

MITEL

5000

Features and Programming Guide



Part Number
580.8006



Mitel 5000 Features and Programming Guide

Issue 3.0, October 2008

Notice

This manual is released by Mitel Networks Corporation as a guide for certified service personnel. It provides information necessary to properly configure, maintain, and operate the product.

The contents of this document reflect current company standards and are subject to revision or change without notice. Some features or applications mentioned may require a future release and are not available in this release. Future product features are subject to availability and cost. Some features may require additional hardware and/or specific software.

The contents of this manual may include technical or other inaccuracies. Mitel reserves the right to make revisions or changes without prior notice. Software packages released after the publication of this manual will be documented in addenda to the manual or succeeding issues of the manual.

For additional information and/or technical assistance in North America, certified technicians may contact:

Technical Support Department (USA)
Mitel Networks, Inc.
7300 West Boston Street
Chandler, AZ 85226-3224
1-888-777-EASY (3279)

For information on how to contact Mitel Technical Support outside of North America, please refer to your Channel Support Agreement.

If you have any questions or comments regarding this manual or other technical documentation, contact the Technical Publications Department (USA) at:

tech_pubs@mitel.com

Mitel® is a registered trademark of Mitel Networks Corporation.
Inter-Tel® is a registered trademark of Inter-Tel (Delaware), Incorporated.

All other trademarks mentioned in this document are the property of their respective owners, including Mitel Networks Corporation and Inter-Tel (Delaware), Incorporated. All rights reserved.

© 2005–2008 Mitel Networks Corporation

Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from Mitel Networks Corporation.

Limited Warranty

Mitel warrants that its products will, if delivered to the end-user in undamaged condition, be free from defects in material and workmanship under normal use and service for the period set forth on the current warranty periods as published in the U.S. Price List from time to time and substantially in conformance with the documentation (functional and operating specifications) that Mitel publishes regarding same (end-user reference and operating manuals and guides relating to the program). Mitel does not, however, warrant that the functions contained in the software program will satisfy Dealer's particular purpose and/or requirements or that the operation of the program will be uninterrupted or error free.

Mitel shall incur no liability under this warranty and this warranty is voidable by Mitel (a) if the product is used other than under normal use, with certified repair and maintenance service and under proper environmental conditions, (b) if the product is subject to abuse, misuse, neglect, flooding, lightning, power surges, third-party error or omission, acts of God, damage, or accident, (c) if the product is modified or altered (unless expressly authorized in writing by Mitel), (d) if the product is installed or used in combination or in assembly with products not supplied or authorized by Mitel and/or which are not compatible with or are of inferior quality, design, or performance to Mitel or Mitel supplied products so as to cause a diminution or degradation in functionality, (e) if there is a failure to follow specific restrictions in operating instructions or (f) if payment for product has not been timely made.

The sole obligation of Mitel and the exclusive remedy and recourse of Dealer under this warranty, or any other legal obligation, with respect to product, including hardware, firmware, and software media, is for Mitel, at its election, to either repair and/or replace the allegedly defective or missing product(s) or component(s) and return (prepaid) same (if necessary), or grant a reimbursement credit with respect to the product or component in the amount of the sales price to the Dealer. With regard to a software program design defect, however, to the extent it prevents the program from providing functionality and/or operating as intended by Mitel, is service affecting, and prevents beneficial use of the product, Mitel does undertake to use its best efforts to devise a suitable corrective solution to the problem within a reasonable period of time; should said action, however, not substantially resolve the problem, then Mitel reserves the right to substitute a new release ("stream") of software as soon as it is generally made available by Mitel. The above, with regard to a software design defect, likewise, constitutes the sole obligation of Mitel and exclusive remedy of Dealer hereunder.

The responsibility of Mitel to honor the express limited warranty stated above also shall be predicated on receiving timely written notice of the alleged defect(s) with as much specificity as is known within thirty (30) calendar days of the malfunction or by the expiration of the warranty period (plus thirty [30] calendar days), whichever occurs first. Mitel shall further have the right to inspect and test the product to determine, in its reasonable discretion, if the alleged malfunction is actually due to defects in material or workmanship. Unless waived by Mitel, Dealer agrees to return (prepaid) the allegedly defective product or component to Mitel for inspection and/or testing, and, if appropriate, for repair and/or replacement.

