunk Attributes Dial In vs Non-Dial In	Program Dial in Trunk destinations or Incoming Direct Inward Dial digits to Absorb/Insert
	Digit translation	Verify that the call has been routed to the correct destination.
	Dialing conflicts	Verify that the call has been routed to the correct destination.
	Call forwarding or rerouting when the Call Forward destination is Out of Service.	Disable the Forwarding
Caller reports busy tone when calling to another system.	Insufficient DID numbers allocated in the XNET ICP/PBX Networking form to set up voice channels to another PBX.	Allocate additional DID numbers.
	The Do Not Disturb (DND) function is turned on.	The Do Not Disturb (DND) functionality is enabled for the device or user you called.
	The call was forwarded to a busy line.	The call was routed or diverted to another busy destination by the system. Try again after sometime.
	The callee made the line busy.	When the person on the other end of the line rejects the incoming call.
	The called group has been marked as absent.	No one from the dialed group is available to attend the call.



**Table 6.4:** XNET Troubleshooting (Continued) (Sheet 5 of 5)

Symptom	Probable Cause	Corrective Action
Call does not have the correct service profile.	Incorrect Local Profile Number.	Correct in the IP/XNET Trunk Groups form on the Local PBX.
	Incorrect Remote Profile Number.	Correct in the IP/XNET Trunk Profiles form on the Local PBX.
	Incorrect Trunk Service Number or Interconnect Number.	Correct in the IP/XNET Trunk Profiles form on the Local or Remote PBX.
Signaling connection will not clear down or does not stay up.	Signaling Inactivity Timer fields are blank for the PBX pair in the ICP/PBX Networking form (blank at one or both of the systems).	Enter a value in the Signaling Inactivity Timer fields on both of the systems.
You cannot make XNET calls after a switch has been upgraded to a later version of software.	Max Number of VoTDM Calls field in the XNET ICP/PBX Networking form is not completed.	Complete the Max Number of VoTDM Calls field in the XNET ICP/PBX Networking form.
One ore more of the following network features is not available: <ul style="list-style-type: none"> <li>• IP Networking</li> <li>• XNET</li> <li>• Voice mail Networking</li> </ul>	System Type is "Standalone".	Program the System Type as "Enterprise" in the AMC.

## IP Trunking (IP Networking)

**Table 6.5:** IP Trunk Troubleshooting

Symptom	Possible Cause	Corrective Action
IP trunk does not recover after router crash.	ICMP redirect is enabled.	<ol style="list-style-type: none"> <li>On the Linux shell, enter the following command to find the redirected route entry:  <pre>root@mxei111:~# route -n</pre> Kernel IP routing table is displayed.</li> <li>If you want to delete route Destination <i>&lt;IP address&gt;</i>, enter the following table:  <pre>root@mxei111:~# route del -net &lt;Destination IP address&gt; netmask &lt;Genmask IP address&gt; gw &lt;Gateway IP address&gt;</pre></li> <li>For a permanent solution: <ul style="list-style-type: none"> <li>Make sure that the route has a “permanent” static route to the remote IP trunk network.</li> <li>Turn IP redirect off.</li> <li>Turn on the routing protocol between local router and ISP router.</li> </ul> </li> </ol>
Unable to place calls between systems via IP trunks in a clustered, redirected, or resilient environment.	ARS Routes or PBX Number in the ICP/PBX Assignment forms of the systems are programmed incorrectly.	For each system in the cluster, ensure that the system’s PBX Number matches its CEID Index Number as defined in the Cluster Elements form.
Receive “out of service” tone while dialing across IP trunks to a remote element.	<p>Congested trunks at remote node.</p> <p><b>NOTE:</b> This is not a local trunk congestion issue, the congestion is at the remote site. The remote site will have less trunks programmed than the originating site.</p>	<ol style="list-style-type: none"> <li>Launch the System Administration tool on the remote element.</li> <li>Access the XNET ICP/PBX Networking form.</li> <li>Increase Max Number of VOIP calls.</li> </ol>

## SIP Trunking

**Table 6.6:** SIP Trunk Troubleshooting

Symptom	Possible Cause	Corrective Action
When making a call in or out on SIP trunks the trunk number in the SMDR record is blank.	SMDR for SIP Trunks use the SMDR Tag field from the SIP Peer Profile form for the trunk number. If this field is blank, the trunk number in the SMDR record is blank.	Enter a Trunk Number (for example, 99) in this field and the number will be displayed as the trunk number in the SMDR record (for example, T099).

# Tools and Embedded Applications

## System Management Tools

**Table 7.1:** System Administration Tool Troubleshooting (Sheet 1 of 10)

Symptom	Probable Cause	Corrective Action
<b>System Administration Tool</b>		
Unable to log into System Administration Tool, Group Administration Tool, Desktop Tools, or Visual Voice Mail phone application.	Database restore in progress	Wait for Database Restore operation to complete. Perform restores outside of business hours to minimize impact to users.
	Cookies are disabled in Firefox. All management tools depend on being allowed to set cookies to maintain session ID state, login fails if cookies are not enabled.	If the management tool fails to launch: <b>Firefox</b> <ol style="list-style-type: none"> <li>1. Click on the Firefox button and then select <b>Options</b>.</li> <li>2. Select the <b>Privacy</b> panel.</li> <li>3. Set <b>Firefox will:</b> to Use custom settings for history.</li> <li>4. Make sure <b>Accept cookies from sites</b> is selected.</li> <li>5. Click <b>Exceptions.....</b></li> <li>6. Make sure the MiVoice Business system you're trying to access isn't listed.</li> <li>7. If it is listed, click on its entry, then click <b>Remove Site</b>.</li> </ol>

**Table 7.1:** System Administration Tool Troubleshooting (Continued) (Sheet 2 of 10)

Symptom	Probable Cause	Corrective Action
		<p><b>Chrome</b></p> <ol style="list-style-type: none"> <li>1. Open Chrome.</li> <li>2. From the <b>More Options</b> menu, click <b>Settings</b>.</li> <li>3. Scroll down and click <b>Advanced</b>.</li> <li>4. Under <b>Privacy and Security</b>, click <b>Content Settings</b>, and then click <b>Cookies</b>.</li> <li>5. Click the toggle switch next to <b>Blocked</b>. The <b>Blocked</b> option changes to <b>Allow sites to save and read cookie data (recommended)</b>.</li> </ol> <p><b>Edge</b></p> <ol style="list-style-type: none"> <li>1. Open Edge.</li> <li>2. Click <b>More Options ( ... )</b>, and then click <b>Settings</b>.</li> <li>3. Scroll down and click <b>View Advanced Settings</b>.</li> <li>4. Scroll down to <b>Cookies</b> and select <b>Don't block cookies</b> from the drop-down list.</li> </ol>
Unable to log into System Administration Tool, Group Administration Tool, Desktop Tools, or Visual Voice Mail phone application.	5550 IP Console is running on Windows 98 operating system on the PC.	Close the 5550 IP Console application. The 5550 IP Console must be run as a standalone application on Windows 98 (that is, with no other application open while it is running).

**Table 7.1:** System Administration Tool Troubleshooting (Continued) (Sheet 3 of 10)

Symptom	Probable Cause	Corrective Action
<p>The System Administration Tool displays a license violation message in one or more of the following formats:</p> <ul style="list-style-type: none"> <li>• Status banner in the top left corner of the System Administration Tool.</li> <li>• Pop-up during log in and log out.</li> <li>• Pop-up when forms are opened.</li> <li>• Pop-up when you are about to over-allocate licenses.</li> </ul>	<p>The controller is in license violation mode.</p>	<p>Correct the license violation event. Examples include:</p> <ul style="list-style-type: none"> <li>• License over allocation</li> <li>• Missing Designated License Manager</li> <li>• Missing Application Group Member</li> <li>• Core Package capability exceeded</li> <li>• License Keys cannot be validated</li> <li>• System ID mismatch</li> <li>• SDS is off (Enterprise System Type)</li> <li>• Duplicate System</li> <li>• Multiple Designated License Managers</li> <li>• Failure of timely synchronization with AMC</li> <li>• Application Group is in license violation mode</li> <li>• “licensekeys” or “licensecert” file has been corrupted</li> </ul>
<p>System Administration Tool unable to connect through Mozilla Firefox to MiVoice Business for ISS following reboot. Receive the following error:</p> <p>“Secure Connection Failed”</p> <p>Your certificate contains the same serial number as another certificate issued by the certificate authority. Please get a new certificate containing a unique serial number. (Error code: sec_error_reused_issuer_and_serial)</p>	<p>Browser cache conflict.</p>	<p>Clear Firefox cache:</p> <ol style="list-style-type: none"> <li>1. Select <b>Options &gt; Options</b>.</li> <li>2. Click <b>clear your recent history</b>.</li> <li>3. Under <b>Details</b> , ensure <b>Cache</b> is selected, and then click <b>Clear Now</b> .</li> <li>4. Restart Firefox and attempt to reconnect to the MiVoice Business for ISS.</li> </ol> <p>If problem persists, switch to Chrome.</p>

**Table 7.1:** System Administration Tool Troubleshooting (Continued) (Sheet 4 of 10)

Symptom	Probable Cause	Corrective Action
The Group Administration Tool displays a license violation message when you log in or out.	The controller is in license violation mode.	Correct the license violation event.
“Script Error” Error Message, or a Dialog Fails to Appear	If the computer that you are using to access a MiVoice Business tool has pop-up blocker software installed, the administration tools (System Administration, Group Administration, or Desktop Tool) may not operate properly.	To access the administration tool or perform the administrative activity that the pop-up blocker software is preventing, you must allow pop-ups from the 3300 ICP to your PC.
Form fails to load. May be accompanied by “Document is Empty” error.	Browser cache conflict.	Clear the browser cache: In <b>Firefox</b> : press CTRL+SHIFT+DEL, select Everything for “Time range to clear” and Cache, then click OK. In Chrome: press CTRL+SHIFT+DEL, select the beginning of time next to <b>Clear the following items from</b> and <b>Cached images and files</b> , then click <b>Clear Browsing Data</b> . In <b>Edge</b> : press CTRL+SHIFT+DEL, select <b>Cached data and files</b> , and then click <b>Clear</b> .
Data Add/Change pop-up window fails to refresh in Firefox. After selecting URL in the window’s Navigation Bar and pressing ENTER, a message sometimes appears saying “Please wait while the form is loading”. Data may reload but pressing Cancel fails to dismiss pop-up (Cancel, Save, and Preview buttons also disabled).	Indeterminate.	Click <b>X</b> button in pop-up window to close. NOTE: You can prevent re-occurrence by disabling the Navigation Bar via the Options menu in Firefox.

**Table 7.1:** System Administration Tool Troubleshooting (Continued) (Sheet 5 of 10)

Symptom	Probable Cause	Corrective Action
When you connect to the MiVoice Business tools for the first time from a client PC, you receive a warning that the site is not certified—for example: “This Connection is Untrusted” (Firefox - Error code: sec_error_untrusted_issuer)	<p>You need to install the trusted Mitel Root CA certificate on the client PC. If the web server is accessed by a URL not matching a DNS or local host filename in the certificate, your browser displays a warning that the name in the certificate does not match the name of the site.</p> <p>If the certificate is not installed, a security window is displayed. Firefox users must click <b>“I understand the risks”</b> followed by <b>Add Exceptions</b>, disable <b>Permanently store this exception</b>, and click <b>Confirm Security Exception</b>, and then install the Mitel Root CA certificate as described in the next column.</p>	<p>The MiVoice Business System Tools login page contains a link to a help topic that provides instructions on how to download and install the Mitel Root Certificate.</p> <p><b>Firefox</b> If you have already downloaded the Mitel Root Certificate, skip to step 6.</p>



**Table 7.1:** System Administration Tool Troubleshooting (Continued) (Sheet 6 of 10)

Symptom	Probable Cause	Corrective Action
		<ol style="list-style-type: none"> <li>1. Launch Firefox.</li> <li>2. Start an ESM session.</li> <li>3. Click <b>I Understand the Risks</b> followed by <b>Add Exception...</b> .</li> <li>4. Clear the <b>Permanently store this exception</b> check box, and then click <b>Confirm Security Exception</b> .</li> <li>5. ESM Login page will now display. Download the Mitel Root Certificate and install it by following the remaining steps.</li> <li>6. Click the Firefox button at the top of the Firefox window and select <b>Options &gt; Options</b> (or select it from the Tools menu if the Menu Bar is showing).</li> <li>7. Click <b>Advanced&gt; Encryption &gt; View Certificates</b>.</li> <li>8. Make sure the focus is on the <b>Authorities</b> tab, and then click <b>Import</b> .</li> <li>9. Navigate to the mitelcert.cer file you saved and click <b>Open</b> .</li> <li>10. In the resulting dialog box, select <b>Trust this CA to identify websites</b> and <b>Trust this CA to identify software developers</b> .</li> <li>11. Click <b>OK &gt; OK</b> .</li> <li>12. Exit FireFox, and then restart it. You can now log in to ESM.</li> </ol>
Attempts to log in to the MiVoice Business tools using FireFox results in "Secure Connection Failed" (Error code: sec_error_reused_issuer_and_serial).	Firefox missing the Mitel Root CA certificate. Also failed to clear the <b>Permanently store this exception</b> check box in the Firefox Certificate Manager on first log in attempt.	<ol style="list-style-type: none"> <li>1. In Firefox, remove the IP address of the MiVoice Business system from the Servers tab in the Certificate Manager.</li> <li>2. Install the Mitel Root CA certificate (see previous Symptom for instructions).</li> </ol>

**Table 7.1:** System Administration Tool Troubleshooting (Continued) (Sheet 7 of 10)

Symptom	Probable Cause	Corrective Action
After upgrading to MiVoice Business Release Release 7.1, attempts to log in the System Administration tool using FireFox 33+ results in "This connection is untrusted."	Firefox is blocking the Mitel Root CA certificate.	Restart Firefox.
System Administration Tool Online help is not available. When you click on the help buttons in the System Administration Tool, the help window displays "404 Page Not Found" error.	Web server that hosts the Online help files is down.	Ensure web server is running.
Online help not appearing in System Administration Tool	Help not installed on external server or the path to the help is incorrect	Correct the path or install the help on the external server. See the System Administration Tool online help for instructions.
Non-Unique Match error when entering commands via the System Administration tool.	The busy command was entered and has not been completed. The system is waiting for further input (for example, FORCE) before executing the command.	Issue the FORCE command.

**Table 7.1:** System Administration Tool Troubleshooting (Continued) (Sheet 8 of 10)

Symptom	Probable Cause	Corrective Action
System Administration Tool Online help is not available. When you click on the help buttons in the System Administration Tool, the help window displays “404 Page Not Found” error.	Online help files are not installed either locally on the 3300 ICP system or remotely on a web server.	<p>Install online help locally on your PC or remotely on a web server</p> <p><b>Locally:</b></p> <ol style="list-style-type: none"> <li>1. Copy the /Documentation/Help.zip file from the 3300 ICP software CD-ROM to the hard drive on your PC.</li> <li>2. Using WinZip, extract the files to a folder on your PC.</li> <li>3. Open the “sysadmin” folder and locate the “sysadmin.html” file.</li> <li>4. Create a shortcut on your Desktop to the “sysadmin.html” file.</li> <li>5. Double-click the “sysadmin.html” shortcut to launch the help.</li> <li>6. Navigate to the required help topic by using the Table of Contents, Index, or Search field.</li> </ol> <p><b>Remotely:</b></p>
		<ol style="list-style-type: none"> <li>1. Copy the /Documentation/Help.zip file from the 3300 ICP software CD-ROM to the web server.</li> <li>2. Using WinZip, extract the files to a folder on the web server.</li> <li>3. In the Remote Help Server field of the System Options form, enter the enter the URL to the location of the help files using the following syntax: http://&lt;IP Address of Remote Server&gt;/help/</li> </ol> <p>For example: http://10.117.7.39/help/ where 10.117.1.39 is the IP Address of the remote help server.</p> <ol style="list-style-type: none"> <li>4. Click <b>Save</b>.</li> </ol>
	URL to the remote help files is entered incorrectly	Enter the correct URL to the help files on the web server. You enter the URL to the help in the Remote Help Server field of the System Options form.

**Table 7.1:** System Administration Tool Troubleshooting (Continued) (Sheet 9 of 10)

Symptom	Probable Cause	Corrective Action
The Export button in a System Administration tool form fails to launch the Microsoft Excel spreadsheet,	Pop-up blocker is enabled, preventing Excel Spreadsheet from opening.	<p>Disable the pop-up blocker in your browser.</p> <ol style="list-style-type: none"> <li>1. In Windows Explorer, click <b>Tools &gt; Folder Options</b>.</li> <li>2. Click the <b>File Types</b> tab.</li> <li>3. In the <b>Registered File Types</b> list, select the <b>XLS Microsoft Excel Worksheet</b> type.</li> <li>4. Click the <b>Advanced</b> button.</li> <li>5. Clear the <b>Browse</b> in same window box.</li> <li>6. Check the <b>Confirm open after download</b> box.</li> <li>7. Click <b>OK</b>, and then click Close.</li> </ol>
Data errors occur when you use the Import Spreadsheet to import data into the System Administration Tool.	CSV files generated by the Import Spreadsheet and subsequently modified using Microsoft Excel may cause errors after you import them into the 3300 ICP.	Use Windows Notepad or other text editor to edit the file or edit the original worksheet in the Import Spreadsheet and regenerate the Comma Separated Values. A type of database file that separates data fields with a comma .csv file.
Unable to complete a Form Print and or complete a Logs Capture from the System Diagnostics Reporting form of the System Administration Tool	System Name is unknown. Check the top left corner of the System Administration Tool main window to verify that the system name is programmed properly.	If the System Name is unknown, enter a System Name in the Network Elements form.
<b>Desktop User Tool</b>		
The Desktop Tool displays a license violation message when you log in or out.	The controller is in license violation mode.	Correct the license violation event.
The Desktop Tool is disabled.	An over-allocation license violation event has been left uncorrected.	Correct the license violation event. In this case, you must reduce or eliminate the number of over-allocated licenses.
Audio File Download (for Music on Hold and Greetings)		

**Table 7.1:** System Administration Tool Troubleshooting (Continued) (Sheet 10 of 10)

Symptom	Probable Cause	Corrective Action
Audio File cannot be located	Corrupted file	Verify that the audio file is not corrupted.
Audio File is rejected	Incorrect audio file specifications	Verify that the audio file meets the required specifications (see System Audio File Update form in the System Administration Tool).
System Greeting is in the wrong language	Incorrect language file downloaded	Download a file in the correct language using the System Audio File Update form or MiVoice Enterprise Manager.
System error log is generated	Downloading file when system is unavailable	Verify that you are not downloading a file during a backup, restore or upgrade, or while someone is recording the same greeting from a telephone.
Unable to complete a Form Print and or complete a Logs Capture from the System Diagnostics Reporting form .	System Name is unknown. If the System Name is programmed properly, it appears in the left corner of the System Administration Tool window.	Enter the System Name properly in the Network Elements form.
<b>ISDN Maintenance &amp; Administration Tool (IMAT)</b>		
Receive a “missing DLL file” error while loading IMAT software on PC running Windows 98.	Missing required DLL file.	Obtain and install required DLL file. Refer to Mitel Knowledge Base article 05-3849-01044. The required DLL file is attached to this article.
When you use IMAT to retrieve the database from the Universal NSU, the database files do not appear to have been downloaded	NSU is running as ISDN node.	Refer to Mitel Knowledge Base article 06-5104-00038.

## Automatic Call Distribution

**Table 7.2:** ACD Troubleshooting

Symptom	Probable Cause	Corrective Action
Calls stay in Queue and are <b>not rerouted to path unavailable point</b> .	Programming error.	Refer to Mitel Knowledge Base article 06-5163-00009.
ACD RAD ports don't play for incoming calls on SIP Trunks	Programming error.	In the SIP peer profile, make sure that "Suppress Use of SDP Inactive Media Streams" is set to NO. Refer to Mitel Knowledge Base article 07-5157-00018 for more information.
The "Generic Group Alert" key does not work.	The Generic Group Alert function is intended to display single queue status when an agent logs in. If the agent belongs to multiple groups, the function does not know which group to display and will not work.	To display the queue status for each group that includes that particular agent, program a "Specific Group Alert" key for each group.

## Hot Desking

**Table 7.3:** Hot Desk Troubleshooting (Sheet 1 of 2)

Symptom	Probable Cause	Corrective Action
When a hot desk user attempts to log in, the following error message appears on the display of the IP phone: "Error: feature failure". Both the hot desk enabled set and the hot desk user are local on the 3300 ICP.	The PBX Number and the Cluster Element ID that are programmed for the 3300 ICP do not match.	Ensure that the PBX Number in the ICP/PBX Networking form matches the Cluster Element ID in the Cluster Elements form.

**Table 7.3:** Hot Desk Troubleshooting (Continued) (Sheet 2 of 2)

Symptom	Probable Cause	Corrective Action
“Phantom” ringing occurs when an ACD Hot Desk Agent is logged into an ACD.	The user profile for a hot desk agent supports up to 47 programmable keys. If an agent is assigned 47 feature keys and then logs into an ACD hot desk set that has fewer than 47 programmable keys on it, the extra keys are not accessible. If one of these “inaccessible” keys is programmed as a line appearance, calls for the line appearance will still ring at the phone.	To avoid this problem, choose one device type that supports 13 programmable keys, program a consistent layout for the buttons, and provide printed button templates for each ACD hot desk set.
Unable to log in to a 5560 IPT. Set display shows “Login failed due to an invalid dn”.	DNs for both the HDU and the 5560 IPT are on different ICPs/MiVoice Business systems. If the 5560 IPT is resilient, the 5560 IPT and the hot desk user DN must have the same primary and secondary.	Re-assign DNs so that the 5560 and HUD are on the same system(s).
Device behaving incorrectly after logging in with a 5560 IPT user profile. Display continues to show previous hot desk login and keys. Attempts to log in again results in “Login failed due to a system error”	The device is NOT a 5560 IPT. Users of a 5560 IPT can only hot desk into another 5560 IPT.	Reboot the device to restore in to normal operation.

## Emergency Call E911 Support

**Table 7.4:** Emergency Call Support Troubleshooting

Symptom	Probable Cause	Corrective Action
Emergency calls do not trigger E911 local notification. Calls placed on a designated “emergency” route do not trigger local notification.	E911 local notification will not be activated <i>if an emergency hunt group is not fully programmed and a call is placed on a designated “emergency” route.</i>	Refer to Mitel Knowledge Base article 04-1000-00020 for programming instructions.
Emergency call does not trigger E911 local notification	Enhanced 911 (E911) operation not fully supported for the device. There are some exception cases whereby emergency calls do not trigger E911 local notification.	<p>None. Currently, the following devices do not fully support Enhanced 911 (E911) operation:</p> <ul style="list-style-type: none"> <li>• Hot Desk users</li> <li>• IP consoles</li> <li>• Teleworker Solution users</li> <li>• Your Assistant and Your Assistant Softphone users</li> <li>• Any other mobile IP phones or phones that are carried from location to location</li> </ul> <p>Refer to the Engineering Guidelines for details.</p>

### Troubleshooting MiVB Next Generation 911 (NG911) with Red Sky

This section outlines the possible issues with MiVB Next Generation 911 services and the steps to troubleshoot NG911 issues with Red Sky.

Types of issues that can occur:

1. MiCollab can call 933 and location is not sent-->933 may not be configured on MiCollab user configuration-Location service. Also, MiCollab client emergency location must be configured and Mitel Network helper has to be running.
2. MiCollab cannot dial 933-->Redsky api may not be configured correctly. Hence, test connection from MiCollab.
3. Teleworker client cannot send the location-->MyE911 must check for location configuration and COS must check for Device move detection enable.



## Dailing 911 Does Not Work

If 911 services does not work, follow these steps in the System Administrator tool to troubleshoot the issue:

1. Review ARS and COR configurations.
2. Make sure you have an ARS route for emergency calls matching the 911 or 9911 digits (933/9933 for testing).
3. Confirm that the emergency route is using the SIP trunk with the NG911 provider and not the trunks previously used for emergency calls.
4. Validate that the SIP trunk is in service (you can use the maintenance command SIP LINK STATE ALL).
  - a. If the SIP trunk not in service, review the Network Element form Configuration:
    - i. Confirm the transport protocol used (TCP, UDP, and TLS).
    - ii. If MBG is used as a proxy, make sure MBG is able to connect to the SIP NG911 provider, if required start a packet capture on MBG to review.
    - iii. Validate the correct IP addresses have been whitelisted (For example, MBG WAN, if it is used as the SBC).
5. Start a packet capture using SIP TCPDUMP ALL and review the trace to confirm the following:
  - a. The INVITE is sent from MIVB to the NG911 provider.
  - b. The request is processed accordingly (responses 18x, 200 OK expected).
  - c. If the call is rejected by the NG911 provider, check the SIP Peer's custom headers to specify the E911-Organization-ID/<customer ID>.

## PSAP Does Not Receive Accurate Information

Follow these steps to verify, review, and confirm the configuration in the System Administrator tool when the 911 call works, but the Public Safety Answering Points (PSAP) does not receive accurate location information:

1. Verify the information configured in the NG911 provider's portal (this the customer's/VAR responsibility) such as:
  - ERLS - Emergency Routing Locations
  - Location's name, house, street, city, county, state/province, postal code and so on.
  - Subscribers
  - Valid 10-digit DID for callbacks
  - Any other relevant information that needs to be sent to the PSAP (this information is not stored in the MIVB)
2. Review the NG911 provider's portal, which can display a history of calls from which you can select a specific call, and see further details.
  - RedSky - Monitoring -> Call History
    - You can view a summary of the location information, and by clicking the "sip handset" icon, bring up the SIP Header information. From there you can determine if MIVB sent the right information (based on the device that is calling), and/or the location information that Redsky looked up.
3. Confirm that the MiVB is configured properly to send the relevant information to the NG911 provider:

- DID and CPN Substitution - configure per device or location that has the ability to make Emergency Calls.
- SIP Peer Profile - configure a SIP Peer Profile dedicated to signaling with the NG911 provider.
- SIP Devices Capabilities - configure SIP devices to provide location information.
- Class of Service - configure a COS for devices that will use the MyE911 Application from the NG911 provider.

## Gathering Information

If both the NG911 provider's portal information and the MiVB appear to be configured correctly, gather the following information:

- Validate with the NG911 provider which number(s) they are expecting in the following SIP headers:
  - PANI Header (information regarding the BSSID - provided by the WiFi Base Stations)
  - FROM Header (CESID Information)
  - PAI - P-Asserted-Identity (CESID Information)
  - If the device originating the call has the capability to provide geolocation according to RFC 6442, then the Geolocation header also applies.
  - If the integration with the NG911 requires so, verify that you have the correct values configured in the SIP Peer profile:
    - User-Defined Header Name = E911-Organization-ID
    - User-Defined Header Value = Provided by the NG911 provider
- Confirm which header is used by the NG911 provider to extract the CESID info (FROM or PAI).

## Next Steps

After you have gathered the information mentioned in the preceding section, proceed with the following action plan:

1. Start a packet capture in the MiVB by using the Maintenance Command SIP TCPDUMP ALL.
2. Make a test call (you can dial 911 or 933 for testing purposes).
3. Stop the packet capture in the MiVB by using the Maintenance Command SIP TCPDUMP OFF.
4. Retrieve the WS\_\*.pcap file from the MiVB using sftp; the file is located under the `/vmail directory`.
5. Open the trace in wireshark.
6. Using the VoIP Calls option, locate the 911 or 933 call.
7. Click the first **INVITE** from MiVB.
8. Identify the headers/numbers listed in the preceding section.
9. Compare notes with the NG911 provider.

At this point, you have two possible options:

- MiVB is sending the correct information:
  - Review the NG911 provider and correct the customer's info in the portal.
- MiVB is NOT sending the right information:
  - Review CESID configuration and refer to the *MiVoice Business RAY BAUM'S Act Solution Deployment Guide* for more information

Ensure that there are sufficient SIP trunk licenses are available. Refer to the *MiVoice Business Red Sky Deployment Guide* for more information.

## Embedded Voice Mail

**Table 7.5:** Embedded Voice Mail (Sheet 1 of 8)

Symptom	Probable Cause	Corrective Action
After upgrading from 8.0, the embedded voice mail fails to start. Monitoring the journalctl logs you will see the following: Starting iPVM Version 9.2.1.4 *** Fatal error starting the voice driver. iPVM stopped. Voice Mail Did not start Successfully	Obsolete DSP (Quad DSP 21061) installed.	Replace with a Quad 21161 or DSP II depending on the platform and function they are being used for.
Notification calls are configured for a mailbox but don't seem to work.	Notification is not enabled at the system level.	Enable notification in VM Options form.
	CO line access is restricted for voice mail port extension numbers.	Ensure that voice mail port numbers are not restricted from access to CO lines.
Notification calls use the correct outside lines but the pager never beeps.	Notification phone number or pager type programmed incorrectly.	Check the notification phone number and pager type.
The date and time that a message was left is incorrect.	3300 ICP system clock is wrong.	Adjust 3300 system date and time using <b>Server Manager Configuration -&gt; Date and Time</b> form.
The system is warning that the disk space is almost full.	Too many voice mail messages stored in mailboxes.	Delete unused mailboxes and have subscribers clean out unnecessary saved messages.
Too much silence before or after a greeting or mailbox name.	Hesitating before starting to record. Waiting too long before ending recording.	When recording greetings and names, start speaking immediately after the tone and press any key as soon as you are finished.

**Table 7.5:** Embedded Voice Mail (Continued) (Sheet 2 of 8)

Symptom	Probable Cause	Corrective Action
When outside callers reach the auto attendant and press 0, either no phones ring or the incorrect phone rings.	Mailbox 0 is not associated with operator's extension.	Check that mailbox 0 is correctly associated with the operator's extension.
When outside callers reach the auto attendant press 0, the operator's telephone rings and never forwards to voice mail.	Call Forwarding not set correctly on the Operator's phone.	Set Call Forward-Busy/No Answer on the Operator's phone to forward to voice mail.
Internal/external callers occasionally reach the Operator when calling the auto attendant.	The operator extension/voice mail ports are all busy.	Try again later.
Message Waiting indication is slow to appear	Not enough voice mail ports.	Ensure that voice mail ports count defined in VM Port Capacity form is programmed in the VM Ports form.
MWI light is flashing in the morning but no new messages waiting (i.e., phantom MWI).	Either Message Waiting - Deactivate field in Feature Access Code form is not set.OrPorts are not available .	Program Message Waiting - Deactivate field in Feature Access Code form.
If bilingual option is enabled in the VM Prompt Languages form then greeting is played once.	The second language is set to the same as the first language.	Set different language in the Default Language and Set Alternate Language To field.
The voice mail system is not responding after all 20 ports are programmed.	Voice mail application is not initialized on ports.	Restart the 3300 ICP system using the Reset System maintenance command to initialize the voice mail application on all ports.
The voice mail system resets itself at times.	In the event of a critical error, the voice mail system resets.	Contact Mitel Technical Support.
A minor alarm is raised after adding voice mail ports.	Not enough DSP resources available in the system.	Add more DSP resources. To calculate the amount of DSP resources that will be required for your system, please see the 3300 Engineering Guidelines.

**Table 7.5:** Embedded Voice Mail (Continued) (Sheet 3 of 8)

Symptom	Probable Cause	Corrective Action
Callers are greeted by a FAX tone instead of the company greeting.	Programming error.	See “System Greetings” and/or “RAD Greetings” in the System Administration Tool online help for programming instructions.
Cannot modify voice mailbox settings from the Group Administration Tool.	Voice mailbox length and directory number length are different.	If the voice mailbox length and directory number length are different, you can only edit voice mailboxes from the System Administration Tool or the system Administrator Mailbox.
Callers are transferred to Auto Attendant when pressing a Personal Contact key.	An invalid phone number was programmed.	Reprogram the Personal Contact.
When an external trunk is speed-dialed to the embedded Auto Attendant, the incoming caller receives the wrong greeting of “Please Enter a Mail Box number”. The Auto Attendant greeting should be heard instead.	Improper options are enabled in the Auto Attendant’s Class of Service.	Set the following COS options to either both “Yes” or both “No”. <ul style="list-style-type: none"> <li>• “Display ANI/DNIS/ISDN Calling/Called Number”</li> <li>• “Display ANI/ISDN Calling Number Only”</li> </ul>
Users suddenly cannot access Visual Voice Mail.	Range programming in progress.	While an administrator is using range programming in the System Administration Tool to modify the system database, users will be unable to access Visual Voice Mail. Perform range programming outside of regular business hours. Also if Audit/ Backup/ Restore in progress. User can not login into VVM.

**Table 7.5:** Embedded Voice Mail (Continued) (Sheet 4 of 8)

Symptom	Probable Cause	Corrective Action
Unable to add or edit mailboxes. Attempts result in an error message, "A Voice Mail Server Name for a local mailbox must match System Name."	Voice mail server host name doesn't match 3300 ICP system name.	The host name of the voice mail server in the VM Network Servers form must match the entry in the Name field in the Network Elements form. To correct the problem, change the Name field in the Network Elements form to match the voice mail server name.
Embedded Voice Mail cannot transfer or page externally (fails or rings only once).	Supervised Transfer is enabled, and the Transfer Ringback Timeout is set to default 17 sec.	In the VM Options form, disable the "Enable Supervised Transfer". However, the default Transfer Ringback timeout is 17 sec now.
Embedded RAD does not answer.	If a incoming call is blind-transferred to an Embedded RAD, the embedded RAD will experience "ring no answer" and/or "Do Not Disturb" conditions.	<ol style="list-style-type: none"> <li>1. Ensure that the embedded RAD port is in a RAD Hunt group.</li> <li>2. Program the phase timer of RAD hunt group to be 1 second or higher.</li> <li>3. Ensure that all calls are transferred to the RAD Hunt group. Call should not be made directly to the RAD port.</li> <li>4. 4. Ensure RAD is configured properly in "Class of Service Options" form. Check ESM help to ensure RAD Hunt group is programmed successfully.</li> </ol> <p>Also check ESM help to configure RAD Hunt Group.</p>
When voice mail is forwarded to e-mail, the e-mail indicates an incorrect sent time.	The wrong time being shown in e-mails forwarded from voice mail usually indicates that the Time Zone is not set correctly. The default value is GMT - 4:00.	In the VM Network Servers form of the System Administration Tool, change the Time Zone field to match your time zone.

**Table 7.5:** Embedded Voice Mail (Continued) (Sheet 5 of 8)

Symptom	Probable Cause	Corrective Action
Voice mail integration fails between an SX-2000 and a 3300 ICP that is acting as a voice mail server.	<p>Integration fails if all of the following conditions are present:</p> <ul style="list-style-type: none"> <li>• Systems are connected through a MSDN link</li> <li>• COS for the voice mail MSDN link has <b>COV/ONS/E&amp;M voice mail port</b> option enabled.</li> <li>• Diversion is turned off on both systems.</li> </ul>	<ul style="list-style-type: none"> <li>• Disable the <b>COV/ONS/E&amp;M Voice Mail Port</b> option, or</li> <li>• Enable Diversion on both the 3300 ICP and the SX-2000.</li> </ul>
Users cannot program Forward to E-Mail using the Desktop Tool.	Programming incomplete.	<ol style="list-style-type: none"> <li>1. Verify that Forward to E-mail is enabled for that user (see Forward to E-mail feature description in the System Administration Tool online help).</li> <li>2. Ensure feature is programmed on the user's set. If you have a centralized Networked Voice Mail voice mail server configuration, users can only program Forward to E-mail using the telephone interface.</li> </ol>

**Table 7.5:** Embedded Voice Mail (Continued) (Sheet 6 of 8)

Symptom	Probable Cause	Corrective Action
User needs to recover a voice mail message that he or she has forwarded; however, "Delete After Forwarding" is enabled.	If "Delete After Forwarding" is enabled, voice mail messages are deleted from the user's mailbox as soon as the message is forwarded.	All sent messages are available for a limited time in the /vmail/vpim/sent folder (see Networked Voice Mail Detailed Description). Administrators can recover them from this folder using FTP, and then e-mail the recovered message to the user. <b>NOTE:</b> Users will need an audio editing tool to listen to the recovered message. Standard media players (such as those from Microsoft) cannot play Mitel voice mail messages directly. <b>NOTE:</b> Once the message is deleted from the /vmail/vpim/sent folder, the message is irretrievable.
ALL Visual Voice Mail users get the following response when they try to access a message. "NO AUDIO CONNECTION"	Either Hunt group is not programmed in "Voice Mailboxes" form. Or All ports are busy.	Ensure that the Hunt group is programmed in the Voice Mailboxes form. Or As all voice mail ports are busy so Program more voice mail ports/ try after sometime.
Telephone only rings once OR Call transfer fails.	Supervised transfer timed out.	In the ESM VM Options form, disable the "Supervised Transfer" option. Default value of "Transfer Ringback timeout" is 17 seconds now.
Minor Alarm is raised.	Not enough DSP Resources available.	Add DSP resources. See "Increasing DSP Resources" in the "Installation Planner" chapter of the <i>Technician's Handbook</i> .



**Table 7.5:** Embedded Voice Mail (Continued) (Sheet 7 of 8)

Symptom	Probable Cause	Corrective Action
Sent time is wrong on e-mails forwarded from voice mail.	Time Zone not set correctly in Voice Mail programming.	In the ESM VM Network Servers form, program the "Time Zone" field.
Message waiting lamp is on but there is no message in your mailbox.	Multiple possible causes. Request to off MWI is failed as all ports were busy. Message Waiting Activate/ Deactivate Programming is wrong.	Program more VM ports to avoid this issue. Get ESM help to program Message Waiting Deactivate code.
MWI lamp on ONS sets failing to light.	Message Waiting Lamp disabled in circuit descriptor and/or ONS CLASS/CLIP Message Waiting option incorrectly set.	Verify that the circuit is assigned an ONS/OPS Circuit Descriptor that has the Message Waiting Lamp field on set to "Yes." Verify that CLASS/CLIP sets have a COS with the ONS CLASS/CLIP Message Waiting option set to "Yes" and that non-CLASS/CLIP sets have a CoS with the same option set to "No." Also check "CLASS/CLIP Station Side Software Support" in ESM help for message notification.
In the VM Mailboxes form of the System Administration Tool, voice mail boxes appear multiple times, or groups of voice mail boxes may repeat when changing from page to page.	Possible voice mail database corruption.	<ol style="list-style-type: none"> <li>1. Reboot the system.</li> <li>2. If still issue, then consult Mitel Technical Support team.</li> </ol>
Embedded voice mail fails to page external, or fail to perform supervised transfer to external number.	Programming conflict.	Set "Allow transfer to any number" field in "VM Options" form to "True".

**Table 7.5:** Embedded Voice Mail (Continued) (Sheet 8 of 8)

Symptom	Probable Cause	Corrective Action
Embedded voice mail goes out of service after “Load Controllers” command issued	The “Load Controllers” command is used to reboot the Peripheral Cabinet and/or the DSU. This has had the unexpected effect of causing the Embedded Voice to go out of service.	Avoid the use of the “Load Controllers” command. To do this you must physically reset the Peripheral Cabinet and/or the DSU. If this command has already been issued reset the 3300 controller to get the embedded voice mail back in service.
Voice mail message playback contains noise or audio level is too low.	The cause of voice quality problems can be associated with the TDM network, analog network, PSTN, IP network, user’s environment, or due to configuration errors in the equipment.	Refer Voice Quality Troubleshooting Guide.
User receives extra audio (tones and noise) on his or her voice mail message	Voice Mail system is not starting or stopping the recording at the right time due to incorrect correct tone detection file.	In the License and Option Selection form, ensure that the Country field is set correctly for the system. The Country setting determines the default language, dialing plan, tone plan, and loss and level plan for the system. Refer to the Hardware Technical Reference Manual for tables that list the Tone Plans.

## Networked Voice Mail

**Table 7.6:** Troubleshooting Networked Voice Mail (Sheet 1 of 3)

Symptom	Corrective Action
Internal system error when adding voice mail boxes.	Ensure that the name of the networked voice mail server matches the system name of controller.

**Table 7.6:** Troubleshooting Networked Voice Mail (Continued) (Sheet 2 of 3)

Symptom	Corrective Action
A mailbox number is not recognized when creating or forwarding a voice message.	<ol style="list-style-type: none"> <li>1. Make sure that the Networked Voice Mail option is enabled on all nodes.</li> <li>2. Make sure that the Primary Node ID length is the same for all nodes.</li> <li>3. Make sure that all mailboxes (excluding resiliency mailboxes) have different numbers.</li> <li>4. Make sure that the mailbox length is the same for all nodes.</li> </ol>
A mailbox number is not recognized when creating or forwarding a voice message to a remote mailbox on another cluster.	Enter the PNI before the mailbox number when addressing a message to a remote mailbox. Also, ensure that the programming in Network elements, VM Network Users and VM Network Server forms is correctly done.
The voice messages for resilient users are received in their mailboxes on the secondary controller while the user devices are on the primary controller.	<p>If a caller leaves the resilient user a voice message while the user's device is on the secondary controller, the message is recorded in the user's mailbox on the secondary controller.</p> <p>However if voice messages are being recorded in the mailbox on the secondary when the user's device is on the primary, ensure that the voice mail server is configured correctly. In a distributed voice mail configuration, ensure that the user's voice mail server is on their extension's primary controller.</p>
Message sent to a known valid user is returned with Failed to Deliver message.	<ol style="list-style-type: none"> <li>1. Ensure that the remote server is available.</li> <li>2. Ensure that the remote server has not failed over to its secondary server.</li> <li>3. Ensure remote node is programmed properly in the VM Network Servers form.</li> <li>4. If you have a centralized voice mail configuration, make sure that the user's voice mail server is not configured on the primary ICP of the user's extension.</li> </ol>
User can't use Dial-by-Name feature.	Dial-by-Name is not available for remote mailboxes.

**Table 7.6:** Troubleshooting Networked Voice Mail (Continued) (Sheet 3 of 3)

Symptom	Corrective Action
<p>You see the following log while you are monitoring the journalctl logs shell on boot up:</p> <pre>Starting up VM Corp Dir... ...Fault detected while starting up VM Corp Dir. Starting up SMTP Client Starting up SMTP Server tAppStartup ProcessorCoordinator started component ADAPTATION_LAYER_COORDINATOR tAppStartup ProcessorCoordinator started component APPLICATION_LAYER_COORDINATOR ResourceAlarmStartup ready. Task StartupHwRst being deleted while ACTIVE Voice Mail Starting in 0 minutes. Starting iPVM Version 6.21.00 Voice Mail Successfully Started.</pre>	<p>This log appears if you haven't enabled Networked Voice mail . Enable by adding entry in VM Network Servers form of local ICP controller.</p> <p>If you see "Voice Mail Successfully Started" at the end of this log, you will be able to log into the System Administration tool and your phones will come up.</p>
Voice messages are not compressed.	None. Networked Voice Mail does not support compression.

## Station Message Detail Recording

**Table 7.7:** Station Message Detail Recording Troubleshooting (Sheet 1 of 2)

Symptom	Probable Cause	Corrective Action
IP trunk call unsupervised transfer and queued to ACD path reports path extension instead of path reporting number.	Refer to Mitel Knowledge Base article 06-9999-00002 for possible causes.	Refer to Mitel Knowledge Base article 06-9999-00002.
When making a call in or out on SIP trunks the trunk number in the SMDR record is blank.	SMDR for SIP Trunks use the SMDR Tag field from the SIP Peer Profile form for the trunk number. If this field is blank, the trunk number in the SMDR record is blank.	Enter a Trunk Number (for example, 99) in this field and the number will be displayed as the trunk number in the SMDR record (for example, T099).

**Table 7.7:** Station Message Detail Recording Troubleshooting (Continued) (Sheet 2 of 2)

Symptom	Probable Cause	Corrective Action
Entering a non-verified account code during a call generates a single SMDR record instead of the normal two, one for the initial call and a second for the subsequent account code entry.	Account code entered within five seconds of call answer.	Change the “Suppress Initial SMDR record with Account Code Entered Time” in the SMDR Options form in ESM. The default is five seconds which generates one SMDR record if the account code is entered within 5 seconds of answering a call. If the account is entered after 5 seconds, two records are generated.

# Voice Networking

## Voice Networking Troubleshooting Tips

- Refer to the Voice Networking book in the System Administration Tool online help for information on Voice Networking.
- To view and manage pending (in-progress) SDS distribution updates and update errors, see the SDS Distribution Errors form in the System Administration Tool online help.

## Bandwidth Management

**Table 8.1:** Troubleshooting Bandwidth Management

Symptom	Possible Cause	Corrective Action
Bandwidth Statistics show duplicate CAC rejections.	ARS Routes not programmed correctly.	Ensure that ARS Routes form is programmed correctly.
Bandwidth Statistics are not being generated at the ZAPs.	Bandwidth Statistics and Reporting is not enabled.	Enable Bandwidth Management Statistics and Reporting in the Bandwidth Management Configuration form.

## Clustering

**Table 8.2:** Troubleshooting Clustering

Symptom	Possible Cause	Corrective Action
Unable to place calls between systems via IP trunks in a clustered, redirected, or resilient environment.	PBX Number in the ICP/PBX Assignment forms of the systems are programmed incorrectly.	For each system in the cluster, ensure that the system's PBX Number matches its CEID Index Number as defined in the Cluster Elements form.

## IP Networking

See [IP Trunking \(IP Networking\)](#).

## Multi Node Management

### MNM Fault Management

**Table 8.3:** Troubleshooting MNM Fault Management

Symptom	Possible Cause	Corrective Action
MNM Fault Management not functioning.	Too many elements in MNM Administrative Group.	MNM applications are only supported for up to 20 elements in an Administrative group. After you add the 21th element to the group, the MNM applications are disabled for the entire group. Reduce the number of elements to 20 or fewer.
	MNM Fault Management has been disabled.	Enable Fault Management in the Admin Group Fault Management form.

## MNM Backup and Restore

**Table 8.4:** Troubleshooting MNM Backup and Restore

Symptom	Possible Cause	Corrective Action
MNM Backup and Restore not functioning.	Too many elements in MNM Administrative Group.	MNM applications are only supported for up to 20 elements in an Administrative group. After you add the 21th element to the group, the MNM applications are disabled for the entire group. Reduce the number of elements to 20 or fewer.
	FTP server is down.	Ensure FTP server is working properly and that there is sufficient disk space on the server for the database files.
	Not enough client sessions available on FTP server.	Ensure that the FTP server supports the required number of concurrent client sessions. For example, if the Administrative Group has 10 elements, the FTP server must support a minimum of 10 concurrent client sessions.



## MNM Application Reach Through

**Table 8.5:** Troubleshooting MNM Application Reach-Through (Sheet 1 of 2)

Symptom	Possible Cause	Corrective Action
Cannot reach through to an element in the Administration Group.	Element has pre-MCD Release 4.0 software installed.	Upgrade element to MCD Release 4.0 or later software.
	Form incompatibility. The requested form is not supported. The local element has a later software version than the remote element and the selected form does not exist in the software version on the remote element.	Upgrade elements to same software version.
	Form not licensed. Some forms, such as the Fax Service Profiles form must be licensed on the element before they are available. If a form is licensed on the local element, but not licensed on the remote element, you cannot modify it.	License the functionality associated with the form on the remote node.
Application Reach-Through request fails.	User authorization profile is out of sync on the remote node	Use SDS to sync the User Authorization Profiles form across the Administrative Group.
	A network problem is preventing the local element from connecting to the remote element.	Contact your IT Support administrator.
	You do not have permission to access the requested form on the remote element. The Admin Policies form is not synchronized across all the elements in the Administrative Group.	Ensure that SDS is sharing the Admin Policies form to all elements in the Administrative Group.