NOTICE

The above express Limited Warranty is in lieu of all other warranties, express or implied, from Mitel Networks Corporation, or Inter-Tel, Inc., and there are no other warranties which extend beyond the face of this warranty. All other warranties whatsoever, including the implied warranty of merchantability and the implied warranty of fitness for a particular purpose relating to use or performance of the product, including its parts, are hereby excluded and disclaimed.

In no event shall Mitel Networks Corporation, under any circumstances, be liable for nor shall a purchaser (directly or indirectly) be entitled to any special, consequential, incidental, indirect, punitive, or exemplary damages as a result of the sale or lease of product including but not limited to failure to timely deliver the product or failure of product to achieve certain functionality, or arising out of the use or inability to use the product, in whole or in part and including but not limited to loss of profit, loss of use, damage to business or damage to business relations even if notified of the possibility of such damages. Mitel shall not be liable for personal injury or property damage unless caused solely by Mitel's negligence.

NOTICE

For complete information on returning equipment, refer to the current *Mitel Repair and Return Policy*, document part no. 835.1065. This document includes specific information on the following subjects: warranty, procedures to follow when returning equipment, equipment damaged in shipment, insurance, repair policy, and advance replacement policy.

Network Security Statement

Although no telecommunications system or data network is entirely secure, as long as appropriate security measures are put in place and properly maintained by both the customer and the installing company, this Mitel® Advanced Communications Platform architecture and its associated server-based applications are substantially secure against unauthorized access to the customer's data network via the telecommunications system. Appropriate security measures include, but are not limited to, the proper implementation of user/administrative accounts, passwords, firewalls, Network Address Translation (NAT), access control lists, virus protection, security updates, etc., and the proper maintenance of access points/programs and their respective accounts/passwords.

Secure Socket Layer

Copyright© 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL. This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.

If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Contents

Tables	xxvii
---------------	--------------

Figures	xxxix
----------------	--------------

New Features	1-1
---------------------	------------

Introduction	1-3
New Features and System Changes Described in This Book	1-3
New Features for Hardware and Installation	1-3
Mitel Cordless Devices	1-3
Mitel 5000 v3.0 New Features in DB Programming	1-4
Mitel NuPoint Messenger	1-6
SIP Peer Voice Mail	1-7
New Alarms and Messages	1-9
Licenses	1-9
OAI Caller ID Control	1-9
DB Programming Changes	1-10
General DB Programming Application Changes	1-10
License Changes	1-10
Session Manager	1-11
Voice Processing Changes	1-11
E-Mail Gateway	1-12
Call Configurations	1-12
Passwords\Edit Access Rights	1-13
New Features in Administrative Web Session (AWS)	1-14
New AWS Pages	1-14
Modified AWS Pages	1-18

About Database Programming 2-1

Introduction	2-2
Technical Support	2-2
Planning the Programming Session	2-2
Programming Wizards	2-2
Programming Checklist	2-3
Session Manager	2-4
Session Manager Interface	2-4
Session Menu	2-5
Settings Menu	2-6
Session Description	2-7
Session Manager Connection Tabs	2-7
Starting a DB Programming Session	2-8
Session Manager Connection Options	2-9
Local (Stand-Alone)	2-9
Network (Over IP)	2-10
Network (Using a Modem)	2-10
DB Programming User Interface	2-12
DB Studio Elements	2-13
Menu Bar	2-13
Toolbar Buttons	2-14
Directory Folders	2-15
Status Bar	2-15
Programming the Inactivity Timer	2-15
Selection Wizards	2-16
DB Programming Tips	2-17
Viewing DB Studio Programming Panes	2-17
Changing Displayed Information in the Programming Window	2-17
Using a Keyboard Instead of a Mouse	2-18

System Management 3-1

Introduction	3-3
Passwords	3-4
Programming a Password	3-4
Assigning Administrator Access Rights	3-5
System Software Licenses	3-6
About Software License	3-9
Software License Operations – Upload Software License	3-10
Comparing or Uploading a Software License	3-11