**Table 8.5:** Troubleshooting MNM Application Reach-Through (Continued) (Sheet 2 of 2)

Symptom	Possible Cause	Corrective Action
Cannot find user on remote element.	User does not exist on the remote element because the user information was not distributed to the remote element by SDS.	Resolve any SDS pending updates or errors on the local element. Refer to the System Administration Tool online help for instructions.
Remote element not listed in <b>Show form on</b> field in Mozilla Firefox	Remote element running incompatible MiVoice Business software.	Upgrade remote element to MiVoice Business Release 9.0 or switch to Chrome.
Application Reach Through fails from MiVoice Business Release 9.2 or 9.1 SP1 PR1 to MiVoice Business Release 9.1 SP1 or earlier using Google Chrome or Microsoft Edge browser and the system displays the following error message: <b>Access Error: Forbidden</b>	This is due to the security enhancement in Chromium-based browsers.	<p>Upgrade to the latest version of the browser before you perform the following procedure:</p> <ol style="list-style-type: none"> <li>Do one of the following: <ul style="list-style-type: none"> <li>In the address bar of the Chrome browser, enter chrome: <b>//flags/#same-site-by-default-cookies.</b></li> <li>In the address bar of the Edge browser, enter edge: <b>//flags/#same-site-by-default-cookies.</b></li> </ul> </li> <li>Change the setting for <b>Same-Site by default cookies</b> from <b>Default</b> to <b>Disabled</b>.</li> <li>Close and restart the browser.</li> </ol>

# Resiliency

## IP Device Resiliency

**Table 8.6:** Troubleshooting IP Device Resiliency (Sheet 1 of 8)

Symptom	Possible Cause	Corrective Action
All resilient devices are not functioning (no dial tone) after the primary ICP goes out of service.	Secondary ICP is not in service.	Ensure that the secondary ICP is operating.
	IP phones are not provisioned as resilient.	Enter the Locate commands on the secondary ICP to determine the status of the IP phone. Check that the correct secondary CEID index appears in the Remote Directory Numbers form for each resilient IP phone. If not, provision the IP phones for resiliency, using the System Administration Tool. Refer to the System Administration Tool Online help.
	Cluster is not programmed correctly.	<p>Enter the Locate commands (see <a href="#">Locating Resilient Devices</a>) on the secondary controller to determine the status of the IP Phone.</p> <p>Refer to <i>Voice Networking -&gt; Configure Network in the System Administration Tool Online Help</i> for procedures on the following tasks:</p> <ol style="list-style-type: none"> <li>1. Ensure that the optional software required for clustering is enabled at each element.</li> <li>2. Ensure that each resilient IP device is connected to a controller that has Release 4.0 or later.</li> <li>3. Ensure that each element in the cluster is assigned a unique CEID in its Cluster Elements form.</li> <li>4. Ensure that ARS is programmed correctly to route calls to all the other elements in the cluster.</li> <li>5. In the Cluster Elements form ensure that you have programmed the Feature DN fields.</li> <li>6. In the ICP/PBX Networking form of each element, ensure that the PBX Number matches the CEID index number that is programmed in the Cluster Elements form.</li> <li>7. Check that the correct secondary CEID index appears in the Remote Directory Numbers form for each resilient IP phone.</li> </ol>

**Table 8.6:** Troubleshooting IP Device Resiliency (Continued) (Sheet 2 of 8)

Symptom	Possible Cause	Corrective Action
Resilient phones do not fail over to their secondary ICP when their primary fails.	The network may not be clustered or it may have been improperly clustered.	<p>To learn how to properly cluster a network, refer to <b>Configure Network</b> in the <i>System Administration Tool Help</i>.</p> <p>If you have clustered your network, verify that it has been properly clustered. Using the System Administration Tool on each 3300 ICP, verify that the Cluster Element Index in the Cluster Elements form has the same value as the PBX Number in the ICP/PBX Networking form. (In the Remote Directory Numbers form, look up the number of the phone or phones that are not failing over. Note the CEID number for the phones. Check the CEID numbers against those for the phones in the ICP/PBX Networking form. The numbers must match, and their values must not be higher than 1 to 999.</p> <p>On each phone that is not failing over, use the debug function to verify that its current ICP list contains a primary and a secondary ICP.</p>

**Table 8.6:** Troubleshooting IP Device Resiliency (Continued) (Sheet 3 of 8)

Symptom	Possible Cause	Corrective Action
		<p>For the 53xx phones, and for the 5540 console:</p> <ol style="list-style-type: none"> <li>1. Press both volume keys at the same time, release the volume-down key, dial 234 (“CFG”), then release the volume-up key to display configuration options.</li> <li>2. Press *to select <b>NETWORK PARAMETERS</b>, press * to select <b>VIEW CURRENT VALUES</b>, then press * to select <b>VIEW CURRENT NETWORK</b>.</li> <li>3. Press the volume-down key until <b>CUR CONTROLLER IP</b> is displayed. This is the address of the phone’s current ICP.</li> <li>4. Press the volume-down key until <b>ICP1 IP ADDRESS</b> is displayed. This is the address of the phone’s primary ICP.</li> <li>5. Toggle the volume keys (press the volume-down and then volume-up key, or vice-versa) to display <b>ICP2IP ADDRESS &lt;IP ADDRESS&gt;</b>. This is the IP address of the phone’s secondary ICP. Verify that this IP address is correct. If the phone does not display an IP address for a secondary ICP, use the <b>User and Services Configuration</b> form in the <i>System and Administration Tool</i> to provision the device with a secondary ICP.</li> </ol>

**Table 8.6:** Troubleshooting IP Device Resiliency (Continued) (Sheet 4 of 8)

Symptom	Possible Cause	Corrective Action
		<p>For the 69xx phones, and the 6970 conference unit:</p> <ol style="list-style-type: none"> <li>1. Press the Settings key on the phone to enter the Settings menu</li> <li>2. Select <b>Status</b> to view current status settings</li> <li>3. Press the right navigation key to select <b>Network General Info</b> then press the down navigation key to scroll through the values. On the 6940 and 6970, swipe up on the right side of the screen to scroll through the values.</li> </ol> <p>The <b>Current Call Server</b> entry displays the address of the phone's current ICP.</p> <p>The <b>Call Server 1</b> entry displays the address of the phone's primary ICP.</p> <p>The <b>Call Server 2</b> entry displays the address of the phone's secondary ICP.</p> <p>Verify that this address is correct. If the phone does not display an address for a secondary ICP, use the <b>User and Services Configuration</b> form in the <i>System Administration Tool</i> to provision the device with a secondary ICP.</p>
Resilient phones do not fail over to their secondary ICP when their primary fails.	The network may not be clustered or it may have been improperly clustered.	<p>On a 5020/5010 IP Phone</p> <ol style="list-style-type: none"> <li>1. Hold down both volume keys at the same time, and dial <b>33284</b> ("debug") to display debug options.</li> <li>2. Press <b>Superkey</b> until <b>Network</b> is displayed.</li> <li>3. Press the <b>volume-down</b> key until <b>Network – PBX IP &lt;IP address&gt;</b> is displayed. This is the address of the phone's current ICP.</li> <li>4. Press either the volume-up or volume-down key until <b>Network – PBX IP &lt;address&gt; #1</b> is displayed. This is the IP address of the phone's primary ICP.</li> <li>5. Toggle the volume keys (press the volume-down and then the volume-up key, or vice versa) to display <b>Network – PBX IP &lt;IP address&gt; #2</b>. This is the IP address of the phone's secondary ICP. Verify that this IP address is correct. If the phone does not display an IP address for a secondary ICP, use the User and Services Configuration form in the System Administration Tool to provision the device with a secondary ICP.</li> </ol>

**Table 8.6:** Troubleshooting IP Device Resiliency (Continued) (Sheet 5 of 8)

Symptom	Possible Cause	Corrective Action
One or more resilient phones are not functioning (no dial tone) after the primary ICP goes out of service	An IP device license is not available for the affected device(s) on the secondary ICP.	Ensure that you have provisioned enough IP device licenses on the secondary ICP. Refer to the <i>MiVoice Business Resiliency Guidelines</i> for details.
	May indicate a network failure.	Verify the network.
One resilient phone is not functioning (no dial tone) after its primary ICP goes out of service.	IP phone is not provisioned as resilient.	Enter the Locate commands <a href="#">Locating Resilient Devices</a> on the secondary ICP to determine the status of the IP phone. Check that the correct secondary CEID index appears in the Remote Directory Numbers form for each resilient IP phone. If not, provision the IP phones for resiliency, using the <i>System Administration Tool</i> . Refer to the <i>System Administration Tool Online</i> help.
While on a call at a resilient phone, the primary ICP goes out of service and the call is immediately dropped (no call survival). After you hang up the IP phone and go off-hook again, the IP phone is functioning on its secondary ICP.	The call was connected through a TDM trunk (for example PRI trunk) on the primary ICP that failed.	Program IP trunking on all ICPs.
While on a call at a resilient phone, the primary ICP goes out of service, and the call is immediately dropped (no call survival). After you hang up the IP phone and go off-hook again, the IP phone remains out of service.	Network failure (for example a Layer 2 switch that connects the IP phone to both the primary and secondary ICPs goes down).	Program redundancy into the network layer

**Table 8.6:** Troubleshooting IP Device Resiliency (Continued) (Sheet 6 of 8)

Symptom	Possible Cause	Corrective Action
After an IP phone fails over to its secondary ICP, you can make calls from it, but other TDM phones, trunks, or IP devices in the cluster cannot call it.	Call routing is not setup correctly.	<p>Enter the Locate commands <a href="#">Locating Resilient Devices</a> on the secondary controller to determine the status of the IP Phone. Refer to <b>Voice Networking -&gt; Configure Network</b> in the <i>System Administration Tool Online Help</i> for instructions on the following tasks:</p> <ol style="list-style-type: none"> <li>1. Ensure that each element in the cluster is assigned a unique CEID in its Cluster Elements form.</li> <li>2. Ensure that ARS is programmed correctly to route calls to all the other elements in the cluster.</li> <li>3. In the Cluster Elements form ensure that you have programmed the Feature DN fields correctly.</li> <li>4. In the ICP/PBX Networking form of each element, ensure that the PBX Number matches the CEID index number that is programmed in the Cluster Elements form.</li> <li>5. Check that the correct secondary CEID index appears in the Remote Directory Numbers form for each resilient IP phone.</li> </ol>



**Table 8.6:** Troubleshooting IP Device Resiliency (Continued) (Sheet 7 of 8)

Symptom	Possible Cause	Corrective Action
After the primary ICP is returned to service, the IP phones do not fail back to the primary. If an IP phone is on its secondary ICP, you hear beeps every 20seconds, and the phone display is frozen.	The “Allow Return to Primary ICP” is set to “No” in the Controller Registry form of the primary ICP.	In the System Administration Tool on the primary ICP, navigate to the following form: System Administration->System Options-> Controller Registry Configuration. In the Controller Registry form of the primary ICP, ensure that “Allow Return to Primary ICP” is set to “Yes”
	The duration of the health check is set too long in the Controller Registry form of the secondary ICP. The amount of time that elapses before an IP phone fails back to its primary can be quite long, depending on the health-check settings. With the default settings, after the primary ICP is back in service, the IP phones will take approximately 5minutes to fail back.	<b>WARNING: Contact Mitel Customer Engineering Services. Parameters must be changed in the Controller Registry form. DO NOT change any of these parameters without consulting Mitel Customer Engineering Services.</b>
Message waiting indicator on a resilient phone continues flashing for a Call back message that has already been returned	Cluster is configured to absorb routing digits	<ol style="list-style-type: none"> <li>1. In the <i>System Administration Tool</i>, ensure that routing digits on inbound and outbound routes are not being absorbed:– In the <b>Trunk Attributes</b> form, check how many digits are configured to be absorbed in the <b>Dial In Trunks Incoming Digit Modification - Absorb</b> field (should be blank).– In the <b>ARS Digit Modification Plans</b> form, check how many digits are configured to be absorbed in the <b>Number of Digits to Absorb</b> field (should be 0(zero)) for the appropriate Digit Modification Number.</li> <li>2. If digits are configured to be absorbed, create a new instance for the appropriate route(s) that does not absorb digits.</li> </ol>
Hot desk user does not receive voice mail.	Voice mail is embedded in an ICP that has failed or become unreachable.	Use centralized external voice mail system.

**Table 8.6:** Troubleshooting IP Device Resiliency (Continued) (Sheet 8 of 8)

Symptom	Possible Cause	Corrective Action
Hot desk user logs out previous user but cannot log in.	Both primary and secondary ICPs of the resilient hot deskphone are unreachable	Expected behavior. If both ICPs of a resilient hotdesk phone are unreachable, a Logout triggers the phone to rehome. User must wait until one of the phone's ICPs recovers and becomes reachable for the phone to be in service before they can log in to the phone.

## IP Console Resiliency

**Table 8.7:** Troubleshooting IP Console Resiliency (Sheet 1 of 2)

Symptom	Possible Cause	Corrective Action
A resilient IP console is not functioning (no dial tone) after the primary controller goes out of service.	IP Console is not programmed correctly for resiliency.	Ensure that the IP console is programmed for resiliency. Check that the correct secondary CEID index appears in the Remote Directory Numbers form for the IP console. See “IP Console Resiliency” in the <i>MiVoice Business Resiliency Guidelines</i> for details.

**Table 8.7:** Troubleshooting IP Console Resiliency (Continued) (Sheet 2 of 2)

Symptom	Possible Cause	Corrective Action
After an IP console fails over to its secondary ICP, you can make calls from it, but other IP devices in the cluster cannot call it.	Call routing and ARS are incorrectly programmed.	<p>Enter the Locate commands (see <a href="#">Locating Resilient Devices</a>) on the secondary controller to determine the status of the IP console. Refer to <i>Voice Networking -&gt; Configure Network in the System Administration Tool Online Help</i> for instructions on the following tasks:</p> <ol style="list-style-type: none"> <li>1. Ensure that each element in the cluster is assigned a unique CEID in its Cluster Elements form.</li> <li>2. Ensure that ARS is programmed correctly to route calls to all the other elements in the cluster.</li> <li>3. In the Cluster Elements form ensure that you have programmed the Feature DN fields correctly.</li> <li>4. In the ICP/PBX Networking form of each element, ensure that the PBX Number matches the CEID index number that is programmed in the Cluster Elements form.</li> <li>5. Ensure that the correct secondary CEID index appears in the Remote Directory Numbers form for the resilient IP console.</li> </ol>
Console fails back to its primary by queued calls are lost.		Ensure the Console is connected to the MiVoice Business.

## Voice Mail Resiliency

**Table 8.8:** Troubleshooting Voice Mail Resiliency (Sheet 1 of 2)

Voice Mail Type	Symptom	Possible Cause	Corrective Action
Embedded	After an IP phone fails over to the secondary, user cannot connect to their voice mail box.	A second voice mailbox has not been configured on the secondary ICP for the resilient device.	Configure a second voice mailbox.
		Call routing on the secondary ICP is not configured to allow a user to access the voice mail ports (by dialing the hunt group number).	Ensure that call routing is set up to allow the user to access the hunt group number of the voice mail port.
		The centralized 3300 ICP embedded voice mail controller is out of service.	Check the 3300 ICP embedded voice mail server.
	Users indicate that they are missing messages.	Messages are in mailboxes on both the primary and secondary ICPs.	Instruct user to check voice mail messages in both of their voice mail boxes (user must dial different hunt group numbers to access the voice mail systems on the primary and secondary ICPs).

**Table 8.8:** Troubleshooting Voice Mail Resiliency (Continued) (Sheet 2 of 2)

Voice Mail Type	Symptom	Possible Cause	Corrective Action
Centralized external	After an IP phone fails over to the secondary ICP, user cannot connect to the voice mailbox.	A voice mail box has not been configured on the external centralized voice mail controller for the resilient device.	Configure a voice mailbox for the user.
		Call routing on the secondary controller is not configured to allow a user to access the voice mail ports (by dialing the hunt group number).	Ensure that call routing is set up to allow the user to access the hunt group number of the voice mail port. Refer to the <i>MiVoice Business Resiliency Guidelines</i> for call routing configuration.
		The centralized voice mail application or server is out of service.	Check the voice mail application and server.

## T1 E1 Trunk Resiliency

**Table 8.9:** Troubleshooting T1/E1 Trunk Resiliency (Sheet 1 of 2)

Symptoms	Possible Cause	Corrective Action
Users cannot make T1/E1 calls through T1/E1 MMC modules in the primary or secondary controllers.	<b>Links are connected in reverse:</b> You have programmed T1/E1 trunk resiliency correctly, but the physical connections are reversed. The Input port on the secondary controller is connected to the PSTN and the Failover port on the secondary is connected to the main port on the primary.	Reverse the connections. See “Configuring T1/E1 Trunk Resiliency” in the <i>MiVoice Business Resiliency Guidelines</i> for a configuration diagram.

**Table 8.9:** Troubleshooting T1/E1 Trunk Resiliency (Continued) (Sheet 2 of 2)

Symptoms	Possible Cause	Corrective Action
The physical connections are correct and the primary controller is out of service, but users cannot make T1/E1 calls through the T1/E1 MMC on the secondary controller.	<b>Secondary is not programmed as resilient:</b> In the Digital Links form of the secondary controller, the Resiliency Link box is not checked, or you have not programmed the “Primary System Name” and “Secondary System Name”.	In the Digital Links form of the secondary controller: <ul style="list-style-type: none"> <li>• Select the T1/E1 link and click <b>Change</b> . Check the “Resilient Link” box.</li> <li>• From the Resilient Link ID drop-down menu, select a link identifier (1 to 4) for the secondary link. This link ID must match with the link ID that you assigned to the primary link.</li> </ul>
The physical connections are correct. However, alarms for the Trunk Alarm category on the secondary controller are exceeding the threshold limit. In addition, if the primary controller is out of service, users cannot make T1/E1 calls through the T1/E1 MMC on the secondary controller.	<b>Both links are designated as primary controller:</b> In the Digital Link Assignment forms of both controllers, the “Primary System Name” is set to the name of the Local controller.	<ul style="list-style-type: none"> <li>• Set the Primary System Name to the system name of the primary controller.</li> <li>• Set the “Secondary System Name” to the name of the secondary (Local) controller.</li> </ul>
When the primary controller is out of service, the T1/E1 trunks are not transferred to the secondary controller. No alarms are generated.	<b>Both links are designated as secondary controller :</b> In the Digital Link Assignment forms of both controllers, the “Primary System Name” is set to the name of the other controller. Both controllers have their own system name selected as the “Secondary System Name”.	Correct the T1/E1 trunk resiliency programming in the Digital Link Assignment forms of both systems. Refer to the <i>MiVoice Business Resiliency Guidelines</i> for T1/E1 trunk resiliency programming.
The primary controller fails over to the secondary but users are unable to make calls through the resilient T1/E1 MMC in the secondary controller. When the user attempts to make an outgoing call, the system is unable to seize the T1/E1 trunk.	<b>Route List Assignment form is programmed incorrectly.</b> The route list programming on either the primary or secondary controller is reversed.	Correct the route list programming. Refer to the <i>MiVoice Business Resiliency Guidelines</i> for T1/E1 trunk resiliency programming.

# System Data Synchronization

## Sharing Operations

**Table 8.10:** Troubleshooting Sharing Operations (Sheet 1 of 8)

Symptom	Possible Cause	Corrective Action
Unable to initiate sync following an MiVoice Business software upgrade/ downgrade. Sync button is grayed out.	Browser cache contains stale Sys Admin Tool data which is preventing the sync from working.	<p>Clear the browser cache.</p> <p>In Internet Explorer: press CTRL+SHIFT+DEL, select Temporary Internet Files, and clear Preserve Favorites website data. Leave other check boxes cleared, and then click OK.</p> <p>In Firefox: press CTRL+SHIFT+DEL, select Everything for "Time range to clear" and Cache, then click OK.</p> <p>In Chrome: press CTRL+SHIFT+DEL, select the <b>beginning of time</b> next to <b>Clear the following items from</b> and <b>Cached images and files</b>, then click <b>Clear Browsing Data</b>.</p> <p>- In Edge: press CTRL+SHIFT+DEL, select <b>Cached data and files</b>, and then click <b>Clear</b>.</p>

**Table 8.10:** Troubleshooting Sharing Operations (Continued) (Sheet 2 of 8)

Symptom	Possible Cause	Corrective Action
When you click the <b>Sync</b> button in Network Elements form, you receive the following Internet Explorer script error: “Object doesn’t support this property or method”	Internet Explorer security settings are preventing the synchronization.	<ol style="list-style-type: none"> <li>1. In Internet Explorer, click <b>Tools</b> and then click <b>Internet Options</b>.</li> <li>2. Click the <b>Security tab</b> and then click <b>Local internet</b>.</li> <li>3. Click Sites and then click Advanced.</li> <li>4. Add the IP address of the 3300 ICP to the zone.</li> <li>5. Close all Internet Explorer windows and then relaunch Internet Explorer.</li> <li>6. Log back into the 3300 Controller.</li> <li>7. Access the Network Elements form, select the controller and click <b>Sync</b>.</li> </ol>
The Start Sharing operation has not displayed any signs of progress for more than an hour (that is the operation appears to be hung).	Your Internet Explorer session is timing out before the Start Sharing operation is complete.	Install the required Internet Explorer registry file on your PC. The registry file extends your Internet Explorer session and prevents it from timing out before a Start Sharing is complete. Refer to Mitel Knowledge Base article HT1862 on Mitel Online for instructions.
Cannot start sharing with an element	SDS is not enabled on the remote element.	Ensure SDS is enabled in the System Options form of the remote element.



**Table 8.10:** Troubleshooting Sharing Operations (Continued) (Sheet 3 of 8)

Symptom	Possible Cause	Corrective Action
	Remote element not included in data sharing community.	Ensure that the remote (slave) element has been brought into the data sharing community. See “Start Sharing with a New Element” in the System Administration Tool online help for instructions. You must always bring a new element into an existing data sharing community from an element that is already in the data sharing community.
Data Sharing alarms are appearing	A minor system alarm is generated whenever an SDS data distribution error occurs.	Resolve the distribution error in the SDS Distribution Errors form. See “Resolving Pending Updates or Errors” in the System Administration Tool online help.
Data sharing forms not appearing in System Administration menu.	SDS is not enabled on the local element.	Ensure SDS is enabled in the System Options form of the local element.
	Form is not configured as shared.	Configure the form to be shared in the SDS Form Sharing form. See “Specifying the Shared Data” in the System Administration Tool online help.
	Shared form icon does not appear beside form name in System Tool Administration menu.	After you configure forms as shared, you must log out and log back into the System Administration Tool to see the Shared form icons.

**Table 8.10:** Troubleshooting Sharing Operations (Continued) (Sheet 4 of 8)

Symptom	Possible Cause	Corrective Action
Data not being shared	Data sharing status of remote element is set to "No".	You must start sharing with the remote element. See "Start Sharing Data" in the System Administration Tool online help.
	Scope of sharing is not set correctly.	Set the scope of the sharing. See "Identifying the Shared Data" in the System Administration Tool online help.
	Specific forms are not set as shared.	Ensure that the required forms are set to be shared. See "Identifying the Shared Data" in the System Administration Tool online help.
	Forms are set as shared but you have not started sharing with the element(s) yet at the corresponding scope.	Use the Start Sharing button in the SDS Form Sharing form to initiate sharing.
Data record exception is not working as expected	Record exception rules are not entered correctly.	Check to ensure that you have entered exception rules correctly. See "Specifying the Shared Data" in the System Administration Tool online help.
Unexpected application errors are being generated on the local element.	The system dimensions are not set the same across the elements. For example, one system supports 96 Classes of Service, the other element supports only 64 COS. The mismatch results in application errors.	Delete the errors and exclude the additional records from being shared. See "Specifying the Shared Data" in the System Administration Tool online help.