Database Backup Options	3-12
Backup Database Save	3-14
Scheduled Backups	3-15
Default Database	3-34
System Error Information	3-35
System Maintenance Options	3-36
Call Costs	3-37
Freeze Zones	3-39
System Health Report	3-40
System Resets	3-44
Immediate System Resets	3-44
Call Processing Resets	3-44
Major Reset Scheduling	3-44
Message Print	3-48
Station Message Detail Recording	3-50
Remote Configuration	3-54
 Private Networking and System Nodes	 4-1
<hr/>	
Introduction	4-2
Nodes	4-2
Local Nodes	4-2
Remote Nodes	4-3
Remote Node Trunk/IP Connection Groups	4-4
Using The Networking Wizard	4-6
Starting the Private Networking Wizard	4-6
Configuring IP Networking	4-7
Configuring T1/E1 PRI Networking	4-10
Node Devices – Importing and Exporting	4-19
Modems	4-23
Off-Node Modems	4-24
Local Modems	4-25
System Manager	4-26
Configuring the Node to Interface with System Manager	4-26
Uploading the System Manager CA Certificate	4-27

Numbering Plans 5-1

Introduction	5-3
Area Flags	5-4
Classes of Service (COS)	5-5
COS for U.S. Systems	5-5
COS for European Systems	5-6
Programming COS Options	5-7
Device Baseline Extensions	5-9
Automatic Route Selection (ARS)	5-10
Planning ARS Requirements	5-11
Programming ARS Dial Rules	5-12
Programming ARS Facility Groups	5-13
Programming ARS Route Groups	5-16
Emergency Calls	5-21
Home Area Codes	5-22
Toll Strings	5-23
Programming Toll Strings	5-24
Adding or Deleting Toll String Dial Patterns	5-25
User Groups	5-25
Planning User Groups	5-25
Programming Area Codes	5-26

Trunks and Gateways 6-1

Introduction	6-3
Trunk Programming	6-3
Viewing or Programming Trunks	6-4
Changing Trunk Extension Numbers	6-4
Copying Trunks	6-5
Assigning Trunks to CO Trunk Groups	6-5
SIP Gateways	6-6
Understanding NAT Challenges for SIP Devices	6-6
Placing a SIP Gateway Behind a NAT Device	6-7
SIP Trunks	6-8
Creating SIP Trunks	6-8
Programming SIP Trunk Options	6-8

MGCP Gateways, Devices, and Trunks	6-9
Creating an MGCP Gateway and Endpoint	6-9
Adding an MGCP Endpoint	6-10
Changing the MGCP Gateway IP Address	6-10
Trunk Programming Options	6-11
CO Trunk Group	6-13
Service Type	6-13
DTMF Signaling	6-13
Start Type	6-14
DID Disconnect Timer	6-14
Answer Supervision Types	6-15
Connect Trunk-to-Trunk Calls on Polarity Reversal	6-16
Send Digits En Bloc	6-16
Echo Profile	6-16
Connected to CO	6-17
Hybrid Balance	6-17
Measured Echo Return Loss	6-17
Service Prefix Base Number	6-17
Number Of Digits To Receive	6-18
Language	6-18
Network Group	6-18
Reserve IP Resources for Device	6-19
NAT Address Type	6-19
Call Configuration	6-20
CP History	6-20
MGCP Gateway Port	6-20
Communication Timeout	6-21
Manufacturer	6-21
Gateway Name and Endpoint Name	6-21
Associated Gateway	6-21
Call Routing Tables	6-22
Changing Call Routing Table Descriptions	6-23
Programming Call Routing Keys	6-23
Call Routing Patterns	6-24
Editing Call Routing Table Patterns	6-25
Persistent Music-On-Hold Selection	6-29

Loop Loss Measurement Test	6-31
Configuring Loop Loss Measurement Test Fields	6-32
Starting a Loop Loss Measurement Test	6-32
Loop Start AC Impedance	6-33
ISDN PRI Two B-Channel Transfer	6-34