**Table 8.10:** Troubleshooting Sharing Operations (Continued) (Sheet 5 of 8)

Symptom	Possible Cause	Corrective Action
Data Sharing status for the element is not consistent with all the other SDS elements in the data sharing network even after you perform a sync operation. That is, the other elements indicate in their Network Element Assignment forms that they are sharing with the element, but data is not actually being shared.	You restored an old database that had SDS disabled.	To resolve this issue: <ol style="list-style-type: none"> <li>1. At the element at which SDS is off (element A). Turn SDS on and then back off again.</li> <li>2. Perform a Start Sharing operation from another SDS element (element B) in the data sharing community with element A.</li> <li>3. Perform a Sync operation from element B to element A to update any data that may be out of sync on element A.</li> </ol>
	You disabled SDS while the element was disconnected from the network.	To resolve this issue: <ol style="list-style-type: none"> <li>1. At the element at which SDS is off (element A), turn SDS on again.</li> <li>2. Perform a Sync operation from another SDS element (element B) in the data sharing community with element A. Do not share any forms.</li> </ol>
Unexpected transport errors are being generated at the local element.	The network connection between the elements is down resulting in transport errors.	Fix network issue and retry update errors.
Data Sharing Mismatch errors are being generated at the local element in the SDS Distribution Errors form.	A record has been updated on local element and sent to a remote (slave) element. The slave element has rejected the update because the slave's sharing status is out of sync with the local element (that is, the slave does not recognize that it should be sharing with the local element).	If you want the slave element to accept updates from the local element, perform a sync operation from the local element with the slave. If you want to stop sharing data with the slave element, perform a sync operation from the local element with the slave and then disable SDS at the slave element.
Unexpected Concurrent Change Rejected errors are being generated at the local element in the SDS Distribution Errors form.	Concurrent Change Rejected errors were created because during a network outage changes were made on individual elements.	Fix network issue and retry update errors.

**Table 8.10:** Troubleshooting Sharing Operations (Continued) (Sheet 6 of 8)

Symptom	Possible Cause	Corrective Action
	The shared data has different default settings because the system Country variants (set in the License and Option Selection form) are different on the master and remote elements.	Accept the values using the Force Change option, or do not share this data.
Resilient user and device data is not being shared after you upgraded the controllers to 3300 Release 7.0 software or higher.	By default, user and device data is not shared. You must first specify the resilient user and device data that you want to be shared with the secondary elements.	Specify the resilient user and device data that you want to be shared with the secondary elements.
	Version of the remote peer has not been updated on the local controller	Perform a synchronization from the local element to the remote peer.
Data for some fields are not being shared. Upgrade the controller to the higher software level.	If a 3300 Release 7.0 or later SDS-enabled controller is communicating with a 3300 Release 6.x SDS-enabled controller, only the forms that are supported by the Release 6.x SDS will be shared. User and device resiliency data will not be shared to the Release 6.x controller.	Upgrade the controller to the higher software level.
In the SDS Form Sharing form, some record restrictions appear as “Not supported in this Release”.	If you share the SDS Form Sharing form from a 3300 Release 7.0 controller to a controller running an earlier software release (from 3300 Release 6.1 UR2 to pre-Release 7.0) any new Release 7.0 fields that are not supported on the older software release are displayed as “Not supported in this Release” on the controller with the older software.	Upgrade the controller to the higher software level.

**Table 8.10:** Troubleshooting Sharing Operations (Continued) (Sheet 7 of 8)

Symptom	Possible Cause	Corrective Action
In the SDS Form Sharing form of a controller that has pre-3300 Release 6.1 UR2 software, some record restrictions are incorrectly displayed as "Account Code".	If you share the SDS Form Sharing form from a 3300 Release 7.0 or later controller among controllers that have pre-3300 Release 6.1 UR2 software, restrictions in the Feature Access Codes form may appear incorrectly. If you restrict sharing of the Call Park and Call Park Retrieve fields from the 3300 Release 7.0 system, these restrictions are incorrectly displayed as "Account Code" on the controllers with the older software.	Upgrade the controller to the higher software level.
Errors show that data has been distributed to a network element in a way that is not consistent with the data in the Remote Directory Number form.	An administrator made an incorrect entry to the Remote Directory Number form at an element somewhere in the network and the change has been propagated by SDS.	Delete the inconsistent record from the Remote Directory Number form, and reprogram it appropriately.
Errors show that login status for a hot desk user has been improperly shared between the user's primary and secondary ICP.	A failover occurred between the time the user logged in from one device and then another. For example, an external hot desk user logs in from their cell phone, there's a failover, and before a failback can occur, they log into from their office desk phone.	Perform a sync operation from the local element to the remote peer.
There are many SDS Data distribution errors occurring on the department/location forms. Performing a Form Comparison results in conflicts for department/location. A change to the department field is not distribute throughout the network or cluster.	In a heavily congested clustered hospitality deployment, if there are a many hospitality operations being performed at the same time (either via PMS or GSA or a combination of both), then there is the possibility that department/location operations may result in distribution errors.	Perform an SDS synchronization of the department/location forms. This will update all users that reference the department/location fields with the new department/location strings.

**Table 8.10:** Troubleshooting Sharing Operations (Continued) (Sheet 8 of 8)

Symptom	Possible Cause	Corrective Action
When adding a new element to a migrated network, you receive either of the following error messages after you initiate the <b>Start Sharing</b> operation: “Synchronization failed. You must migrate this node to the new data model before attempting to join the SDS network” “Synchronization failed. The target for this operation must migrate to the new model first”.	You attempted to add a non-migrated element to the GDM network.	Follow the procedure described in “Adding an Element to the Migrated Network” in the System Administration Tool online help.
Start Sharing operation fails in a mixed release network and the node initiating the sync is an older release than the slave node.	Releases may have database schema differences that result in some data not being accepted on some nodes.	Retry operation by initiate Start Sharing from node running newer release.
Distribution error caused by associating two users to the same phone service (which is not allowed) from MiCollab persists after problem corrected.	Failed to perform Sync operation after problem corrected.	Perform an SDS synchronization of the User and Services Configuration form to MiCollab.

## Sync Operations

**Table 8.11:** Troubleshooting Sync Operations (Sheet 1 of 4)

Symptom	Possible Cause	Corrective Action
Specified data has not been synchronized after you complete a Start Sharing operation.	The <b>Start Sharing</b> operation does not synchronize all the shared data across the elements. Only data in the Network Elements form and Cluster Element Definition form. It adds the element to the sharing community (member elements) and begins the sharing of data at the specified scope.	If you want to synchronize the shared system form data across the elements, you should compare the forms and then perform a <b>Sync</b> operation. See “Comparing Forms and Synchronizing Data” in the System Administration Tool online help.

**Table 8.11:** Troubleshooting Sync Operations (Continued) (Sheet 2 of 4)

Symptom	Possible Cause	Corrective Action
Cannot sync from the local element to a remote element.	The IP addresses assigned to the elements in the Network Elements form are not unique.	Ensure that each element in the Network Elements form is assigned a different IP address.
	The system name or type for the network element on the local and remote nodes do not match.	Ensure that the same system name or type is assigned to the element in the Network Element Assignment forms of both the local and remote element.
Synchronizations take too long.	Traffic on the network is slowing the rate of record updates.	Perform the synchronization during a period of low network traffic (for example, after business hours).
	Large amounts of data are being synchronized across many elements.	Perform concurrent synchronizations to reduce the amount of time required to complete the synchronizations.
After a sync operation, large numbers of data distribution update errors appear in the SDS Distribution Errors form.	The remote element did not get the updates because the network connection to that element was down.	Fix the network issue. Retry the distribution updates. See “Resolving Pending Updates or Errors” in the System Administration Tool online help.
Many data distribution update errors appear in SDS Distribution Errors form after a concurrent sync operation.	During a concurrent synchronization, both the master and member elements reject changes coming from other network elements. Rejected changes create distribution update errors on the master element.	See “Resolving Pending Updates or Errors” in the System Administration Tool online help.
Cannot sync with the remote element (transport error).	SDS is disabled on the remote element.	Enable SDS in the System Options form of the remote element.
	Network connectivity is broken.	Fix network issue.

**Table 8.11:** Troubleshooting Sync Operations (Continued) (Sheet 3 of 4)

Symptom	Possible Cause	Corrective Action
Synchronization fails due to a form interdependency rule violation.	A synchronization may fail if you attempt to synchronize a form before a form that it is dependent on is completed. For example, you might be unable complete the ARS Digits Dialed Assignment form until the ARS Routes form has been completed.	Synchronize the form data in order of form dependency.
Errors show that data has been distributed to a network element in a way that is not consistent with the data in the Remote Directory Number form.	An administrator made an incorrect entry in the Remote Directory Number form at an element somewhere in the network and the change has been distributed.	Delete the inconsistent record from the Remote Directory Number form, and reprogram it appropriately.
Sync operation from MCD 4.2 network element to network elements with previous releases installed fail.	The previous MiVoice Business software does not recognize the MCD 4.2 DEI (Data Entity of Interest).	Refer to Mitel Knowledge Base article HO834 .
When adding a new element to a migrated network, you receive either of the following error messages after you initiate the <b>Start Sharing</b> operation: “Synchronization failed. You must migrate this node to the new data model before attempting to join the SDS network” “Synchronization failed. The target for this operation must migrate to the new model first”.	You attempted to add a non-migrated element to the GDM network.	Follow the procedure described in “Adding an Element to the Migrated Network” in the System Administration Tool online help.



**Table 8.11:** Troubleshooting Sync Operations (Continued) (Sheet 4 of 4)

Symptom	Possible Cause	Corrective Action
After adding a new element to an SDS network, the elements have inconsistent on as (where a directory number occurs in one database but not another).	The new element contains form data which requires synchronization.	<ol style="list-style-type: none"><li>1. Access the Network Elements form on the primary element.</li><li>2. Click the check boxes beside the primary and secondary elements that you want to synchronize.</li><li>3. Click <b>Sync</b> .</li><li>4. Select the <b>Data Repair</b> option in Confirm Sync to Element.</li><li>5. Select the following form data:<ul style="list-style-type: none"><li>– Service Hosting Data</li><li>– System Level Call Handling</li></ul></li><li>6. Click <b>OK</b> .</li></ol>

## Hunt Group or Ring Group Data Distribution Errors

**Table 8.12:** Troubleshooting Hunt Group or Ring Group Data Distribution Errors (Sheet 1 of 2)

Symptom	Possible Cause	Corrective Action
Data distribution alarm is generated. Data distribution errors related to resilient hunt groups or ring groups are displayed in the SDS Distribution Errors form.	Remote (secondary) controller does not support hunt group or ring group resiliency. The controller that you have selected as the secondary is not running the required software: Release 7 (or later) for hunt group resiliency or 3300 Release 8.0 (or later) for ring group resiliency.	Install the required software on the secondary controller, or select a different controller that is running the required software as the secondary controller. Then, delete the distribution error updates.
	Hunt group or ring group already exists on remote (secondary) controller. When you enable resiliency for a group in the Hunt Group Assignment or Ring Group Assignment form, the system adds the group data to the secondary controller. If a group with the same pilot number already exists on the secondary controller, the add group operation fails.	To fix this problem, you must <ul style="list-style-type: none"> <li>• Delete the hunt group or ring group from the secondary controller and then retry the updates from the SDS Distribution Errors form, or</li> <li>• Disable resiliency for the hunt group or ring group, delete the corresponding error updates, and leave the two hunt or ring groups separate, or</li> <li>• Perform a synchronization of the hunt group or ring group data from the primary controller to the secondary controller.</li> </ul>

**Table 8.12:** Troubleshooting Hunt Group or Ring Group Data Distribution Errors (Continued) (Sheet 2 of

Symptom	Possible Cause	Corrective Action
Data distribution alarm is generated. Data distribution errors related to resilient hunt groups or ring groups are displayed in the SDS Distribution Errors form - continued.	SDS failed to delete the Remote Directory Number (RDN) entry for the hunt group or ring group pilot number from the secondary controller's Remote Directory Numbers form. Because the RDN entry could not be deleted, SDS could not update the secondary controller with the hunt group or ring group data.	Manually delete the RDN entry for the hunt group or ring group pilot number from the secondary controller's Remote Directory Numbers form. Then, retry the updates from the SDS SDS Distribution Errors form.
	Hunt group or ring group member does not exist on (remote) controller. If you add a member to a resilient hunt group or ring group and the directory number of the member is not programmed as a RDN or a device on the secondary controller, the update fails and SDS generates a distribution error.	Log into the secondary controller and program the DN of hunt group or ring group member into the Remote Directory Numbers form. Then, log into the primary controller and retry the updates from the SDS Distribution Errors form.
	A new device was added to a resilient hunt group or ring group in the Group Administration Tool. Because the member is not programmed as a RDN on the secondary controller, the update fails and SDS generates a distribution error.	

# Local Area Network

## LAN Troubleshooting Tips

For AX, CX(i)-II and MXe-III controllers, see section Using Layer 2 Statistics for Ethernet architecture in these controllers.

Release 9.0 uses Linux as its operating system. This brings with it network tools `ethtool` and `tcpdump`. These tools are run using the Linux shell.

- For IP Phone and physical network connectivity problems:
  - Verify that the device has power.
  - Verify the Ethernet port LEDs on the device that the set connected are on.
  - If the link is down, try with another port. Verify that proper cabling is installed between the end devices.
  - Verify that a crossover cable was not installed instead of a straight-through cable, and vice-versa.
- For network media problems:
  - If there is excessive noise, check for cabling problems.
  - If there are excessive collisions, check for duplex mismatch problems.
  - For Cyclic Redundancy Check (CRC) errors, check if there is a faulty NIC or flow-control.
  - If there are excessive runt frames, check for bad cables, duplex mismatches or a bad PC NIC.
- For network connectivity problems, identify the path between two end devices by doing the following PING test (in order):
  - Local
  - Local gateway
  - Remote gateway
  - Remote IP.
- There are several L2 maintenance commands that are useful for collecting details: See [Using Layer 2 Statistics](#).
- Maintenance and troubleshooting of your LAN/WAN network is the responsibility of your network provider. Mitel Technical Support can help you isolate minor network problems; Technical Support will escalate complex network problem to Professional Services, a billable service. Before contacting Mitel Technical Support with a LAN issue, ensure that you have the following information ready:
  - network diagram
  - “route -n” command results
  - results of PING test between controller and IP Phone
  - “rness verify” command results
  - “state xnet all”, “ESM Maintenance” command results

# LAN Troubleshooting

**Table 9.1:** LAN Troubleshooting

Symptom	Possible Cause	Corrective Action
Loss of PC network connectivity through IP phone	<p>If your PC is connected to the network through an IP phone, your PC network connection is interrupted for approximately 1 to 2 seconds</p> <ul style="list-style-type: none"> <li>• if the IP phone momentarily loses power</li> <li>• if you manually reset the IP phone via the debug menu, or</li> <li>• if the IP phone automatically resets because it loses connectivity to the 3300 ICP for 10 minutes.</li> </ul> <p><b>NOTE:</b> If a resilient IP phone fails over to its secondary controller, the PC does not lose network connectivity.</p>	None. Connection is automatically restored in 1 to 2 seconds.
LAN Port 2 does not work for the MXe III-L controller	LAN Port 2 has been disabled for normal usage on the MXe III-L controller.	None. However, LAN port 2 can be used when debugging LAN issues.

## Using Layer 2 Statistics

The System Administration Tool provides various Layer 2 (L2) Ethernet traffic counters that can help with debugging LAN problems. The counters appear in the output of the “L2 Stat Port” maintenance command.

A LAN that is not operating correctly can cause IP voice quality issues ranging from minor annoyance to an inability to hold an intelligible phone call.

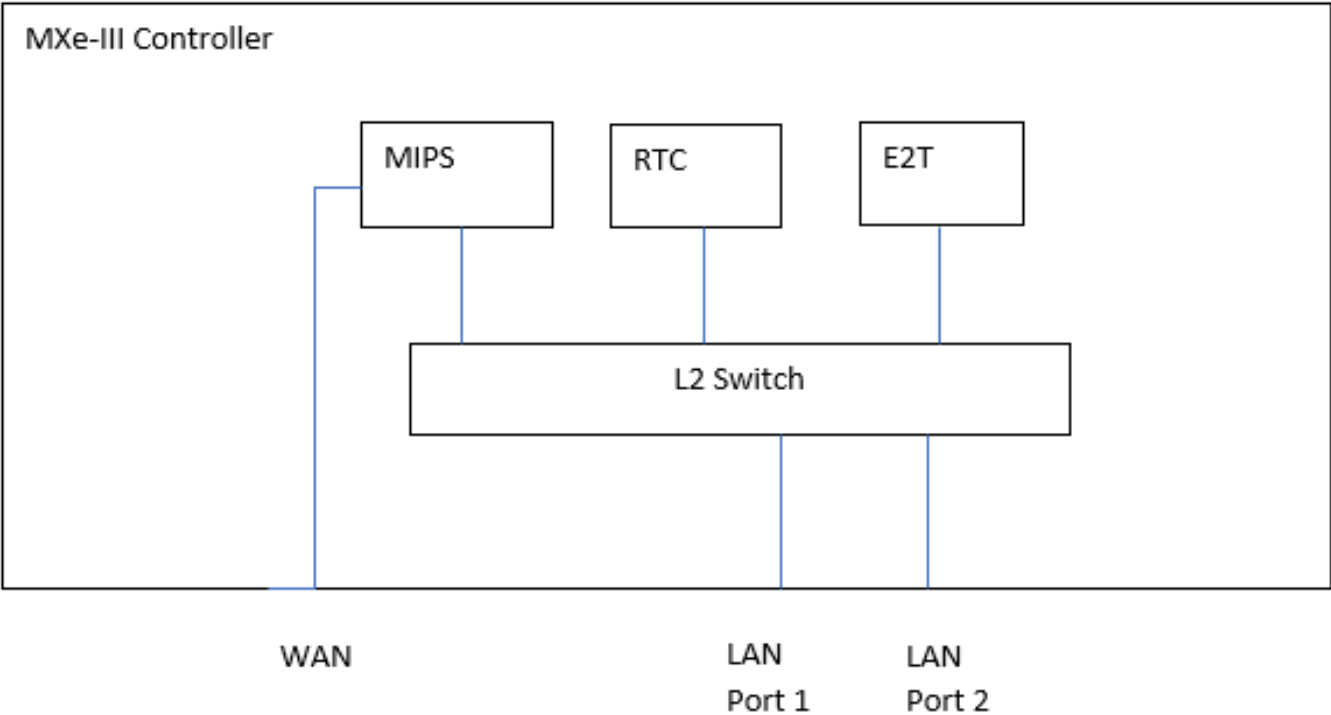
Incorrectly operating LANs can also cause data transfer problems for computer users such as slow response times.

The following is general information regarding LANs and what the L2 traffic parameters mean. The table at the end indicates probable causes of a particular L2 error and actions to take to try and resolve the error.

### AX, CX(i) 2 and MXe-III/MXe III-L Layer Statistics

To help with debugging LAN issues with the AX, CX(i)-II, and MXe-III/MXe III-L controllers, please review the following architecture of these controllers. An example is shown for the MXe-III controller, and the same concept applies for the other controllers.

These controllers have an internal L2 switch. This is shown in MXe-III LAN Architecture in the below figure. To debug network interface issues, Linux commands such as **mii-tool** cannot be used as this gives debug information for the RTC card network interface that is internal to the controller.



The following commands are available to assist in debugging networking issues. Note that for MXe-III and CXi-II controllers, the L2 address must be programmed for these commands to work.

The L2 debug information is available using System Administration Tool maintenance commands, or using the Linux shell.

**LAYER 2 SWITCH STATUS**

System Administration Tool Maintenance Command
L2 STATUS SWITCH

System Administration Tool Maintenance Command
L2 STATUS SWITCH

Linux Shell Command	Software Version
mcdDebug icpl2StatShow 1	9.0
mcdDebug L2SwitchStatus	9.1 and higher

These commands show the status of the internal L2 switch of the controller.

**LAYER 2 PORT STATUS**

System Administration Tool Maintenance Command	
L2 STATUS PORT	Summary of port information.
L2 STATUS PORT <portnum>	Detailed port information.

These commands are used to show the physical (speed, duplex, flow control) status and Ethernet packet information for the L2 switch ports. Specify 0 for a summary of all ports. For detailed information, specify a specific port number. Ports 1 and 2 refer to the front panel Ethernet ports.

**LAYER 2 SPANNING TREE STATUS**

System Administration Tool Maintenance Command
L2 STATUS ST
L2 STATUS SPANNIG-TREE

Command	Software Version
mcdDebug icpl2StatShow 3	9.0
mcdDebug L2SpanningTreeStatus	9.1 and higher

These commands are used to show the spanning tree information for ports 1 and 2. Spanning tree is disabled by default.

**LAYER 2 MAC FORWARDING TABLE STATUS**

System Administration Tool Maintenance Command	
L2 STATUS PORT	MAC Forward table for all ports.
L2 STATUS PORT <portnum>	MAC Forward table for specific ports.

Command	Software Version
mcdDebug icpl2StatShow 4	9.0
mcdDebug L2MACForwardTable	9.1 and higher

These commands are used to show the MAC forwarding table in the L2 switch.

**LAYER 2 Mirror Command (Excluding Mx III-L Controller)**

The L2 mirror command provides the ability to monitor various Ethernet ports on the L2 switch. The mirror command is not available for the CX-II controller.

The monitoring is done by connecting the Ethernet port of a laptop to port 2 of the controller and then use Wireshark program to monitor the network traffic.

The L2 mirror commands are entered using mcdDebug command. On the Linux shell enter:

```
mcdDebug
```

Enter CTRL-C to exit mcdDebug.

For a list of the mirror commands, enter:

- Enter mcd command -> xmirrorHelp
  - The syntax is:
 

```
xmirror "<sniffer_port> <port_mirror1> ..."
```

```
xmirror 0 (turns off port mirroring)
```
  - CXi: The sniffer\_port must be between 1 and 17.
  - MXe: The sniffer\_port must be 1 or 2.
  - AX: The sniffer\_port must be 1 or 2.
  - You may use port designation for the ports to mirror:
    - internal ports:
      - RTC port: rtc (except in AX)
      - APC port: apc
      - E2T port: e2t (if no E2T module, RTC will be mirrored)
      - all internal ports: internal
    - external ports: external (excludes target port).
    - all ports: all (excludes target port).
  - Port listing is available with command: icpL2StatShow 2 value = 653 = 0x28d

### Example

The following examples assume that port 2 is connected to the laptop that is monitoring the network traffic:

To monitor port 1, enter:

- Enter mcd command -> xmirror "2 1"
- Port mirror is set to '2 1'.
- IGMP snooping stopped
- port mirroring 2 <- 1 started

To monitor the rtc card enter:

- Enter mcd command -> xmirror "2 rtc"
- Port mirror is set to '2 rtc'.
- port mirroring 2 <- 1 stopped
- port mirroring 2 <- RTC started

To monitor the RTC card and E2T card, enter:

- Enter mcd command -> xmirror "2 rtc e2t"
- Port mirror is set to "2 rtc e2t"
- port mirroring 2 <- RTC stopped
- port mirroring 2 <- RTC, E2T started



To show the state of the mirroring, enter:

- Enter mcd command -> xmirrorShow
- port mirroring 2 <- RTC, E2T

To stop monitoring, enter:

- Enter mcd command -> xmirror 0
- port mirroring 2 <- RTC, E2T stopped
- IGMP snooping started

### Example

The following examples show enabling port mirroring, displaying the status and then disabling port mirroring for an MxIII controller:

To enable mirroring, enter:

```
Enter mcd command -> xmirror "2 1"
Port mirror is set to '2 1'
%IGMP snooping stopped;
port mirroring 2 <- 1 started
```

To display the status of the mirroring, enter:

```
Enter mcd command -> mips_xconfig "mirror show"
port mirroring 2 <- 1
value = 0 = 0x0
```

To disable mirroring, enter:

```
Enter mcd command -> xmirror 0
port mirroring 2 <- 1 stopped
IGMP snooping started
value = 0 = 0x0
```

Type CTRL-C to exit mcdDebug.

### LAYER 2 Mirror Command (MxIII-L Controller)

The L2 mirror command provides the ability to monitor Ethernet traffic on LAN port 1 of the MxIII-L controller.

You can monitor Ethernet traffic by connecting the Ethernet port of a laptop to LAN port 2 of the MxIII-L controller, and then using the Wireshark program.

**NOTE:** LAN port 2 of the MxIII-L controller is disabled by default, and is enabled when mirroring is turned on.

The L2 mirror commands are entered using mcdDebug command. On the Linux shell enter:

```
mcdDebug
Enter mcd command:->
```

For the syntax of the mirror command, enter:

Enter mcd command -> xmirrorHelp

The syntax is:

```
xmirror "<sniffer_port>"
```

```
xmirror 0 (turns off port mirroring)
MXeIII-L: The sniffer port must be 2
Mirrors LAN port 2 to LAN port 1.
xmirrorShow
```

### Example

To enable mirroring, enter:

```
Enter mcd command -> xmirror "2 1"
Mirroring to port 2
value = 0 = 0x0
```

To display the status of the mirroring, enter:

```
Enter mcd command -> xmirrorShow
Mirroring to port 2
value = 0 = 0x0
```

To disable mirroring, enter:

```
Enter mcd command -> xmirror 0
Disabled port mirroring.
value = 0 = 0x0
```

## CRC FCS and Alignment Errors

When a network device transmits a packet, it appends a Cyclical Redundancy Check (CRC) to the end of the frame. The CRC value is unique for the particular packet since, like checksum generation, the data in the packet is used by the CRC generation algorithm to generate the CRC value.

If the data in the packet gets altered between the transmitting device and the receiving device, then the receiving device will detect that the packet has been altered since the CRC will not match the contents of the packet. The result is an CRC error.

An FCS error (Frame Check Sequence) is another name for a CRC error.

An alignment error occurs when a packet has an FCS error and the packet also fails to have octet alignment. When a packet has octet alignment the packet has an even byte count.

# Diagnosing Problems

## Diagnostic Tools

The following table lists the tools available to help you diagnose problems on a 3300 ICP system.

**Table 10.1:** Diagnostic Tools (Sheet 1 of 5)

Tool Name	Function	Location	Applies to
Alarm Details	Provides the definition and location of the alarms.	In Maintenance and Diagnostics form of the Administration Tool. Refer to the System Administration Tool online help for instructions on how to use these tools.	3300 ICP system
Alarm Email Notification	Sends an email notification to specified personnel whenever a Minor, Major, or Critical occurs or whenever an existing alarm transitions to a different level.		
Bandwidth Statistics IP network	Allows you to see to see real-time bandwidth usage as well as historical bandwidth statistics.		IP Network
CESID Logs Emergency Services feature	Allows you to monitor and troubleshoot device moves and automatic CESID updates.		Emergency Services Feature
Device Connectivity (Device Connectivity forms) IP network and IP phones	Reports previous and latest Layer 2 MAC and port number.		IP network and IP phones
IP Telephone Status (IP Telephones -All form) IP phones	Displays all of the IP telephones that are part of the system and information concerning their status.		IP phones

**Table 10.1:** Diagnostic Tools (Continued) (Sheet 2 of 5)

Tool Name	Function	Location	Applies to
L2 STAT commands	Provides L2 switch ports details: MAC address, status, Spanning Tree information.		IP network
Line Measure Tool (Line Quality Measure form)	Tests to determine 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:		Loop Start trunks
Audit Trail Logs	Audit Trail Logs provide a historical record of changes made to the system from the System Administration Tool and various other user interfaces and applications. It does this by recording certain actions (such as who logged in and when) and storing this information.		System administration
Shared Data Update Logs	Allows you to view and manage all pending (in-progress) SDS distribution updates and update errors.		System Data Synchronization
Server Manager SOS Logs	Collects system-level logs and diagnostic information that Mitel Technical Support can use to diagnose problems.	In View Logs Files form of Server Manager.	3300 ICP system

**Table 10.1:** Diagnostic Tools (Continued) (Sheet 3 of 5)

Tool Name	Function	Location	Applies to
System Diagnostics Reporting	Allows you to collect system diagnostics information. The 3300 ICP system records diagnostic information about the system performance in a series of files. These files includes xrtc, pstswlog.db, hdrswlog.db logs, call control statistics and other information that Mitel Technical Support can use to diagnose system problems.	In Maintenance and Diagnostics form of the Administration Tool. Refer to the System Administration Tool online help for instructions on how to use these tools.	3300 ICP system users who do not have permission to collect SOS logs using Server Manager.
Voice Quality Monitoring and Statistics	Monitors voice quality for selected MiVoice IP Phones to identify and record: <ul style="list-style-type: none"> <li>voice quality problems requiring immediate attention.</li> <li>trends in voice quality performance.</li> </ul>		3300 ICP system and NetAlly tool. (Note that the NetAlly tool must be purchased separately).
IP Phone Analyzer	Supports IP Phone troubleshooting.	IP Phone Analyzer PC. See IP Phone Analyzer online help.	IP phones
Java Console	Supports IP Console troubleshooting.	5550 IP Console PC. To launch the Java console: at the IP Console PC, select <b>Start/ Settings/ Control Panel</b> , and then click <b>Java Plug-in</b> .	5550 IP console

**Table 10.1:** Diagnostic Tools (Continued) (Sheet 4 of 5)

Tool Name	Function	Location	Applies to
LEDs	Indicate overall status of unit.	Front of each unit. See “Appendix D: Status LEDs” in the <i>Technician’s Handbook</i> for details. 3300 ICP hardware	3300 ICP hardware
	Indicate status of power supplies and RAID controller.	Back of MxIII/MxIII-L	
Mitel System Platform Log Viewer	Enables the monitoring of Post software logs on an PC.	Utility that runs on a PC and connects to the system to be monitored. See the “View Logs” section in the “Maintenance” chapter of the <i>Technician’s Handbook</i> .	3300 ICP software
Journalctl logs	Shows error messages during the installation of the 3300. Monitors the boot sequence.	Controller Maintenance Port. See <i>Technician’s Handbook</i> .	3300 ICP software
Phone Configuration (Debug) Menu	Allows you to <ul style="list-style-type: none"> <li>Monitor the phone settings</li> <li>Program a static IP address</li> <li>Hard code connection speed and duplex mode (reboot while pressing 9)</li> <li>Auto-negotiation is preferred.</li> </ul>	IP phones with display. See <a href="#">Access Configuration Menu on Single Mode IP Phones</a> for details.	Single Mode IP phones
Dual Mode Phone Configuration (Debug) Option	Allows you to configure/view: <ul style="list-style-type: none"> <li>Network parameters</li> <li>Hardware components</li> <li>Set the phone mode</li> <li>PIN, IP address, DHCP, Video.</li> </ul>	5215 IP Phone (Dual Mode), 5220 IP Phone (Dual Mode), 5320 IP Phone, 5330 IP Phone, and 5340 IP Phone. See <a href="#">Access Configuration Menu on Dual Mode Phones</a> .	Dual Mode IP phones

**Table 10.1:** Diagnostic Tools (Continued) (Sheet 5 of 5)

Tool Name	Function	Location	Applies to
SMDR	Provides the call paths (call logs).	Controller (telnet from Maintenance PC).	3300 ICP system
SNMP Traps	Contain information about system resource usage for consumption by an SNMP manager.	The SNMP agent communicates with SNMP-compatible Network Management Stations and supports industry-standard MIB-II definitions as well as proprietary SNMP extensions. See the System Administration Tool online help.	3300 ICP system

## Working with Logs

The MSP Log Viewer provides a way for you to view logs in real time as they are happening and read log files generated by the logging service. The application can connect to any Mitel application/service or component that uses the OtpLogs server with a Report Device.

MSP Log Viewer displays logs based on severity, log type and log source.

### Subscribing to logs in real time

Subscribing to logs in real time is preferred as it provides a view of the logs as they are posted (active MSP log file). The server knows what subscriptions are active and does not process logs that are not currently wanted by MSP Log Viewer. MSP Log Viewer filters the desired logs using the severity field. It can also subscribe to lesser severity logs (logs that would normally be filtered out) for specified log sources.

To subscribe to logs in real time you must connect to the IP address or network name of the MiVB

1. Select **File > Connect**.  
A Log Viewer Connect window appears.
2. Enter the IP address where the application is running using the IP address or known network name, for example:  
10.10.10.10  
MyServer
3. Click **OK**.

If the application you are connecting to is listening at the address you entered in step 2 and it is reachable from MSP Log Viewer, then you will see some logs posted on the success of your configured subscriptions (Error, Warning, etc). Otherwise you will see the error "Target is not ONLINE". If you see this error,

check the IP address you entered and make sure you can route to the IP address from your PC. If you have multiple IP addresses, you may need to configure MSP Log Viewer to use the IP address that can be routed from the application you are trying to connect with.

## Viewing logs from an inactive file

You can open and view logs in inactive files, including files in MSPLog format. For example, opening the logs for MiVBC from this location: C:\ProgramData\Mitel\LogView\console. The MiVB logs when collected using Server Manager can be found at <folder sos extracted to>\var\mivb\active\db\database\sw\_logs.

To read logs from a file

1. Select **File > Open Log File**.
2. Browse to the location of the file and select it.

## Filtering subscription logs

You can filter logs by severity field. Subscribing to an application's active logs requires that the application be configured to publish its logs using Mitel's logging service through the report logging device.

To filter subscription logs

1. Select **Edit > Filters**.
2. In the **Filter Settings** dialog, select the **Source** tab.
3. In the **General filter applied to all sources** section, select the severity level of logs you want to see from any log source.
4. To add a source log, click **Add** and enter the name of the source in the **Source Name** box.
5. Leave the **Use Legacy Subscriptions** option unchecked and click **OK**.

**NOTE:** It is possible that the application's log server is blocking logs when there are subscriptions to them. If the application you are connecting to has filtered its logs, consult the application's documentation to find out how to change those settings.

To save a subscription filter

1. Select **Edit > Save Filters**.
2. Enter a name in the **File Name** box and click **Save**.

To load a subscription filter

1. Select **Edit > Load Filters**.
2. Browse to the location of the filter file and select it.
3. Click **Open**.



## Filtering your view

In addition to filtering subscription logs, you can filter the view of the logs you have received. Filtering a view works the same way as filtering the subscription logs except that you are filtering logs that you have already received.

1. Select **Edit > Filters**.
2. In the Filter Settings dialog, select the **View** tab.
3. In the **General filter applied to all sources** section, select the severity level of logs you want to see from any log source.
4. To add a source log, click **Add** and enter the name of the source in the **Source Name** box.
5. Leave the **Use Legacy Subscriptions** option unchecked and click **OK**.

## System Performance

### Diagnosing CPU slowdowns and overloads

Tasks such as Ethernet packet processing, voice encryption, and call control affect call processing. To determine how busy the system is at processing calls, the CPU usage of these tasks is calculated.

### Show Status Resource

System resource commands provide information for diagnosing a system that is running slow or is overloaded:

**CP CPU:** The percentage of CPU used for call processing in the last second. The "XX ..." is a graphical indication of the use.

**CPLoad:** The average of the percentage of CPU used for call processing in the last minute. The "XX ..." is a graphical indication of the use.

**TotCPU:** The percentage usage of CPU since start time. The default start time is when the system started. Use TotCPU when trying to measure how busy the system is over a period of time that is longer than 1 minute. Example usages are how much CPU is used when starting up, or how much CPU is used for an upgrade. Total values of less than 100% may indicate that the startup/upgrade times can be improved.

### Resource History Files

A history of the system's resource usage is stored in CSV files. These files are collected with system diagnostics and you can manually or automatically schedule the files for transfer from the controller using ftp.

#### **CPU history file**

CPU usage information is collected once per second. This data is written to the disk once every 15 seconds (bulk write of data to the disk). Writing the data this way reduces the number of disk accesses and the CPU overhead. A new file is created after 8 hours.

#### **SiloShow (MEM) history file**

SiloShow data is collected once every 2 minutes and added to the siloshow resource file. One file is created per day. Here is a partial example of the MEM file. It contains one of the system partitions and two process partitions, with two memory snapshots.

```
Time,Name,Free bytes, Alloc bytes,Fblocks,Ablocks, Avg Fblock, Avg Ablock, Max Fblock,
12/4/9 10:44:23, silo-nodes, 475048,53064, 1,1977, 475948,26,475048
12/4/9 10:44:23, PID 00 - kernel - private,0,0,0,0,0,0,0
12/4/9 10:44:23, PID 00 - kernel - public,81864,136592360,,15,1201,5457,28886,72680
12/4/9 10:44:23, PID 01 - appStartup - private,1304280,6228280,171,5430,7627,1147,1117936
12/4/9 10:44:23, PID 01 - appStartup - public,134896,0,1,0,134896,0,134896
12/4/9 10:54:23, silo-nodes, 475048,53064, 1,1977, 475948,26,475048
12/4/9 10:54:23, PID 00 - kernel - private,0,0,0,0,0,0,0
12/4/9 10:54:23, PID 00 - kernel - public,81864,136592360,,15,1201,5457,28886,72680
12/4/9 10:54:23, PID 01 - appStartup - private,1304280,6228280,171,5430,7627,1147,1117936
12/4/9 10:54:23, PID 01 - appStartup - public,134896,0,1,0,134896,0,134896
```

### **System resource history file**

Information such as free memory, cluster, DSP resources active is collected one every 60 seconds. Here is an example of a resource file (first 4 lines). This file includes memory use per silo.

```
Time, Memory, Clusters, DTMF Det, DTMF Gen ,
2012/04/09 10:54:00, 512,4000, 32, 32,
2012/04/09 10:54:00, 164,3800,1,1
2012/04/09 10:55:00, 164,3700,5,5
```

The second line in the example shows that data collection began on April 9th, 2012 at 10:54:00. At that time, the system had a total of 512M of memory available, 4000 clusters, 32 DTMF detectors, and 32 DTMF generators.

The 3rd row, at the same time, shows that 164M of memory is available, 3800 clusters are available, 1 DTMF detector and 1 DTMF generator is in use.

The fourth row shows that at 10:55, there was still 164M of memory available, the number of free clusters reduced from 100 to 3700, and the number of DTMF detectors and generators increased by 4 to 5.

## **Using Shell Commands when a system is busy**

### **MONITORING SYSTEM PERFORMANCE**

On the Linux shell, enter the following performance commands. To exit the utility, press <CTRL-C>.

#### **TDSTAT - SYSTEM RESOURCE STATISTICS**

The following dstat command gives a summary the system resources.

```
root@mxei11:~# dstat -tcdnD total 60
```

The output is shown below. The utility updates the last line with the average usage for the current minute. After a minute, a new line is created.

```

----system----  ----total-cpu-usage----  -dsk/total-  -net/total-
      time      |usr sys idl wai hiq siq| read  writ| recv  send
09-09 11:43:20|  7  4  87  2  0  0|4617B  19k|   0    0
09-09 11:44:20|  5  2  90  2  0  0|   0   14k|1137B  863B
09-09 11:45:20| 14 12  72  2  0  1|  59k 257k|2553B 4696B
09-09 11:46:09| 59 17  20  2  0  2|  26k 1104k|2655B   65k

```

- **System time** - The time of the 60 second sample.
- **total-cpu-usage** - The **idl** column is the percentage of time the CPU was idle. A system that is idle will have an CPU idle value around 90.
- **dsk/total** - The per second average amount of bytes read/written from/to the disk. An idle system on an average has 0 byte read and 14k bytes written.
- **net/total** - The per second average of bytes received/sent on the network interface.

## TOP - DISPLAY PROCESS STATS

The top command shows the top CPU usage of the processes that are running on the system.

A process contains one or many tasks.

To start the top utility, on the Linux shell, enter **top**. An example output of the top command for an MXe-III system is shown below.

```

Tasks:  96 total,    1 running,  95 sleeping,    0 stopped,    0 zombie
%Cpu(s):  5.2 us,  2.6 sy,   0.0 ni, 81.4 id, 10.5 wa,   0.0 hi,   0.3 si,   0.0 st
KiB Mem :  994232 total,   11184 free,   265820 used,   717228 buff/cache
KiB Swap:    0 total,    0 free,    0 used.  689076 avail Mem

   PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM    TIME+  COMMAND
  1024 voicead+  20   0 1367148 125764  62968 S   7.5 12.6 228:53.63 mcd
 29717 voicead+  20   0   3916    2320   1940 R   1.6  0.2   0:00.66 top
     7 root       20   0     0     0     0 S   0.3  0.0   1:34.96 rcu_preempt
   654 voicead+  20   0   31308   8160   3272 S   0.3  0.8   9:16.50 python
  1018 root       20   0  142456  13524   7444 S   0.3  1.4  16:47.04 python
  1023 voicead+  20   0  100456  45956  18724 S   0.3  4.6  32:37.16 call_control
  2739 voicead+  20   0  167788  69180  10476 S   0.3  7.0  27:23.33 JavaLayerVMJRE5
     1 root       20   0    6336   4356   3000 S   0.0  0.4   0:19.24 systemd

```

The first 4 lines gives the system resource usage. The stat 81.4 id is percentage of time the CPU is idle.

The rest of the rows show information for each process. Three columns are explained below:

- **% CPU** - The percentage of CPU the process is taking.
- **% MEM** - The percentage of memory the process is using.
- **COMMAND** - The name of a process.

A MiVoice Business system has two main processes:

- **Call control** - Call control controls the routing of calls.
- **mcd** - The mcd process runs the System Administration Tool and does the routing of voice packets.