Endpoints and Devices **7-1**

Introduction	7-4
Viewing System Endpoints	7-4
Creating (Adding) Devices	7-4
Adding Digital Endpoints	7-4
Creating Local IP Endpoints and Devices	7-5
Creating Endpoints from CSV Files	7-8
Creating Off-Node Devices	7-13
Using the Wildcard Character in Off-Node Extensions	7-14
Programming Device Descriptions and User Names	7-15
IDS Support	7-15
Hiding User Names in Voice Mail Directories	7-15
Copying Endpoint Programming	7-16
Viewing Associated Devices and References	7-17
Converting Usernames to Mixed Case	7-18
Converting Inter-Tel IP Endpoints to Mitel IP Endpoints	7-19
Editing IP Device MAC Addresses	7-20
Changing Endpoint Extension Numbers	7-21
Changing a Single Extension Number	7-21
Changing Multiple Extension Numbers at One Time	7-21
Endpoint Flags	7-22
Programming Flags for Individual Endpoints	7-22
Programming Flags for Multiple Endpoints	7-22
Keymaps	7-27
Viewing Default Keymaps	7-28
Adding New Keymaps	7-29
Programming Endpoint Keymaps	7-30
Selecting Standard or Alternate Keymaps	7-39
Changing Keymap Types	7-40
Copying and Pasting Keymaps	7-41
Programming Endpoint Keymap Buttons	7-42
Programming DSS Keymaps	7-44

Programming Endpoint Options	7-50
Associated Extensions	7-51
Call Logging	7-54
Day and Night Classes of Service	7-55
Forwarding Paths	7-56
Mailboxes	7-58
Record-A-Call	7-58
Languages	7-60
Secondary Language	7-61
House Phones	7-62
Remote Programming Password	7-63
Calling Party Name	7-63
Calling Party Number	7-64
Emergency Party Calling Number	7-64
Attached Device	7-64
Device Audio for Calls Settings	7-65
Audio for Calls Camped onto this Device	7-65
Audio for Calls Holding for this Device	7-65
Audio for Calls Ringing this Device	7-66
Phantom Devices	7-67
Account Codes	7-69
Viewing Account Codes	7-70
Programming Forced Account Code Options	7-70
Adding Devices to an Account Code List	7-70
Deleting Devices from Account Code Lists	7-71
Assigning an Account Code Type to an Individual Endpoint	7-71
Setting the Forced Account Code Validated Flag	7-71
Endpoint Messages	7-72
Changing Do-Not-Disturb Messages	7-72
Changing Reminder Messages	7-73
System Forwarding Paths	7-74
System Speed Dial	7-75
Administrator Endpoint DB Programming Password	7-76
Message Centers	7-77
Attendants	7-78
Primary Attendants	7-79
Single Line Endpoint CLID Timers	7-80

Extension Lists and System Groups **8-1**

Introduction	8-4
Extension Lists	8-4
Viewing Extension Lists	8-5
Creating Extension Lists	8-5
Adding Devices to Extension Lists	8-5
Deleting Extension Lists	8-6
CO Trunk Groups	8-7
Viewing Trunks in a Trunk Group	8-7
Adding CO Trunk Groups	8-8
Changing CO Trunk Group Extension Numbers	8-8
Moving Trunks Between CO Trunk Groups	8-9
Programming CO Trunk Group Options	8-10
Node Trunk Groups	8-28
Viewing Node Trunk Group Trunk Lists	8-28
Viewing or Changing Node Trunk Group Information	8-28
Programming Node Trunk Group Options	8-28
Hunt Groups	8-32
ACD Hunt Groups	8-33
Local Hunt Groups	8-35
Local Hunt Group Options	8-37
Node-Spanning Hunt Groups	8-51
Remote (Off-Node) Hunt Groups	8-51
Network Groups	8-52
Hardware Upgrades	8-52
Network Group Assignments	8-52
Creating Network Group Endpoints and Trunks	8-53
Node IP Connection Groups for Remote Nodes	8-54
Node IP Connection Group IP Call Configurations	8-55
Day/Night Emergency Outgoing Access	8-56
Day/Night Outgoing Access	8-56
Remote Node	8-57
Camp-Ons Allowed	8-57