## TOP – DISPLAY ALL THREAD STATS

The top utility can be changed to display threads instead of processes running on the system. To toggle between displaying processes versus threads, press capital **H**. The following is an example of top output showing the top CPU usage threads when an E2T call is up.

```
Threads: 818 total,   1 running, 816 sleeping,   0 stopped,   1 zombie
%Cpu(s):  8.3 us,   8.0 sy,   1.2 ni, 78.0 id,   4.5 wa,   0.0 hi,   0.0 si,   0.0 st
KiB Mem :  994232 total,   10712 free,   265436 used,   718084 buff/cache
KiB Swap:         0 total,         0 free,         0 used.  689464 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
29944	voicead+	20	0	4444	2884	1940	R	9.2	0.3	0:04.59	top
1761	voicead+	-61	-20	1367148	125792	62968	S	2.7	12.7	63:25.98	T2E_VPktFwd
1762	voicead+	-59	-20	1367148	125792	62968	S	1.5	12.7	23:38.51	E2T_VPktFwd
2692	voicead+	18	-2	1367148	125792	62968	S	0.9	12.7	33:50.70	STS
1792	voicead+	-53	-17	1367148	125792	62968	S	0.6	12.7	15:20.98	T38_DIM

## Phones

### Diagnosing Phone Problems

#### *No Dial Tone Analog Phone*

1. Log into the System Administration Tool and navigate to Maintenance Commands.
2. Establish the Location of the analog set using the Locate Extension maintenance command.
3. Run the State <extension> command. You will get one of the following responses: Idle, Busy, Manbusy, or Locked Out.

#### **If the response is Idle:**

- Connect a known good telephone set to the wiring frame.
- If the phone works then the problem is with the wiring from the frame to the set or it is the set.
- Disconnect the suspected set and connect a known good set into the terminal jack.
  - If the test set works then the faulty set should be replaced.
  - If the set does not work then the problem is in the wiring from the frame already tested or the jack.
- Check that the wiring in the jack is correct
  - If the wiring is incorrect then make the adjustment required and try the known good set again.
  - If the set still does not work then the problem is in the wiring.
- Check the wiring from the known good point at periodic intervals.

#### **If the Response is Busy:**

- Is the telephone engaged in a call?
  - If Yes then the phone is functioning normally.
  - If No then the phone is not functioning normally; take the following steps:
- Disconnect the wiring going towards the phone at the internal frame.

- Connect a known good telephone to the internal frame wiring and verify that there is dial tone.
  - If there is dial tone then there is a fault in the wiring.
  - If there is no dial tone then it could be the D-type connector (Amphenol) cable or a fault with the ASU. Verify the integrity of the Amphenol by changing it out.

**CAUTION:** If you change the Amphenol connector this will affect all users who are connected to that ASU.

If the Response is Manbusy:

- Find out why the circuit was busied out.
- Run the RTS <location id> command to return the circuit to service.

#### **If the Response is Locked Out:**

- Disconnect the wiring going towards the phone at the internal frame.
- Connect a known good telephone to the internal frame wiring that connects to the Analog Service unit or peripheral cabinet and verify if there is dial tone.
- If there is dial tone, then there is a fault in the wiring. If there is no dial tone:
  - For an analog phone it could be the D-type connector (Amphenol) cable or a fault with the ASU. Verify the integrity of the Amphenol by changing it out.
  - For a DNI phone, it could be a fault with the DNI card.

**CAUTION:** If you change the Amphenol connector on an ASU it will affect all users who are connected to that ASU.

#### **No Dial Tone IP Phone**

1. Log into the System Administration Tool and navigate to Maintenance Commands.
2. Establish the Location of the analog set using the Locate Extension maintenance command. If Locate Extension command does not work verify the programming in the IP Set Assignment and Multiline Set Key Assignment.
3. Run the State <extension> command. You will get one of the following responses: Idle, Busy, Manbusy, or Out of Service.

#### **If the response is Idle**

- Reset the telephone.

#### **If the response is Busy:**

- Is the telephone engaged in a call?
  - If it is wait for the call to finish and check again for dial tone.
  - If the telephone is not on a call try resetting the handset.

#### **If the response is Manbusy**

- Find out why it is Manbusy.
- Return to Service using the RTS <location ID> command.

#### **If the response is Out of Service:**

- Check the phone has power (does it have a display).
  - If the phone does not have power then connect to an appropriate power source.
  - If the phone does have power then verify the link integrity LEDs.
  - A green LED on the bottom of the phone indicates a proper connection.
  - A flashing yellow LED indicates activity (data flow) on the network.

## Viewing Settings and Network Parameters on IP Phones

Use the Configuration (Debug) Menu on IP Phones to view the settings and network parameters on an IP Phone. The procedures to access the configuration menu on Single Mode IP Phones and Dual Mode IP Phones are different. You can identify a Dual Mode phone by checking the label at the back of the phone. The label will specify the phone as “Dual”.

**NOTE:** The default setting from the factory is MiNet mode. The procedures described here are based on MiNet mode. The phone menus may vary in SIP mode.

**NOTE:** The Configuration Menu is not available on systems that have MLPP option selected.

### Access Configuration Menu on Single Mode IP Phones

1. Hold down both volume keys at the same time.
2. Enter **debug** (33284) on the telephone key pad (handset on hook).
3. Press **Superkey** to the display categories.
4. View details for the following categories. Press the Up/Down volume keys, or softkeys (if available) to navigate the options.
  - **Version info** (Main and Boot loads)
  - **Network** (IP information, such as the telephone’s IP Address, Subnet Mask, ICP List, DHCP Server Address, TFTP Server Address, Gateway IP (Router) VLAN/Priority, DSCP)
  - **Telephony/DSP** (Telephone Directory Number and other design information)
  - **Connection** (Link Reset; Hard Reset; Toggle ERROR persistence; CDP Support; Port Settings; Static Settings)
  - **Browser Config** (Proxy Server Configuration, Debug Stream On/Off, etc.)
  - **Memory Stats** (Various design memory details)
5. Press **Phone View** or **Cancel** to exit the configuration menu.

### Access Configuration Menu on Dual Mode Phones

Use the following procedures to configuration Dual Mode IP Phones, MiNet/SIP phones, and where specified, the 5560 IPT.

On the 5215 IP Phone (Dual Mode), press \*(yes), **0** (default), and **#** (no). On the 5220 IP Phone (Dual Mode), 5224 IP Phone, 5320 IP Phone, 5330 IP Phone, 5340 IP Phone, 5360 IP Phone, and Navigator press the three softkeys to select menu items.

**Method A:** To access the menu during the phone boot sequence:

- Hold down both volume keys until NETWORK PARAMETERS? appears.

**Method A (5560 IPT):** To access the menu during the phone boot sequence:

- While powering up, hold down the Left or Right key to go into configuration mode on that side.

**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. Dial 234 on the telephone key pad and then release the down key.

- NETWORK PARAMETERS? appears.
- 4. Proceed to [Viewing/Modifying Network Parameters](#), [Configuring Hardware Components](#), [Setting the Phone Mode](#), or [Using Tools and Features](#).

**Method B (5560 IPT):** If the phone is already up and running in dual handset mode:

1. Press and hold the Left or Right key and the Volume Up and Down down keys.
2. Release one of the volume keys, and press **234** (CFG) on the selected side.

To enter the Configuration menu on the right side while in single handset mode:

1. Press the hot prime key on the right side.
2. Hold down the Volume Up and Down keys

**Method C:** Using Hotkeys, at power up, press and hold the following key combinations. Note that Hotkeys access provides limited access. Methods A and B provide full access.

**NOTE:** This method is also supported on the 5560 IPT.

**Table 10.2:**Accessing the Configuration Menu: Option C

Key Sequence	Function
* and 6 (M)	Change mode to MiNet
* and 7 (S)	Change mode to SIP (Not supported on the 5560 IPT.)
7	Jump to “Config Teleworker” menu
*	Erase the PIN and VCON configuration
any other keypad keys	Display “Configure Phone” prompt

## Viewing/Modifying Network Parameters

You can view and modify the following network parameters on the phone:

- Phone IP address (current and static)
- Gateway IP address (current and static)
- Subnet mask (current and static)
- Current controller IP address
- TUG1, TUG2, TUG3, and TUG4 IP addresses (current)
- TFTP server IP address (current)
- VLAN ID and priority (current and static)
- DSCP value
- IPA IP address (current and static)
- TUG IP address (static)
- TFTP SVC IP and port (static).



**To view and modify network parameters:**

1. Access the Configuration Menu (see [Access Configuration Menu on Single Mode IP Phones](#)).
2. At NETWORK PARAMETERS?, press **Yes** . VIEW CURRENT VALUES? appears.
3. Do one of the following:
  - Press **Yes** , and then press the Up/Down volume keys to view each setting. When you return to VIEW CURRENT VALUES?, press **No** . VIEW STATIC VALUES? appears.
  - Press **No** . VIEW STATIC VALUES? appears.
4. Do one of the following:
  - Press **Yes** , and then press the Up/Down volume keys to view each setting. When you return to VIEW STATIC VALUES?, press **No** . MODIFY STATIC VALUES? appears.
  - Press **No** . MODIFY STATIC VALUES? appears.
5. Do one of the following and then reboot the phone:
  - Press **Yes** , and then press the Up/Down volume keys to scroll through each setting. Use the keypad to modify parameter(s), and then follow the prompts to store the changes and reboot the phone.
  - To reset the factory defaults, press **Default** , and then follow the prompts to set and store the factory defaults and reboot the phone.
6. To exit the current menu without a reboot:
  - To return to the main menu, press **Yes** at EXIT MENU?
  - To return to the default display, press **Superkey** . (On the 5560 IPT, press **Cancel** or **#** to reach the exit menu and then follow the display prompts.)

## Configuring Hardware Components

You can configure the speed and duplex mode of the LAN and PC ports.

**NOTE:** Speed and duplex mode are not configurable on the 5560 IPT.

**To manually configure speed and duplex mode:**

1. Access the Configuration Menu (see [Access Configuration Menu on Single Mode IP Phones](#)).
2. Press **No** until HARDWARE CONFIG? appears, and then press **Yes** . MODIFY SETTINGS? appears.
3. Do one of the following and then reboot the phone:
  - To modify the current hardware components, press **Yes** , and then follow the prompts to modify each setting and store the changes.
  - To reset the factory defaults, press **Default** , and then follow the prompts to set and store the factory defaults.
4. To exit the current menu without a reboot:
  - To return to the main menu, press **Yes** at EXIT MENU?
  - To return to the default display, press **Superkey** .



## Setting the Phone Mode

You can program the 5215 or 5220 IP Phone (Dual Mode) to use MiNET or to work remotely using either SIP or Teleworker Solution (6010).

For SIP configuration information, refer to the 5207/5215/5220 IP Phone Installation Guide (56006499, Rev A) packaged with the phone, and to the 5215/5220 IP Phone SIP User Guide available at [www.mitel.com](http://www.mitel.com).

## Using Tools and Features

- [Erasing the Registration PIN](#)
- [Pinging IP Addresses](#)
- [Conducting a DHCP Trace](#)
- [Configuring Video Conferencing Parameters](#)
- [Restoring Factory Default Settings](#).

### **Erasing the Registration PIN**

1. Access the Configuration Menu (see [Access Configuration Menu on Single Mode IP Phones](#)).
2. Press **No** until TOOLS AND FEATURES? appears, and then press **Yes** . ERASE PIN? appears.
3. Press **Yes** , and then follow the prompts to erase the PIN and to store the changes and reboot the phone.
4. To exit the current menu without a reboot:
  - To return to the main menu, press **Yes** at EXIT MENU?
  - To return to the default display, press **Superkey** .

### **Pinging IP Addresses**

1. Access the Configuration Menu during the phone boot sequence.
2. Press **No** until TOOLS AND FEATURES? appears.
3. Press **Yes** , and then press **No** until PING TEST? appears.
4. Press **Yes** and then follow the prompts to conduct the PING test.
5. To exit, do one of the following:
  - To return to the main menu, press **Yes** at EXIT MENU?.
  - To return to the default display, press **Superkey** .

### **Conducting a DHCP Trace**

There is a delay while the phone performs DHCP discovery. The result of the trace displays the following information:

- Phone and Gateway IP addresses
- Subnet mask
- WINS, DNS, TFTP, ICP and Video servers
- DHCP server and Mitel IDs
- Lease
- T1 and T2

- VLAN ID and priority
- HTTP proxy
- IPA address.

**To conduct a DHCP trace on the Dual Mode phone:**

1. Access the Configuration Menu (see [Access Configuration Menu on Single Mode IP Phones](#)).
2. Press **No** until TOOLS AND FEATURES? appears.
3. Press **Yes** , and then press **No** until DHCP Trace? appears.
4. Press **Yes** , and press the Up/Down volume keys to view the results of the DHCP trace.
5. To exit, do one of the following:
  - When you return to DHCP TRACE?, press **No** .
  - To return to the default display, press **Superkey**.

**Configuring Video Conferencing Parameters****To configure video conferencing on the 5220 IP Phone (Dual Boot):**

1. Access the Configuration Menu (see [Access Configuration Menu on Single Mode IP Phones](#)).
2. Press **No** until TOOLS AND FEATURES? appears.
3. Press **Yes** and then press **No** until VIDEO CONFIGURATION? appears.
4. Press **Yes** . VIEW PARAMETERS? appears.
5. Do one of the following:
  - Press **Yes** and then follow the prompts. When you return to VIEW PARAMETERS?, press **No** . MODIFY PARAMETERS appears.
  - To continue, press **No** . MODIFY PARAMETERS appears.
6. Do one of the following:
  - Press **Yes** and follow the prompts to modify the video conferencing parameters, store the changes, and reboot the phone.
  - To set the factory default settings, press Default and follow the prompts to set and store the factory defaults and reboot the phone.
7. To exit the current menu without a reboot:
  - To return to the main menu, press **Yes** at EXIT MENU?
  - To return to the default display, press **Superkey** .

**Restoring Factory Default Settings**

**TIP:** Restoring the factory default settings on the 5215 or 5220 IP Phone (Dual Mode) will erase the static network parameters.

1. Access the Configuration Menu (see [Access Configuration Menu on Single Mode IP Phones](#)).
2. Press **No** until TOOLS AND FEATURES? appears.
3. Press **Yes** and then press **No** until RESTORE DEFAULTS? appears.
4. Press **Yes** and then follow the prompts to set and store the factory defaults and reboot the phone.
5. To exit the current menu without a reboot:

- To return to the main menu, press **Yes** at EXIT MENU?
- To return to the default display, press **Superkey** .

## IEEE 802.1X Authentication for IP Phones

The 5215 Dual Mode, 5220 Dual Mode, 5304, 5312 and 5324 IP Phones support IEEE 802.1X Extensible Authentication Protocol (EAP) -Message Digest 5 (MD5) Challenge authentication protocol. Refer to the 3300 ICP Engineering Guidelines for more information about this protocol.

If the network switches and their ports support 802.1.x authorization, the Remote Authentication Dial-In User Service (RADIUS) server checks the username and password of the IP phones against the entries in the database:

- If the username and password of the IP phone match the username and password on the RADIUS server, the IP phone is granted access to the port services. The IP phone boots up.
- If the username and password don't match, the IP phone is denied port access. The IP phone does not boot up.
- If a username and password are not configured for the IP phone, you are prompted to enter them.

### Configuring an Authentication Username and Password

1. Power up or reboot the 5215 Dual Mode, or 5220 Dual Mode.
2. Wait for the prompt: PORT ACCESS CONTROL PRESS # TO CONTINUE.
3. Press **#** .
4. Enter a username of up to 20 characters in length. This username must match a name that is programmed on the RADIUS server. Use the phone keys in the table below to enter the characters:

**Table 10.3:** DTMF Keys for entering Alphanumeric Characters (Sheet 1 of 2)

DTMF Key	Alphanumeric Characters (in order)
1	,&\$!/?%'"-_1
2	abc2
3	def3
4	ghi4
5	jkl5
6	mno6
7	pqrs7
8	tuv8
9	wxyz9
*	Backup and edit previous char

**Table 10.3:** DTMF Keys for entering Alphanumeric Characters (Continued) (Sheet 2 of 2)

DTMF Key	Alphanumeric Characters (in order)
0	./:@0
#	Commit entered data

By default, the user name and password are entered in upper case letters. However, you can use both upper and lower case. To change to lower case, press the Volume Down key while entering a letter. All subsequent letters will be in lower case. To return to upper case, press the Volume Up key while entering a letter.

5. Press **#** to commit the username.
6. Enter a password from 1 to 20 alphanumeric characters in length. This password must match the password that you have programmed on the RADIUS server for the user.
7. Press **#** to commit the password. The message, "Waiting for 802.1X authentication" appears in the phone display. After the server authenticates the username and password, the IP phone boots up.

## Erasing an Authentication Username and Password

1. Access the configuration menu on the 5215 Dual Mode, or 5220 Dual Mode IP Phone. See [Access Configuration Menu on Single Mode IP Phones](#).
2. From NETWORK PARAMETERS? press **No** until on the telephone keypad until TOOLS AND FEATURES? appears.
3. Press **Yes**.
4. Press **No** until EDIT 8021X SETTINGS appears.
5. Press **Yes** ERASE 8021X DATA? appears in the display.
6. Press **Yes** to erase the current username and password.
7. Press **Yes**. The phone erases the data from its flash and then reboots.

**NOTE:** The IP phone username and password that you configured for EAP-MD5 Challenge Authentication do not need to be reprogrammed if power to the phone is lost.

## Enabling or Disabling 802 1X Authentication

By default, EAP- MD5 Challenge Authentication Protocol is enabled on 5215 Dual Mode, and 5220 Dual Mode IP Phones. If your network does not use this protocol, you do need to disable support for it on these phones.

1. Access the configuration menu. See [Access Configuration Menu on Single Mode IP Phones](#).
2. From NETWORK PARAMETERS? press **No** until on the telephone keypad until TOOLS AND FEATURES? appears.
3. Press **Yes**.
4. Press **No** until EDIT 8021X SETTINGS appears.

5. Press **Yes**. ERASE 8021X DATA? appears in the display.
6. Press **No**. If currently enabled, you are prompted to disable 8021X. If currently disabled, you are prompted to enable 8021X.
7. Press **Yes**.
8. Press **Yes**. The phone erases the data from its flash and then reboots.

## IP Phone Boot Sequence

After you connect an IP Phone to the network, it goes through the following boot sequence (this applies to Release 5.0 and later):

**TIP:** MAC Addresses, and Main and Boot versions in the following table are examples for illustration purposes. The numbers displayed at the install site may be different. The x's are IP Address, VLAN, and Priority place holders.

**Table 10.4:** IP Phone Boot Sequence (Sheet 1 of 3)

Boot Sequence	Phone Display
1) Waiting for an Ethernet link to be established.	Waiting for LAN link to come up
1) If an Ethernet link is not established, continue with the bootup process.	Bad LAN link Check Ethernet cable
2) The first stage for bootup. <b>NOTE:</b> Refer to for 802.1x Port Access Control messages.	08-00-0F-AA-BB-CC Booting: 04.02.01.06
3) IP Phone contacts DHCP server to obtain IP address and VLAN information and a list of the controller addresses in the network. <b>NOTE:</b> Go to if DHCP or TFTP fails.	Waiting for DHCP Booting: 04.02.01.06 ----- DHCP: Discovery Booting: 04.02.01.06
4) The internal DHCP server provides one of these options: An external DHCP server provides one of these options: (where n is the number of the sub-option if encapsulation is used for the option.)	Using option 125 Using option 43 Using option 128+ ----- Using option 125:n Using option 43:n
5) The DHCP server on the default VLAN responds with an Offer. If Option 43 or 125 (or option 130 prior to 3300 Release 7.0) is not properly set on the server, the set awaits further Offers (n is offer number).	DHCP: Offer n Rej Booting: 04.02.01.06 ----- DHCP: Offer n Acc Booting: 04.02.01.06
6) The set replies with a Request and the server replies with an Acknowledgement.	DHCP: Ack Booting: 04.02.01.06

**Table 10.4:** IP Phone Boot Sequence (Continued) (Sheet 2 of 3)

Boot Sequence	Phone Display
<b>7)</b> If the data in the Ack does not contain a VLAN ID and a packet Priority value, the set retains DHCP data, jumps to <i>Step 10</i> .	
<b>8)</b> If the data included in the Ack does include a VLAN ID and packet Priority value, the set discards DHCP data and sends an untagged Release.	DHCP: Releasing Booting: 04.02.01.06 ----- Vlan x Priority x Booting: 04.02.01.06
<b>9)</b> The set goes through the Discovery/Offer/ Request/Ack sequence again. The packets sent are tagged to include VLAN and Priority values supplied by the first DHCP server.	
<b>10)</b> The TFTP server downloads the boot image and displays the set IP address. If there is no boot image, the set jumps to <i>Step 12</i> . Refer to <a href="#">Download and Software Error Displays</a> for a description of possible error messages.	xx.xx.xx.xx Downloading
<b>11)</b> The boot file is copied to flash if it is a different version than the one in flash.	Upgrading Flash DO NOT POWER DOWN
<b>12)</b> If the boot load is the same as in flash, it is not copied.	xx.xx.xx.xx Upgrade not required
<b>13)</b> The set downloads a main image. A failure causes a phone reset, and the process starts again at step 1.	xx.xx.xx.xx Download failed ----- xx.xx.xx.xx Downloading ----- xx.xx.xx.xx Starting main
<b>14)</b> The set resets and the main load executes. The display changes to waiting for link. The set requests registration with the ICP (the first time request requires a PIN registration). The set waits for the ICP to take control.	MAIN 08.04.01.01 BOOT 04.02.01.06 ----- Set xx.xx.xx.xx ICP xx.xx.xx.xx ----- Waiting for ACK... ICP xx.xx.xx.xx ----- Waiting for COMMS... ICP xx.xx.xx.xx

**Table 10.4:** IP Phone Boot Sequence (Continued) (Sheet 3 of 3)

Boot Sequence	Phone Display
<b>15)</b> After the main boot load is downloaded, (and only when a phone in a resilient network has homed to the wrong ICP) the phone seeks out the IP address of its primary 3300 ICP from the DHCP ICP Redirect list of 3300 ICPs in the network. It is possible for the phone to be redirected and you may see this display again.	Set xx.xx.xx.xx ICP xx.xx.xx.xx  -----  Set xx.xx.xx.xx ICP xx.xx.xx.xx
<b>16)</b> Once communication is established, the idle display appears on the set.	<idle in service UI> <idle softkeys>

**Table 10.5:** IP Phone Port Access Control Sequence

Sequence	Phone Display
<b>1)</b> Checking the L2 switch for 802.1x Port Access Control.	Waiting for 802.1x authentication
<b>2)</b> With access control, the L2 switch will ask for user and password (unless the data is stored in NVRAM).	PORT ACCESS CONTROL PRESS # TO CONTINUE ----- USER (# to end) — ----- PASSWORD (# to end) —
<b>3)</b> If Port Access Control fails.	Port Access Failure REBOOTING. . . ----- Waiting for 802.1x authentication
<b>4)</b> If the data exchange succeeds or if the L2 switch does not support 802.1x Port Access Control.	Waiting for LLDP

**Table 10.6:** IP Phone Error Handling Displays (Sheet 1 of 2)

Message Description	Phone Display
<b>NOTE:</b> Check the IP Parameters (TFTP address, netmask, gateway address), to make sure that they are valid, before calling Mitel.	

**Table 10.6:** IP Phone Error Handling Displays (Continued) (Sheet 2 of 2)

Message Description	Phone Display
If TFTP fails, usually due to incorrect TFTP Server or Gateway IP address, review IP parameters and correct errors.	RTCS creat err <number> BOOTING xx.xx.xx.xx ----- If add err <number> BOOTING xx.xx.xx.x ----- RTCS Bind err <number> BOOTING xx.xx.xx.x
The TFTP server sent an “I am busy” error so the phone will delay and retry.	xx.xx.xx.xx Waiting for TFTP
If the phone received a bad packet from the TFTP server, audit the TFTP server configuration and the network path.	xx.xx.xx.xx TFTP Err: <number>
This error indicates that you must review the IP parameters on the DHCP server or manually entered for the phone.	xx.xx.xx.xx TFTPerr: Packet send
Internal TFTP errors - contact Mitel Technical Support.	xx.xx.xx.xx TFTPerr: Sock create ----- xx.xx.xx.xx TFTPerr: Sock bind ----- xx.xx.xx.xx TFTPerr: Packet alloc

**Table 10.7:** Download and Software Error Displays (Sheet 1 of 2)

Message Description	Phone Display
<b>NOTE:</b> Check the IP Parameters (TFTP address, netmask, gateway address), to make sure that they are valid, before calling Mitel.	
These errors indicate that the Flash was not upgraded. The phone will pause for 3 seconds and continue.	L2 download err ----- Boot download err ----- L2&Boot download err
The ICP instructs the phone to get a new main executable. Two-line display set: Single-line display set:	TFTP MAIN FROM xx.xx.xx.xx ----- TFTP MAINLOAD



**Table 10.7:** Download and Software Error Displays (Continued) (Sheet 2 of 2)

Message Description	Phone Display
If the phone received a bad packet from the TFTP server, audit the TFTP server configuration and the network path.	xx.xx.xx.xx TFTP Err: <number>
This error indicates that you must review the IP parameters on the DHCP server or manually entered for the phone.	xx.xx.xx.xx TFTPerr: Packet send
Internal TFTP errors - contact Mitel Technical Support.	xx.xx.xx.xx TFTPerr: Sock create ----- xx.xx.xx.xx TFTPerr: Sock bind ----- xx.xx.xx.xx TFTPerr: Packet alloc
TFTP IP address is missing from the configuration string.	125:TFTP tag missing OR 43:TFTP tag missing
ICP IP address is missing from the configuration string.	125:ICP tag missing OR 43:ICP tag missing
Encapsulation is incorrect.	Bad 125 subopt end OR Bad 43 subopt end

## Checking the IP Phone Resiliency Progress Display





A progress bar, consisting of flashing rectangles, is displayed in the upper right corner of the IP Phone display whenever a phone is trying to re-home (except on boot-up) to any ICP controller. The set will display a progress bar if a resilient IP phone re-homes as a result of a Hot Desk login.

Three rectangles indicate the progress of the activity:

- Left block flashing - waiting for TCP link connection with ICP
- Left block solid and middle block flashing - waiting for registration message acknowledgment from ICP
- Left and middle blocks solid, right block flashing - waiting for MiNET communications with the ICP that will take over the display at this point.

When the three rectangles are solid, the activity is complete. If the IP Phone does not complete the activity after several minutes, check the progress status by pressing the \* key on the dial pad.

**Table 10.8:** IP Phone Resiliency Progress Display

Re-home Sequence	Resilient Phone Display
Resilient waiting for link UI (first block flashing) 	<idle ui line1> <idle ui line2>
Resilient waiting for ACK UI (second block flashing) 	<idle ui line1> <idle ui line2>
Resilient waiting for COMMS UI (third block flashing) 	<idle ui line1> <idle ui line2>
Phone connected to secondary ICP (solid block) 	<idle ui line1> <idle ui line2>

## Diagnosing SIP Device Issues

Use the following procedure to diagnose issues with SIP line side devices that are connected to the 3300 ICP system:

- Identify the symptoms:
  - No dial tone at SIP device?
  - Choppy or one-way audio?
  - From an internal display phone what does an internal caller see on display and hear when calling the SIP endpoint?
  - Can you ping the end point unit and the default gateway, proxies from the controller subnet?
  - TLS set takes a long time to come into service following a system reboot (Check the Registration Timer value on the set and if possible, lower the value to 5 minutes.)
- What are the SIP end points devices?
- What is the software revision of the devices?
- What is the extension of the device having the issue?
- Gather the following Information Logs (all information is required to properly diagnose issue)
  - Start trace on MiVoice Business using the maintenance command `SIP TCPDUMP ALL` (on busy switches, use the option `SIP TCPDUMP CCN xxxx`, where `xxxx` is the extension of the device).
  - Reproduce issue
  - Stop trace on MiVoice Business using the maintenance command `SIP TCPDUMP OFF`.
  - System Diagnostics Logs (this includes the tracing above and information about the system).
  - If the problem is related to audio, capture the media near the device or at a firewall/SBC it is passing through.
  - Screen captures of the endpoint configuration information.
  - List of relative IP addresses such as MiVoice Business, end points, outbound proxies, and so forth.

6. For registration issues, enter the following SIP Maintenance Commands and collect the response (see the online help on the Maintenance Commands in the System Administration Tool):
  - SIP REGISTRAR CONTACTS ALL
  - SIP REGISTRAR CONFIG
  - SIP REGISTRAR STATS
7. For Message Waiting Indication issues, collect the data from the following commands:
  - SIP REGISTRAR CONFIG
  - SIP REGISTRAR STATS
  - SIP REGISTRAR CONTACTS <USER\_NAME> (DN or ext)
  - SIP MWI STATS
  - SIP MWI SUBSCRIBER INFO <CONTACT\_NAME>

## Dialing from Aastra SIP DECT handsets

On Aastra SIP-DECT handsets, such as 612d and 622d, the \* and # keys can act as texting keys, bringing up additional menus with options, instead of dialing the \* or # digit. To ensure that these digits are dialed properly, use the following procedure to configure the dial editor to allow only digits: 0-9, \*, and #.

1. Access the Open Mobility Manager (OMP) Portal application (OMP.jar)
2. Select **System -> System settings -> Portable parts** tab
3. Click the **Dial editor supports digits only** check box to enable the parameter.
4. Click **OK**

## Trunks

### Diagnosing Digital Trunk Issues

The following table lists key maintenance commands that you can use to diagnose issues with digital trunks. Note that the following table does not provide a comprehensive listing of all problems, but it does cover the most commonly encountered problems.

**Table 10.9:** Maintenance commands for diagnosing digital trunk issues (Sheet 1 of 3)

Symptom	Commands	Description
Any problem	edt show link config all edt show framer config all edt show link info edt show vdsu table	These commands output generic configuration information about the embedded digital trunks. From the output of these commands, you can tell how the trunks are configured. Use these commands to quickly identify any differences between the perceived and actual configuration of the trunks.

**Table 10.9:** Maintenance commands for diagnosing digital trunk issues (Continued) (Sheet 2 of 3)

Symptom	Commands	Description
Link alarms - Part 1 (System unable to seize trunks or trunks are unavailable, network synchronization issues, and so forth)	edt show framer stats all edt show framer regs all	Outputs the statistical registers of the framers and the register settings. The outputs show exact the physical issue that is affecting the framer. You may have to dump the “framer stats” more than once as these registers change over time. Collect this output in association with the output from the “dtstats read”, “net state” and “show faults digital links” maintenance commands. <b>NOTE:</b> The output from these commands must be interpreted by Mitel Software Design.
Link alarms - Part 2 (Trunks not in idle when there are no calls up)	edt show vdsu alarms <plid>  edt show vdsu channel <plid>	Shows the current digital trunking alarms and channel status. Use this command in conjunction with “dtstats read” and “state” commands. <b>NOTE:</b> The output from these commands may need to be interpreted by Mitel Software Design.
Outgoing or incoming calls rejected	edt trace vdsu namnum	Outputs the calling/called number and calling name of the call. It also displays the reason an ISDN call was disconnected (may be different than what is displayed on a set). Use this command to verify that the ARS is setup correctly and that the correct number of digits are being sent or received.
Call problems (dropped calls, calls getting rejected, set displays not correct, and so forth)	edt trace tsp l2l3 <plid> OR edt trace tsp cc <plid> OR edt trace vdsu cp <plid> edt trace vdsu vb <plid>	For most ISDN/QSIG problems, the “l2l3” command will be adequate. It is recommended that you turn on the “ccs” trace at the same time. For problems involving eT1D4, use the “tsp cc” command. This displays the messages to and from the T1D4 stack. If the problem is not protocol related, turn on the “cp/vb” tracing. <b>NOTE:</b> The output from these commands may need to be interpreted by Mitel Software Design.

**Table 10.9:** Maintenance commands for diagnosing digital trunk issues (Continued) (Sheet 3 of 3)

Symptom	Commands	Description
Call problems are generating message output that you need to capture in a file for interpretation	edt enable logtofile (turns on message tracing) edt disable logtofile (turns off message tracing)	This command puts all of the traces turned on by “edt trace ...” into the “/db/LDS_Trace.rtf” file (DigTrkTrace prior to 3300 RIs 6.1). If you need to enable tracing on a busy switch, you should send the output to the trace file because the output to the response window is slow and can impact the performance of the 3300 ICP This log file must be interpreted by Mitel designers. It is not meant to be interpreted by customers or field technicians.
T1/E1 module (embedded PRI) issues	All ESM digital trunk maintenance commands available to the NSU apply to the T1/E1 module and can be entered through the Maintenance commands form of the System Administration Tool.	Refer to Mitel Knowledge Base article 04-5191-00014

## Hardware

### Using LEDs to Diagnose Faults

Controllers, units, modules and cards have light-emitting diodes (LEDs) that indicate their current status. Refer to the Technician's Handbook for tables that list the LED states and the meaning of each state.

### Reading E2T Card Statistics

When troubleshooting network issues, you can use the `e2tshow` command to read statistics for E2T (only applies to MXe-III/MXe III-L) cards.

1. Login into Linux shell of the RTC.
2. Enter command `e2tCardConsoleStart`
3. Press enter to cause login prompt to appear.
4. Login.
5. Start E2T `mcdDebug` by entering `/sysro/bin/mcdDebug`
6. Enter **e2tshow**.

**NOTE:** E2T statistics accumulate over time and do not clear until the system is reset or the `e2tclear` command is entered. Reading the data without knowing when collection was started may be misleading. We recommend that you clear the statistics first (using `e2tclear`) to set a reference mark and then monitor it at regular intervals.

7. Check the output. When reading the output of `e2tshow`, a large quantity of errors in the following categories indicates a network issue:
  - RTP Seq total missing pkts
  - RTP Seq Packets out of order
  - RTP Seq Pkts duplicate SEQ
  - Jitter Underflow
  - Jitter Overflow

The figure below shows a sample result of the `e2tshow` command:

232

**Figure 10.1:** Example Result of e2tShow command

## Diagnosing DSP Module Related Issues

Refer to Mitel Knowledge Base article 05-5107-00004 for information on how to diagnose DSP module issues.

Use the following maintenance commands to obtain information concerning DSPs:

- DUMPDSPBOOTINFO - to display DSP resource allocation on the system.
- SHOWDSPSTATUS - to display the current status of all detected DSP MMCs on the system.

## Diagnosing MSDN DPNSS Link Problems

If there is a problem with the MSDN/DPNSS link:

Establish whether all calls are affected.

- If all calls are affected check the status of the link by using the DTSTAT READ PLID command.
- If the link is unavailable check the cabling. Test with a back to back cable to prove the DS1 or CEPT card.
- If the link is available check the errors.
- If some calls fail check the following:
  - ARS programming
  - Digit Conflict
  - Interconnect Restriction
  - Far end fault/programming
- If only calls to the central office fail check that the Class Of Service option of Public Network Access via DPNSS is enabled on the extension making the call and the MSDN trunks.

## Loopback Testing on Digital Trunks

You can perform a loopback test on digital trunks to rule out problems with the system hardware. If two trunks can be successfully looped, and calls made that contain no slips, BERs, or framing losses, the system is operating properly. The loopback test requires the use of two trunks.

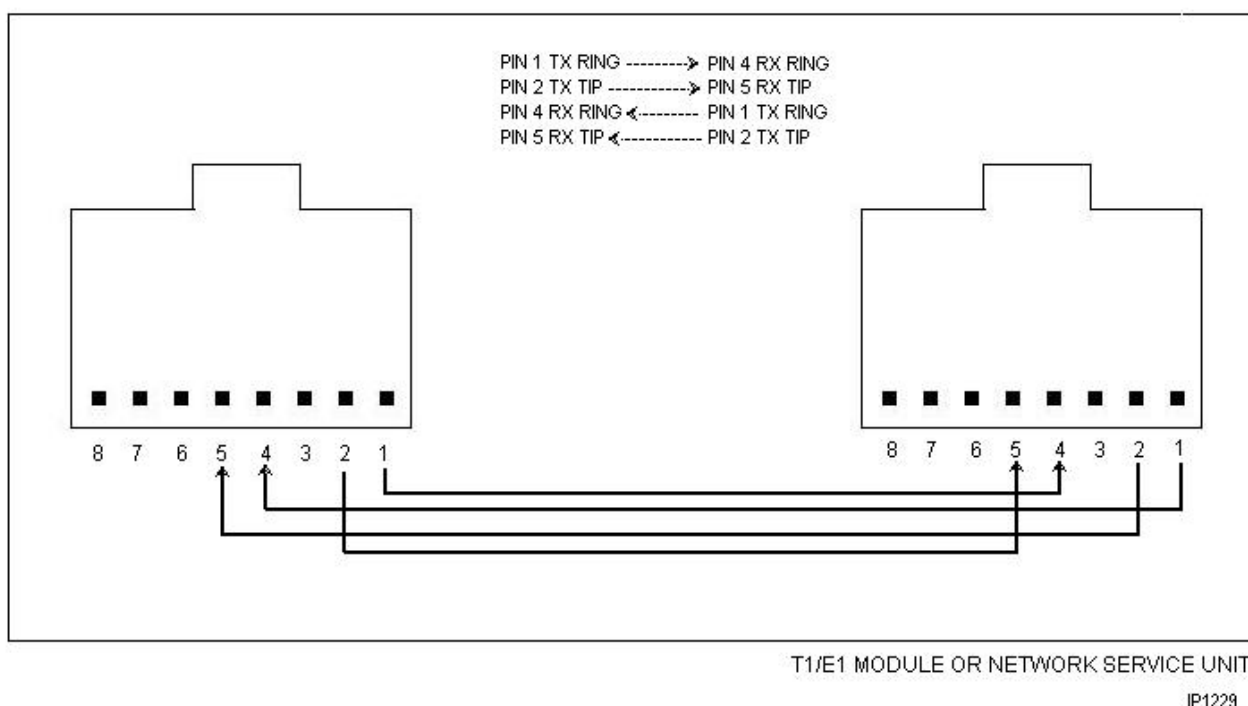
To perform loopback testing:

1. Assign a digital link descriptor to each hybrid (see the Digital Link Descriptors form).
2. Ensure the trunks are the same type. If MSDN will be used, ensure one hybrid is set to A, and the other is set to B.
3. Configure a valid Trunk Descriptor (see the appropriate CO Trunk Circuit Descriptors form).
4. Configure a valid Trunk Service Assignment (see the Trunk Attributes form), and set the Absorb field to "0".
5. Include the trunks in two separate Trunk Groups and routes (see the Trunk Groups and the ARS Routes forms).



6. Complete ARS programming, using unique leading digits and a valid number of digits to follow (extension number length). You should be able to make a call from each Trunk Group back into the switch to a valid extension.
7. Program the Number of Digits to Absorb field, of the ARS Digit Modification Plans form, to strip away the leading digits.
8. To connect loopback between trunks on a T1/E1 Module, you have two options:
  - **Option 1** : Set one trunk in Network Termination (NT) Mode and the other trunk in Line Termination (LT) Mode. You set the line termination mode in the Link Descriptor Assignment forms of the trunks. Then, connect the trunks with a straight-through CAT5 cable.
  - **Option 2** : If you want to have both trunks in the same mode, you must wire the T1/E1 trunk connectors together as shown in [Figure 10.2](#).
9. Complete calls to confirm there are no errors with the system equipment.

BOTH TRUNKS IN NETWORK TERMINATION (NT) MODE  
OR  
BOTH TRUNKS IN LINE TERMINATION (LT) MODE



**Figure 10.2:** Loopback - T1/E1 Connectors (RJ45) on T1/E1 Module

## Resiliency

### Locating Resilient Devices

Use the following three Locate commands to obtain information for resilient devices.

- Locate Extension
- Locate Feature
- Locate Remote

## Locate Extension

You issue the Locate Extension command to acquire information about the 3300 ICP of a resilient or non-resilient extension. For resilient devices, the output of the command

- Provides primary and secondary ICP cluster element index numbers and routing digits
- Identifies the ICP the locate command was issued on ("LEID")
- Indicates the location of the resilient device by placing an asterisk (\*) beside the primary or secondary ICP that the device is in service on

**NOTE:** To determine the state (in service, out of service, idle, busy, and so on) of the device on a given ICP, you must issue the State Extension command. For an overview of this command, see [State Extension](#), and for more detailed information, refer to the *3300 ICP General Information Guide and 3300 ICP System Administration Tool Online Help*.

The table below provides the input and different possible outputs for the Locate Extension command.

**Table 10.10:** Locate Extension Information for Resilient and Non-resilient Devices (Sheet 1 of 2)

Input	Output	Meaning
locate extension 1001	IP Device ID: 3 Circuit Location: 1 3 1 3 1 Extension: 1001 MAC Address: 08:00:0F:01:26:5D  Primary Element: LEID 101 - Routing Digits: 2901 Secondary Element: CEID 102 - Routing Digits: 2902 *	Resilient device located on secondary ICP. Command was issued on primary ICP. LEID is the Local Element Identifier. CEID is the Cluster Element Identifier. * Indicates the known location of the device. LEID identifies the ICP that you issued the command from.

**Table 10.10:** Locate Extension Information for Resilient and Non-resilient Devices (Continued) (Sheet 2)

Input	Output	Meaning
	IP Device ID: 3 Circuit Location: 1 3 1 3 3 Extension: 1001 MAC Address: 08:00:0F:01:26:5D  Primary Element: CEID 101 - Routing Digits: 2901 Secondary Element: LEID 102 - Routing Digits: 2902 *	Resilient device located on secondary ICP. Command was issued on secondary ICP. * Indicates the known location of the device.
	The number refers to a remote directory number. Primary Element: LEID 101 - Routing Digits: 2901 Secondary Element: CEID 102 - Routing Digits: 2902 *	Resilient device is remote and located on secondary ICP. Command was issued on an “other” ICP. * Indicates the known location of the device.
	The number refers to a remote directory number. Remote DN to CEID 101, routing digits 2901.	Non-resilient device is remote and located on ICP with CEID 101 and routing digits 2901 Command was issued on an ICP that is not the device’s home element.
	IP Device ID: 3 Circuit Location: 1 3 1 3 3 Extension: 1001 MAC Address: 08:00:0F:01:26:5D	Non-resilient device is local (located on same ICP where command was issued).

## Locate Feature

The Locate Feature command provides feature information in addition to the same information as the Locate Extension command (see [Locate Extension](#)). The table below provides an example of the output provided for the Locate Feature command. Also see .

**Table 10.11:** Locate Feature Command

Example Input	Example Output	Meaning
locate feature extension 1001	IP Device ID: 3 Circuit Location: 1 3 1 3 3 Extension: 1001 Active Features: Make Busy MAC Address: 08:00:0F:00:AE:B2 Primary Element: CEID - Routing Digits: 2901 Secondary Element: LEID - Routing Digits: 2902 *	Resilient device with active Make Busy feature is located on secondary ICP. Command was issued on secondary ICP. The * indicates the known location of the phone. Local Element Identifier (LEID) identifies the ICP that you issued the command from.

## Locate Remote

You issue the Locate Remote command to determine whether a device is:

- Remote and resilient
- Remote and non-resilient
- Remote and Local (both)

The following table provides possible outputs for the Locate Remote command.

**Table 10.12:** Locate Remote Command Output for Resilient and Non-resilient Devices

Example Input	Example Output	Meaning
locate remote 3001	Remote Directory Number: 3001 Primary Element: CEID 101 - Routing Digits: 2901 * Secondary Element: LEID 102 - Routing Digits: 2902	RDN 3001 is resilient DN, located on primary ICP with CEID 101 and routing digits 2901. Command was issued on the secondary ICP with Local Element Identifier (LEID) 102 and routing digits 2902. The * indicates the known location of the phone.
locate remote 1001	Remote Directory Number: 1001 Primary Element: LEID 101 - Routing Digits: 2901 Secondary Element: CEID 102 - Routing Digits: 2902 *	RDN 1001 is resilient DN, located on secondary ICP with CEID 102 and routing digits 2902. Command was issued on the primary ICP with LEID 101.

**Table 10.12:** Locate Remote Command Output for Resilient and Non-resilient Devices

Example Input	Example Output	Meaning
locate remote 1001	Remote Directory Number: 1001 Primary Element: CEID 101 - Routing Digits: 2901 * Secondary Element: CEID 102 - Routing Digits: 2902	RDN 1001 is resilient DN, located on primary ICP with CEID 101 and routing digits 2901. DN's secondary ICP has CEID 102 and routing digits 2902. Command was issued on an "other" ICP.
locate remote 3002	Remote Directory Number: 3002 Remote DN to CEID 101, routing digits 2901	RDN 3002 is non-resilient DN, located on ICP with CEID 101 and routing digits 2901.

## Locating Resilient Hunt Groups

Use the following maintenance commands to obtain information for resilient hunt groups:

- Locate Hunt Group <pilot number>
- Locate Feature Hunt Group <pilot number>
- Locate Remote <pilot number>
- Locate Extension <pilot number>
- Locate Feature Extension <pilot number>

The table below lists examples of the system outputs for these maintenance commands when you issue them against a resilient hunt group.

**Table 10.13:** Locate Commands for Resilient Hunt Group (Sheet 1 of 2)s

Example Input	Example Output	Meaning
locate hunt group 4001	Pilot Number: 4001 Primary Element: LEID 201 - Routing Digits: 2905 * Secondary Element: CEID 200 - Routing Digits 2904	Hunt group pilot number 4001 is a resilient DN, located on primary ICP with local element identifier (LEID) 201 and routing digits 2905. The hunt group's secondary ICP has CEID 200 and routing digits 2904. LEID identifies the ICP that you issued the command from. The command was issued on the primary ICP. The * indicates the known location of the hunt group.

**Table 10.13:** Locate Commands for Resilient Hunt Group (Continued) (Sheet 2 of 2)s

Example Input	Example Output	Meaning
locate feature hunt group 4001	Pilot Number: 4001 Active Features: Do Not Disturb Primary Element: CEID 201 - Routing Digits: 2905 Secondary Element: LEID 200 - Routing Digits 2904 *	Hunt group pilot number 4001 is a resilient DN, located on secondary ICP with local element identifier (LEID) 200 and routing digits 2904. The hunt group's primary ICP has CEID 201 and routing digits 2905. Do Not Disturb is enabled for hunt group 4001 so the hunt group is not taking calls. Command was issued on the secondary ICP.
locate remote 4001	Remote Directory Number: 4001 Primary Element: LEID 201 - Routing Digits: 2905 * Secondary Element: CEID 200 - Routing Digits: 2904	Hunt group pilot number 4001 is a resilient DN, located on primary ICP with local element identifier (LEID) 201 and routing digits 2905. The hunt group's secondary ICP has CEID 200 and routing digits 2904. Command was issued on the primary ICP.
locate extension 4001	The number refers to a Hunt Group. Pilot Number: 4001 Primary Element: LEID 201 - Routing Digits: 2905 Secondary Element: CEID 200 - Routing Digits 2904 *	Hunt group pilot number 4001 is a resilient DN, located on the secondary ICP with a cluster element identifier (CEID) 200 and routing digits 2904. The hunt group's primary ICP has LEID 201 and routing digits 2905. Command was issued on the primary ICP.
locate feature extension 4001	The number refers to a Hunt Group. Pilot Number: 4001 Active Features: Do Not Disturb Primary Element: LEID 201 - Routing Digits: 2905 * Secondary Element: CEID 200 - Routing Digits 2904	Hunt group pilot number 4001 is a resilient DN, located on primary ICP with local element identifier (CEID) 201 and routing digits 2905. The secondary ICP has CEID 200 and routing digits 2904. Do Not Disturb is enabled for DN 4001 so the hunt group is not taking calls. Command was issued on an "other" ICP.

## Identifying the Status of a Resilient Device

### State Extension

You issue the State Extension command on an ICP to identify the state of a device that is in service on that ICP (in service, out of service, idle, busy). The State Extension command only provides information specific to the state of a given device on the ICP from which you issue the command. For example, if you issue this command on a resilient device's primary ICP and it is out of service there, you must then issue the command on the device's secondary ICP to determine the state of that device on that ICP.

If a resilient device is out of service on both of its ICPs

- The device may, itself, be out of service.
- The device may be in the process of registering on an ICP.

## State XNET ICP

You issue the State XNET ICP command to find resilient calls (calls in survival state) across IP trunks. If a device loses its ICP during a call, it retains PSTN access through a healthy controller. A healthy controller with calls on it that are in survival state is indicated in the command output by a link handle of zero.

**Table 10.14:** State XNET ICP Command Output for ICPs with Resilient Calls

Input	Output for Link Handle Value	Meaning
state xnet icp 44	0 (zero)	ICP 44 is healthy and is currently streaming calls in survival state.

## Obtaining the Status of Resilient Trunks

Use the following commands to obtain the status of resilient T1/E1 trunks:

- EDT Show Resiliency
- Dtstats Read and Dtstats Clear
- Netsync State
- State
- Show Faults

Refer to the System Administration Tool online help for instructions on how to use these commands.

## Controlling the Failover and Failback of Resilient Trunks

Use the following commands to control the failover and failback of resilient T1/E1 trunks:

- EDT Force Failover
- EDT Force Failback
- Programmed Failover

Refer to the System Administration Tool online help for instructions on how to use these commands.

## Identifying the Current ICP

You can determine the current ICP controller for a 5140 or 5240 IP Appliance by using the phone's built in debug function.

1. Press and hold down the volume up and volume down keys.
2. Dial **33284**.

3. Release the volume up and volume down keys.
4. Select **Network**.
5. Select **ICP Server IP(s)**.

Select **Current ICP Server** to display the IP address of the current ICP controller.

## Checking T1/E1 Resiliency Alarms

### *Trunk Alarms*

If the primary controller is supporting the resilient trunks, the resilient trunks are recorded in the Trunks category of the Alarm command output. During a failover from the primary to secondary controller, the failover of the T1/E1 trunks will generate an alarm on the primary controller if the programmed trunk alarm threshold is exceeded. After the trunks fail back to the primary, the system checks the trunk alarm category to determine if the alarm threshold is still exceeded. If the trunks are operating normally on the primary, and the alarm threshold is no longer exceeded, then the system clear the trunk alarm.

During normal operation, resilient trunks that are supported by the T1/E1 Combo MMC in the primary controller are “Not Seizable” on the secondary controller. These “Not Seizable” trunks do not generate alarms on the secondary controller. Instead, the secondary controller includes the resilient trunks in the system total of the “Inactive Trunks” alarm category.

After a failover, the secondary controller controls the resilient trunks. The resilient trunks are temporarily listed in the “Trunk” alarm category of the secondary controller. After the resilient trunks fail back to the primary controller, the trunks reappear in the “Inactive Trunk” alarm category of the secondary controller.

### *Digital Link Alarms*

On the primary controller, digital links that are associated with resilient trunks generate alarms if the links are not in a healthy state. On the secondary controller, the digital links for resilient trunks are included in the system total of the “Digital Links” alarm category.

### *Netsync Alarms*

You can program a resilient trunk on the primary controller as a netsync source. However, do not program a resilient trunk on the secondary controller as netsync source because the system will generate a minor netsync alarm.

Typically, the alarm threshold is set such that a minor netsync alarm is generated if a netsync source is unavailable. While the resilient trunks are supported by the primary controller, the resilient trunks on the secondary controller are in a non-seizable state so the netsync source is considered unavailable. The system, therefore, generates an alarm.

## Checking the T1/E1 Combo MMC Indicators

*Figure 10.3* shows the location of the indicators on the T1/E1 Combo MMC (PN 50005160). The LEDs

show the status of the link while the link is associated with the primary controller.









**Figure 10.3:** T1/E1 Combo MMC Indicators




The following table shows the meaning of the indicators. If the primary controller fails and transfers support for the trunk to the secondary, the LEDs on the T1/E1 Combo MMC will flash red and green.