System and Device IP Settings 9-1

Introduction	9-3
IP Device Status	9-4
System IP Settings	9-5
General IP Settings	9-6
Mitel 5600 Base Server/Processing Server Connection Settings	9-11
Web/SSH Settings	9-13
TFTP Settings	9-14
Advanced IP Settings	9-15
NTP Server Configuration	9-16
Local Processor Module and Expansion Card IP Settings	9-17
NAT IP Address	9-18
Audio RTP Type of Service and Data Type of Service	9-18
Audio Stream Receive Port	9-19
IP Terminal TCP Call Control Port	9-19
IP Terminal General Purpose UDP Port	9-19
MGCP Receive Port	9-20
TCP Call Control Port	9-20
Echo Profile	9-20
Remote Node IP Connections	9-21
Viewing Off-Node IP Connections	9-21
Creating Off-Node IP Connections	9-22
Node IP Connection Group	9-22
Remote IP Address	9-22
Remote Audio Receive Port	9-23
Remote Listening Port	9-23
IP Call Configurations	9-24
Adding Call Configurations	9-25
Adding IP Endpoints to the Call Configuration	9-25
Adding Trunks to the Call Configuration	9-25
Adding SIP Voice Mails to the Call Configuration	9-26
Programming Call Configuration Options	9-27
Sockets	9-34
Enabling or Disabling a Socket Connection	9-34
Entering a Socket Password	9-35

Endpoint and Device IP Settings	9-36
Emergency Extensions for IP Devices	9-37
Network Configuration	9-38
Programming Inter-Tel IP Endpoints in ITP Mode	9-41
Resource Reservation Tool	9-42

System Settings **10-1**

Introduction	10-2
System-Wide Parameters	10-2
Setting the System Date	10-2
Setting the System Time	10-2
Selecting the System Time Zone	10-3
Programming Primary and Secondary Languages	10-3
Programming Daylight Saving Time [British Summer Time]	10-3
Echo Profiles	10-5
Programming Echo Profiles for Trunks	10-5
Programming Echo Profiles for Endpoints	10-6
Voice Over Internet Protocol (VoIP) Echo Canceller	10-8
File-Based Music-On-Hold (MOH)	10-9
Creating File-Based MOH Profiles	10-11
Using a File-Based MOH Source	10-13
Page Zones	10-15
Viewing Page Zones	10-15
Deleting Page Zones	10-15
Planning a Page Zone	10-16
Programming Local Page Zones	10-16
Creating Remote Page Zones	10-17
Deleting Page Zones	10-17
Deleting Items from a Page Zone	10-17
Creating Off-Node Page Ports	10-18
Deleting Off-Node Page Ports	10-18
System Flags	10-19
Timers and Limits	10-24
Feature Codes	10-33
Trunk Access Codes	10-33
Endpoint Feature Codes	10-34
SIP and ITP Default Feature Codes	10-39
ITP Mode Feature Codes	10-40
Administrator Feature Codes	10-41
Diagnostics Mode Feature Codes	10-42

Voice Processor System Programming 11-1

Introduction	11-4
Program Planning Sheets	11-4
Mitel Voice Processing Systems	11-4
BVM – Enabling and Disabling	11-5
Voice Processor Nodes	11-6
Local Nodes	11-6
Remote Nodes	11-6
Creating a Remote Node	11-6
Programming Remote Node Options	11-7
Voice Profile for Internet Mail (VPIM) Networking	11-9
VPIM Messages	11-9
VPIM Programming	11-9
Network Settings	11-13
Timers and Limits	11-13
Validate Off-Node Mailboxes	11-15
Undeliverable Messages Destination Type	11-15
Voice Processor System Settings	11-16
Dial-0 Destinations	11-18
Total Storage Disk Usage Statistics	11-18
System Administrator Mailbox	11-18
VPIM Home Domain	11-19
Alternate Tone Detection	11-19
Volume	11-20
Save Message on Return Call	11-20
Swap “7 for Save” and “9 for Delete” Message Keys	11-21
Identification Prompt	11-21
Management Command and Event Ports	11-22
Automatic Speech Recognition Settings	11-23
E-Mail Retrieval Interval (minutes)	11-25
Monitor Password	11-25
BS-BVM System Recording Codec	11-26
Time Slot Groups	11-27
Changing Time Slot Descriptions	11-27
Changing Time Slot Maximum Channel Allocations	11-27
Voice Processor Applications	11-28
Creating Voice Processor Applications	11-28
Changing Multiple Application Extensions	11-28
Copying and Pasting Application Attributes	11-29

Auto Attendant	11-30
Auto Attendant Information	11-30
Enable Auto Attendant Directory	11-30
Auto Attendant Transfer Prompt	11-30
Auto Attendant Directory Sort Order	11-30
Auto Attendant Transfer Method	11-31
Auto Attendant Recall	11-31
Call Routing Announcements	11-32
Programming a Call Routing Announcement	11-33
Using Digit Translation	11-33
Using Digit Translation Nodes	11-36
Message Notification/Retrieval	11-37
Programming MNR Classes of Service	11-37
Deleting MNR Classes of Service	11-37
Record-A-Call	11-38
Scheduled Time-Based Application Routing (STAR)	11-39
Programming STAR Schedules	11-39
Programming the Default STAR Application	11-40
Programming Automatic Fax Detection for STAR Applications	11-41
Voice Mail (Application)	11-41
Voice Processing Application Options	11-42
Day and Night Greetings for Voice Processing Applications	11-43
Attendants for Voice Processing Applications	11-44
Music-On-Hold for Voice Processing Applications	11-44
Time Slot Group for Voice Processing Applications	11-45
Transfer Recall Destination for Voice Processing Applications	11-45
Automatic Speech Recognition (ASR) Setting	11-46
Automatic Speech Recognition (ASR) Enabled	11-46
Propagate Original Caller ID on Transfer	11-46
Calling Party Name and Number	11-46
Extension IDs	11-47
Group Lists	11-49
Creating a Group List	11-49
Changing a Group List Extension Number	11-49
Adding Mailboxes to Group Lists	11-49
Removing Mailboxes from Group Lists	11-50
Viewing Group List Members	11-50
Audiotex Recordings	11-51

Voice Mail Directory	11-52
Enabling or Disabling the Voice Mail Directory	11-52
Changing the Voice Mail Directory Sort Order	11-52
Voice Processor Timers and Limits	11-53
Programming BVM Timers and Limits	11-54
DTMF Detection Information	11-57
DTMF Generation Information	11-59
Number of Voice Channels	11-60
Unified Messaging with EM Options	11-61
E-Mail Gateway	11-62
E-Mail Gateway Programming Options	11-62
E-Mail Gateway for Mitel CS-5600 Systems	11-66
Fax-On-Demand	11-69
Fax-on-Demand Timers and Limits	11-69
Fax Documents	11-71
Allow International Calls	11-71
Outgoing Access	11-72
Start/Stop Time	11-72
Days of the Week	11-73
Fax Format	11-73

Subscriber Mailboxes 12-1

Introduction	12-3
Creating Mailboxes	12-3
Creating Mailboxes for Extensions with Extension IDs	12-3
Creating Associated Mailboxes	12-4
Creating Non-Associated Mailboxes	12-4
Changing Non-Associated Mailbox Extension Numbers	12-5
Deleting Mailboxes	12-5
Clearing Mailbox Messages	12-5
Copying Mailbox Settings	12-6
Network Mailboxes (Off-Node Mailboxes)	12-7
Remote Mailbox Extension	12-7
Unlisted Number and Private Mailbox Number Options	12-7

Programming Mailbox Options	12-8
Directory Information	12-9
Envelope Settings	12-10
Unified Messaging	12-11
Recording Length	12-15
Message Limits	12-15
Subscriber Statistics	12-16
E-mail Reader Profiles	12-17
Dial-0 Destinations	12-18
Remote Messaging	12-19
Primary and Alternate Message Notification	12-20
Mailbox Initialized	12-23
Receive Only	12-23
Allow Transfer Method Programming	12-23
Play Recording Instructions	12-23
Auto Attendant Transfer Prompt	12-24
Deliver Hangup Message (when ANI is available)	12-24
Swap “7 for Save” and “9 for Delete” Message Keys	12-25
Designate this Mailbox for Play Only	12-25
Password	12-26
Greeting	12-26
Transfer Method	12-27
Message Notification Endpoint	12-27
Time Zone	12-28
Automatic Speech Recognition (ASR) Setting	12-28
Automatic Speech Recognition (ASR) Enabled	12-28
Quota Warning	12-29
Quota Grace	12-29
Mailbox-Related Information	12-30

Voice Processing Management 13-1

Introduction	13-2
Enable Diagnostics	13-2
Saving and Restoring Voice Processing Databases	13-3
Summary of Voice Processor Save and Restore Options	13-3
Voice Processor Save and Restore	13-4
Voice Processor Save Guidelines	13-5
Save To or Restore To Location	13-5
Options	13-6
Completing the Save/Restore	13-7
Enabling or Disabling a Voice Processor	13-8
Saving a Voice Processor Database in Remote Mode	13-8
Selecting a Voice Processor Type in Local Mode	13-9
Saving or Restoring an EM Database	13-11
Saving or Restoring a CS-5600 Database on a Remote Windows Computer	13-15
Saving/Restoring Mitel CS-5600 BVM Data	13-19
Save/Restore BVM Data to a Network File Server (NFS)-Supported Computer	13-20

Database Utilities 14-1

Introduction	14-2
MOH Converter Utility	14-3
DB Test and Repair Utility	14-7
Database Test and Repair Menus	14-8
DB Test Toolbar Icons	14-8
DB Test Guidelines	14-9
Database Test Options	14-9
DB Test Common Error Results	14-10
DB Tests	14-10
Upload Utility	14-21
Database Converter Utility	14-23
Conversion Notes	14-23
Mitel 5000 Database Conversions	14-24

System and Enterprise Messaging Reports 15-1

Introduction	15-2
System Reports	15-3
System Report Types	15-3
Programming a System Report	15-4
Printing System Reports	15-5
Enterprise Messaging Voice Processing Reports	15-6
Report Parameters	15-6
Report Options	15-6
Using Automatic Report Generation	15-8
Using Manual Report Generation	15-10

System Diagnostics 16-1

Introduction	16-3
Digital Trunk Diagnostics	16-3
Database Test and Repair Utility	16-3
Busy Out Manager	16-4
Database Change Log	16-6
General Guidelines	16-6
How to Read the Database Change Log	16-7
Audio Diagnostics	16-19
Network Group Diagnostics	16-24
Oversubscription/IP Resource Sharing Statistics	16-24
IP Resource Sharing Log File	16-25
Hybrid Balance Test	16-26
Improved Hybrid Balance Line Settings	16-26
Hybrid Balance Test Options	16-27
Running a Hybrid Balance Test	16-27
Viewing Hybrid Balance Test Results in Message Print	16-29
Viewing Hybrid Balance Results	16-31
Manually Changing the Hybrid Balance Setting	16-32
Alarms	16-33
Alarm Types	16-33
Network Alarms	16-34
Displaying Alarms	16-34
Alarm Queue	16-35
Clearing an Alarm	16-36
Responding to a Major Alarm	16-36

Diagnostics Through DB Programming	16-37
Automatic Diagnostics Delivery	16-37
System Device Information	16-37
Database Operations	16-41
Voice Processing Diagnostics	16-42
Other Diagnostic Features	16-43
Administrator Endpoint Support	16-43
Diagnostics Feature Codes	16-43
Online Monitor Command Line	16-46
LCD Panel Diagnostic Options	16-47
Resource Manager CPH Diagnostics Flag	16-48
Call Processing History (CPH) Freeze File Compression	16-48
History Queues/Log Files – Clearing	16-48
Traceroute	16-48
External Diagnostic Resources	16-49
Administrative Web Session	16-49
System Manager	16-49
Raw Commands	16-49
Troubleshooting	17-1
Introduction	17-3
Troubleshooting Methodology	17-3
Troubleshooting Processes	17-5
Preliminary Activities	17-5
System Reset Analysis	17-6
Troubleshooting Guidelines	17-6
Hot-Swapping an Expansion Module	17-7
Call Flow	17-8
Network Diagram	17-9
Troubleshooting