**Table 10.15:**Meaning of T1/E1 Combo MMC Indicators

Indicators	Meaning	Action
	Link is functioning properly. No alarms present.	None.
	Primary controller has failed and the system has transferred support for the link to the T1/E1 MMC in the secondary controller.	Investigate reason for failure of primary controller. See <a href="#">IP Device Resiliency</a> .
	Loss of T1/E1 signal.	Check link connection.
	No signal is being received from the PSTN.	Check link with analyzer.
	Signal from the PSTN is faulty.	Check link with analyzer.
	<ul style="list-style-type: none"> <li>• Not programmed. Link descriptor not assigned.</li> <li>• System is out of service</li> <li>• Faulty T1/E1 MMC</li> </ul>	Assign link descriptor. Refer to System Tool Administration online help for programming instructions.

**Table 10.16:**Meaning of T1/E1 MMC Indicators on Secondary Controller (Sheet 1 of 2)

Indicators	Meaning	Action
	If the primary controller is supporting the link, this alarm state on the secondary controller indicates normal operation. Because the link is not connected to this T1/E1 MMC, the alarm is not reported in the system logs of the secondary system.	None.

**Table 10.16:** Meaning of T1/E1 MMC Indicators on Secondary Controller (Continued) (Sheet 2 of 2)

Indicators	Meaning	Action
	Primary controller has failed and support for the link has failed over to the T1/E1 MMC in this secondary controller. However, the signal from the PSTN is faulty.	Investigate reason for failure of primary controller. See <a href="#">IP Device Resiliency</a> . Check the link from the PSTN with analyzer.

**NOTE:** While the secondary controller is supporting the link, any link alarms that occur are shown on the secondary controller's T1/E1 MMC and reported in the logs of the secondary system. The conditions that are listed in , with the exception of the flashing Red and Green alarm, also apply to the secondary controller.

# Using Logs

## Logs

### Software Logs for System Features

Table 11.1:

Feature	Error Log	Possible Cause	Corrective Action
Malicious Call Trace	Not available	The network cannot register the malicious call trace because Malicious Call Trace is not programmed on the destination node	Program destination node to support Malicious Call Trace. See the System Administration Tool online help for instructions
	User not subscribed	The Malicious Call Trace supplementary service has not been subscribed	Obtain service for Malicious Call Trace on the destination node.
	Supplementary service interaction not allowed	Some supplementary services are mutually exclusive. An MCI request cannot be sent while such a supplementary service is active.	None

## Hot Desking Error Logs

**Table 11.2:** (Sheet 1 of 2)

Feature	Error Log	Possible Cause	Corrective Action
Hot Desking	INVALID	Incorrect feature access code	Ensure the feature access code is correct. If the set is on another ICP on a cluster, ensure that the correct access codes for “Hot Desk Login”, “Hot Desk Logout”, and “Hot Desk Remote Logout” are assigned on this ICP.
	INVALID HOTDESK EXT#	Indicates that the user DN specified is invalid	Check the user DN. If the set is on another ICP on a cluster, ensure the user DN has been provisioned for the cluster.
	NOT ALLOWED	Device type does not support hot Desking	Refer to the Hot Desking topics in the System Administration Tool online help for a list of the supported sets.
		Device does not have hot desking enabled	Ensure the “Hot Desk Login Accept” field in the phone’s COS is set to “Yes”
		On remote logout, indicates that the user has an active call on the phone.	The user’s DN must be idle (no ringing, active, or held call) before it can be logged out.

**Table 11.2:** (Continued) (Sheet 2 of 2)

Feature	Error Log	Possible Cause	Corrective Action
	INVALID PIN	Indicates that the hot desk user password specified is invalid	Ensure the password is correct.
	DENIED: EXT# IN USE	On login, indicates the hot desk phone has an active call or a hot desk user is logged in and has an active call	Hot desk phone and all line appearances must be idle before a user can log in. Clear all held or active calls before
	FEATURE FAILED	In a “standalone” (non-clustered) configuration, this error may indicate that a Cluster Element ID has not been programmed for the controller. This problem may arise when a controller with an earlier version of software is upgraded to a later version.	Ensure a cluster element ID is programmed. See Program Nodal Hot Desking topic in the System Administration Tool online help for details.
		In a clustered system, a Remote hot desk user attempts to login into a registration DN that is hosted on a different controller and receives FEATURE FAILED error message.	If a remote hot desk user tries to log into a set on a controller that has a different version of software than the controller that hosts the hot desk registration DN, the feature fails. To correct this problem, upgrade the controllers to the same software version.

## Voice Mail System Logs

The voice mail portion of a system log has five fields:

**DATE TIME LEVEL MSG#-PORT MESSAGE**

- DATE and TIME indicates when the event occurred.
- LEVEL indicates the message category and therefore the level setting required to include such messages in the output stream.
  - 0 = FATAL (voice mail system shuts down)
  - 1 = ERROR (abnormal event)
  - 2 = WARNING (may be an abnormal event)
  - 3 = INFO (normal monitoring)
  - 4 = TRACE (detailed monitoring, intended for lab use only)
  - 5 = DEBUG (very low-level, intended for lab use only)
- MSG# is a unique identifier for each message.
- PORT is the single-digit voice mail port associated with the message (or 0 if not port-specific).
- MESSAGE provides text indicating the event.

**Table 11.3:** (Sheet 1 of 17)

Error Number	Severity	Description	Solution/Action
1208	WARNING	<i>vtlight_extn: no dextens for mailbox m , state = s</i> The MWI could not be turned on( <i>s</i> =1)/off( <i>s</i> =0) for mailbox <i>m</i> because of an invalid mailbox extension.	Check/set the mailbox extension by using the VM Mailboxes form in the System Administration Tool, or the Group Administration Tool.
1216	INFO	An Administrator has logged in. The system administrators mailbox has been logged into using the BOX_ADMIN passcode	No action required.
1221	ERROR	Error calling VTGSERVICE, channel=channel Unable to start service function to initiate modem answer tone on port channel.	Contact service representative.

**Table 11.3:** (Continued) (Sheet 2 of 17)

Error Number	Severity	Description	Solution/Action
1506	WARNING	<p>Message Queue not updated properly from HQ.DAT</p> <p>The message queue file, HQ.DAT, is a backup file in case the system reboots after a message is accepted but before the message is physically delivered to the mailbox.</p> <p>This is a very small window. Regardless, at every boot up, we try to read this HQ.DAT file and deliver any undelivered messages.</p> <p>This warning occurs when the HQ.DAT file is not of the proper length. This could happen if the system was changed from a 4 port to an 8 port system.</p>	No action required
1507	ERROR	<p>Message Queue file, HQ.DAT, not updated properly</p> <p>An attempt to write to the HQ.DAT file failed during the queuing process.</p>	Try rebooting the 3300 ICP controller. If this does not help, contact service representative
1508	ERROR	<p>Message Queue file, %s, is not updated properly</p> <p>An attempt to write to the HQ.DAT file failed during the "de-queuing" process.</p>	
1808	ERROR	<p>MASTER.DAT cannot be opened more than once at any one time</p>	Contact service representative

**Table 11.3:** (Continued) (Sheet 3 of 17)

Error Number	Severity	Description	Solution/Action
1809	INFO	cal_get - Business hours have not been set This is an informational message that appears at reboot if the business hours have not been set by the system administrator.	No action required
1811	INFO	sg_get - No alternate greetings have been set This is an informational message that appears at reboot if there have not been any alternate greetings set by the system administrator.	
1812	INFO	MASTER.DAT was not open, but the 'close' will be executed. A request was made to close MASTER.DAT, but it was not open in the first place.	
2213	ERROR	vtshr_greet: rename ( <b>from</b> , <b>to</b> ) error	Unable to rename a temporary (new) greeting file to its permanent name. Try the operation again. If this still does not work, contact service representative
2216	ERROR	vtadm_enable_disable: Can't update parm.bin While trying to enable or disable a feature, the file PARM.BIN could not be opened or written to.	Try retrieving PARM.BIN. If it is there, reboot the system and try again. If the file is not there, send a fresh version over, then try a fresh install. If this still does not work, contact service representative
2217	INFO	<i>vtadm_enable_disable</i> : Updated parm.bin	No action required



**Table 11.3:** (Continued) (Sheet 4 of 17)

Error Number	Severity	Description	Solution/Action
2218	ERROR	<i>master_set_mailbox_length:</i> master_createmaster.dat file creation failed.	Contact service representative.
2219	WARNING	wakeup_notify_PBX:no dextens for mboxNo extension is configured for this mailbox	No action is required.
2229	ERROR	failed to remove voxdrv.cfg	Log the message in diag.dat and continue.
2230	ERROR	Failed to rename voxdrv.tmp	Contact service representative.
2403	INFO	VT_RECDONE:v Indicates that a recording has terminated. The value v tells how the termination happened: 2 - A terminating DTMF was detected. 5 - End of data reached (?) 7 - Timed out, rarely happens 10 - Terminated due to silence 12 - Terminated due to loop current dropping. 13 - Terminates on EOF, very rare 31 - Terminated due to non-silence; i.e. sound is constantly above a certain threshold. VT_ON:v The port has gone on-hook. VT_OFF:v The port has gone off-hook	No action required

**Table 11.3:** (Continued) (Sheet 5 of 17)

Error Number	Severity	Description	Solution/Action
		<p>VT_BUSY:v An outdial (page) has resulted in a busy signal.</p> <p>VT_NOAN:v An outdial (page) has resulted in no answer.</p> <p>VT_CONN:v An outdial (page) has resulted in a connection being made and the recipient hears/sees the result of the page.</p> <p>VT_INTER:v Operator intercept&amp;will be treated as a no answer. These are informational messages that come out to help give an idea as to the traffic of the system and how recordings were terminated. v only has meaning when on the</p> <p>VT_RECDONE line:</p>	

Table 11.3: (Continued) (Sheet 6 of 17)

Error Number	Severity	Description	Solution/Action
3001	ERROR	vtalist:ret= <b>r</b> ,total_boxes= <b>tb</b> The attempt build a list of mailbox records from MASTER.DAT failed. <b>r</b> = reason write failed: -1 = could not open MASTER.DAT -2 = could allocate space (malloc) <b>tb</b> = total number of records in MASTER.DAT	Contact service representative.
3201	FATAL	vtv40 error,file=[ <b>filename</b> ] The prompt <b>filename</b> cannot be found/opened.	
3207	INFO	vtspeak - Prompt <b>pp</b> File VTP.VAP Missing This means that a requested prompt could not be played. The reason is most likely that the VAP file is corrupt, this usually means truncated. If the prompt number is between 1 and 100, the file in question is VTP.VAP. If the prompt number is greater than 100, the file is VTE.VAP.	
3209	ERROR	Prompt <b>num</b> File VTP.VAP Missing Prompt number, <b>num</b> , does not exist in file VTP.VAP.	Contact service representative
3210	ERROR	MBox size incorrect File= <b>f</b> There is something wrong with the MSG file, <b>f</b> . The most likely reason is that it is full and can not accept new messages. If there is another reason, it would be shown in error message 4706	Check how many messages are in the mailbox. If OK, see message 4706.

**Table 11.3:** (Continued) (Sheet 7 of 17)

Error Number	Severity	Description	Solution/Action
3213	ERROR	<p>Default Language <b>nnn</b> prompts missing, substituting English</p> <p>The prompts for the configured default language are not installed. English is being substituted. The value of nnn indicates the configured language:</p> <p>1 = English 2 = Spanish 3 = French 4 = Dutch 5 = UK English</p>	Select a different default language.
3214	ERROR	<p>Alternate language <b>nnn</b> prompts missing. Language ignored.</p> <p>The prompts for the configured alternate language are not installed. No alternate language has been loaded.</p> <p>The value of nnn indicates the configured language as defined above for message 3213.</p>	Select a different alternate language.
4312	WARNING	<p>vtxd40: Incorrect File Handle for Record</p> <p>The file handle passed into Record_Msg_Enter() is invalid. That is, it is less than 5 or greater than 59.</p> <p>This most likely means that too many files were left in the open state.</p>	In order to get back up and running so that messages can be left, reboot the system. Then contact your service representative so that logs can be retrieved.
4313	WARNING	<p>vtxd40: Invalid event during record d40event=event</p> <p>While a message was being recorded, a Dialogic event was returned that was unexpected. For details on the event, look up the event code in the Dialogic reference guide.</p>	Note the event and contact your service representative.

Table 11.3: (Continued) (Sheet 8 of 17)

Error Number	Severity	Description	Solution/Action
4316	INFO	vtxd40: Voice Mail is gracefully shutting down This message occurs when Contact is rebooted remotely via the System Administration Tool or the Group Administration Tool.	No action required.
4319	ERROR	vtxd40: Dos Error Encountered DOS code= <b>c</b> cstate= <b>s</b> On a record or playback, there was a problem writing to or reading from the voice file. c is the _doserrno value that is set when a write, seek or read fails.	Contact service representative
4320	INFO	stopch() issued Indicates port is being stopped as part of application shutdown.	No action required
4321	INFO	T_STOP received Indicates port is being stopped as part of application shutdown.	
4323	ERROR	vtxd40: Event Error Code= <b>error</b> There was an error when calling the Dialogic get event function ( <b>getevt</b> ). For details on the error, look up the <b>error</b> code in the Dialogic reference guide.	Contact service representative
4324	FATAL	vtxd40: D/40 Driver Not Installed	Make sure the VOXDRV started. Watch the bootup via a serial cable and PCPlus. Otherwise, contact service representative.

Table 11.3: (Continued) (Sheet 9 of 17)

Error Number	Severity	Description	Solution/Action
4326	WARNING	vtxd40 - Unable to set Parameters Dialogic call to setxparm() failed.	Contact your service representative
4327	INFO	vtxd40 - intlevel= <b>irq</b> rc= <b>rc</b> The function startsys() failed. This is because there is something wrong with the VBPC interface.	Make sure phone system is up. If problem persists, contact your service representative.
4328	INFO	vtxd40: <b>p</b> ports available, <b>a</b> installed, hourlim= <b>h</b> , vm_model_no= <b>m</b> <b>pp</b> - The number of ports as indicated by the model number. <b>a</b> - The number of ports that the voice driver detected. 0 = no limit. <b>h</b> - The total number of storage hours available as indicated by the model number. 0 = no limit. <b>m</b> - This is the model number. If 0, then the model has not been set. This message is displayed on system startup, when the phone system is configured, when the fax detection feature is set (with phone or CGM), when a technician uses the technicians users interface to reset the ports, when the D40 token is manually sent from CGM.	No action required
4341	WARNING	vtxd40: Error in Voice Code This happens when the file format to be played in not valid.	Contact your service representative.
4342	WARNING	vtxd40: action= <b>action</b> rc= <b>rc</b> Error occurred while trying to play a file.	Contact your service representative, noting the action and rc values.

Table 11.3: (Continued) (Sheet 10 of 17)

Error Number	Severity	Description	Solution/Action
4350	WARNING	vtxd40: Call to vb_get_cpuid failed vb_get_cpuid() is a call to the VBPC driver that is done through a vtgservice call to the VOXDRV. To examine the exact reason why this failed, look at the VBPC log file which is located in c:\vbpc\log\vbpclog.dat.	If vbpclog.dat does not give enough information, contact your service representative.
4501	FATAL	System Parameters have FAILED to be set This can come out in the same situation as above only if there is a problem with the PARM.BIN file.	Contact service representative
4503	FATAL	vtxinit - Error starting the Voice Board	
4704	ERROR	file_name= <b>file</b> , d40derr= <b>error</b> There was an error attempting to open or write to the named file. It has to do with recording, but the actual filename dictates which part of the recording process was affected.	Contact your service representative
4706 4707 4708	ERROR	Mbox size Error ret= <b>ret</b> Mbox size Error ret= <b>ret</b> x_size_folders:Error ret= <b>ret</b> , tag= <b>tag</b> These messages occur when there is something wrong a particular mailbox MSG file. <b>ret</b> is the return value of x_size() and has the following meanings. -2 = The mailbox is full -3 = The <b>tag</b> value in the file is not correct -4 = The file handle passed in was invalid	Make sure the mailbox is not full. If not full, try renaming the MSG file. Regardless of the results of the above, contact your service representative

Table 11.3: (Continued) (Sheet 11 of 17)

Error Number	Severity	Description	Solution/Action
4907	ERROR	MBox Dir Error fname= <b>n</b> Code= <b>c</b> The message file <b>n</b> is not valid, the reason is indicated by <b>c</b> .	Contact service representative; the situation does not recover by itself.
4711	ERROR	Corrupt MBox handle= <b>handle</b> msg_no= <b>msg_no</b> ret= ret Playing a message failed. The reason is dictated by the return code <b>ret</b> . Below are possible values of <b>ret</b> . <ul style="list-style-type: none"> <li>• Message is too short and will not be played</li> <li>• The actual playing of the file failed. it probably does not exist</li> <li>• File handle bad</li> <li>• The message number is bad (out of range with respect to the system wide max), or the MSG file tag is bad.</li> </ul>	If the return code is -3 or -4, contact your service representative. If the return code is -2, it may have been purged. Otherwise, no action is required
4715	ERROR	I/O Read Problem An error occurred while trying to <b>write</b> to an MSG file. There is no reason as to why.	Even though there is no extra information associated with this message, look at error message 4704 for the filename and associated error. Contact your service representative.



**Table 11.3:** (Continued) (Sheet 12 of 17)

Error Number	Severity	Description	Solution/Action
4716	ERROR	<p>x_record:prev(.\grp\nnnnnnnn n.nnn) not closed,cur=.\MSG\msgnn.vox This has only been seen with the current file being a mailbox file (msgnn.vox). The previous file has been noted to be either a grp, name, or int file - i.e. an actual message file, a name file or a greeting file. Listed below are the scenarios of when each has been reproduced.</p> <p>\grp</p> <ul style="list-style-type: none"> <li>When logged into the mailbox noted in the error message, if 3 is entered to leave a memo, and the prompt begins, but the user hangs up before recording begins.</li> <li>When logged into the mailbox noted in the error message, if 2 is entered to send a message, and the destination list is complete, and the prompt has begun, and the user hangs up before recording begins.</li> </ul> <p>\name No scenarios have been determined.</p> <p>\int No scenarios have been determined.</p>	This has not been noted to cause any other problems, so no action is required by the technician.
4719	Error	<p>x_erase(%d,%d) returning %d : Failed to mark message as erased</p>	Contact your service representative.

Table 11.3: (Continued) (Sheet 13 of 17)

Error Number	Severity	Description	Solution/Action
4720	ERROR	<p>Incorrect File Handle for Erase</p> <p>In all cases, a message could not be deleted due to one of the following with respect to the corresponding MSG file:</p> <ul style="list-style-type: none"> <li>bad file handle</li> <li>message number is out of range of the system default</li> </ul> <p>MSG tag is incorrect</p>	Contact your service representative.
4723	ERROR	<p>x_keep(handle,msg_no,function) returning ret</p> <p>This error is displayed if something goes wrong with saving a message after it has been listened to.</p> <p><b>handle</b> DOS handle to the MSG file of the mailbox in question.</p> <p><b>msg_no</b> - Which message do we want to keep for the mailbox in question</p> <p><b>function</b> 0=Keep, 1=Mark Unread</p> <p>ret return value of x_keep()</p> <p>-1 = lseek() or read() into MSG file failed</p> <p>-2 = file handle bad, or bad tag in MSG file</p>	<p>If isolated incident, no action required. If it continues with only the same mailboxes, listen to all messages in mailbox and then delete the MSG file. Leave a new message to test.</p> <p>If this does not help, contact your service representative</p>
4726	INFO	<p>deleting 0 length file: f</p> <p>This message is generated when a file that was opened to receive a recording is closed and is of zero length. For example, when leaving a message, if the user hangs up before the beep, this will leave around a zero length file. Hence when this file is deleted, the above message occurs.</p>	No action required

Table 11.3: (Continued) (Sheet 14 of 17)

Error Number	Severity	Description	Solution/Action
4729	INFO	Msg <b>f</b> for <b>b</b> When a message is left for a mailbox, the name of the file that holds the voice data is logged. <b>f</b> - file name <b>b</b> - mailbox receiving message	No action required
4900	INFO	Application successfully initialized This message comes out every time the system is booted. It indicates that we have gotten past most initialization routines.	
4907	FATAL	vtxmain: vtxinit failureFailed to start voice driver	Contact your service representative
4908	FATAL	Application Program Failed	
4915	FATAL	vtg_malloc ( <b>size</b> ) Unable to allocate memory block of <b>size</b> bytes.	Contact your service representative
4916	INFO	<b>ptr</b> =vtg_malloc ( <b>size</b> ) System successfully allocated <b>size</b> bytes of memory at location <b>ptr</b>	No action required
		-8 This means there was something wrong with the mailbox file. The rc value in the error message will give you further details on what was wrong. Below is a list of the possible values for rc and what they mean: -1,-2,-3 The <b>msgnn.vox</b> file is somehow corrupt. It is not known how it could get into this state. This probably means that the <b>msgnn.vox</b> file is indicating that there are more than 250 messages.	

Table 11.3: (Continued) (Sheet 15 of 17)

Error Number	Severity	Description	Solution/Action
5309	ERROR vtx\vtxutil.c	x_delete_tmmsg: read error, mbox= <b>mailbox</b> This function will delete the message file that is referenced in a transaction record of the <b>mailbox</b> MSG file. Could not read the correct number of bytes from the <b>mailbox</b> MSG file.	Contact your service representative
5310	ERROR	vtbox_full(Box_Num= <b>b</b> )= <b>r</b> , tot_msgs= <b>tm</b> , box_msgs= <b>am</b> fh= <b>fh</b> , f_size= <b>fs</b> , rc= <b>rc</b> , s/c= <b>s/c</b> Every time a message or memo is left for a mailbox, we first check to make sure there is room for the message/memo in the recipients mailbox. If there is not, the user is vocally informed and this message is logged. am is the maximum number of messages that the mailbox in question can contain. Note that these two messages always come out together.	The user must delete some messages before new ones can be left.
6001	INFO	Msg <b>f( mm/dd hh:mm)</b> for <b>b</b> deleted A voice message sent to a single mailbox has been deleted from the disk <b>f</b> = filename, <b>mm</b> = month, <b>dd</b> = day, <b>hh</b> = hour, <b>mm</b> = minute, <b>b</b> = mbox #	No action required

**Table 11.3:** (Continued) (Sheet 16 of 17)

Error Number	Severity	Description	Solution/Action
6002	INFO	Msg <b>f</b> ( <b>mm/dd hh:mm</b> ) for <b>b</b> deleted A voice message sent to a multiple mailboxes has been deleted from the disk <b>f</b> = filename, <b>mm</b> = month, <b>dd</b> = day, <b>hh</b> = hour, <b>mm</b> = minute, <b>b</b> = mbox #	
6003	INFO	Msg <b>f</b> ( <b>mm/dd hh:mm</b> ) for <b>b</b> is old.This will be deleted during nightly cleanup	
6005	INFO	Msg <b>f</b> ( <b>mm/dd hh:mm</b> ) for <b>b</b> deleted A voice message was erased by the mailbox owner. <b>f</b> = filename, <b>mm</b> = month, <b>dd</b> = day, <b>hh</b> = hour, <b>mm</b> = minute, <b>b</b> = mbox #	No action required
6006	INFO	Msg <b>f</b> ( <b>mm/dd hh:mm</b> ) for <b>b</b> saved. A voice message was saved by the mailbox owner. <b>f</b> = filename, <b>mm</b> = month, <b>dd</b> = day, <b>hh</b> = hour, <b>mm</b> = minute, <b>b</b> = mbox #	No action required
6007	INFO	Mailbox <b>b</b> added The system administrator has added a mailbox, <b>b</b> , to the system.	No action required
6008	INFO	Mailbox <b>b</b> deleted The system administrator has deleted a mailbox, <b>b</b> , from the system. All associated messages and recorded greetings are deleted.	No action required

**Table 11.3:** (Continued) (Sheet 17 of 17)

Error Number	Severity	Description	Solution/Action
6013	WARNING	Rename from msg*.vox to msg*.vox failed	No action required. May need to restore from and to box information
6014	WARNING	Rename from nam*.vox to nam*.vox failed	
6015	WARNING	Rename from int\int*.vox to int\int*.vox failed	
6016	WARNING	Rename from int2\int*.vox to int2\int*.vox failed	
8015	WARNING	Messages still in Queue to VoxDrv. There are messages present in voxdrv queue while the system has started shutdown.	Contact your service representative
8016	WARNING	Messages still in Queue to VoxDrv. There are messages present in voxdrv queue while the system has started shutdown.	
8017	WARNING	Failure to delete toVoxDrv Message Queue. The voxdrv queue could not be deleted when the system shutdown started	Take note of the error, and contact your service representative
8301	ERROR	Failed to start channel timer. Channel timer is already running.	No action required.









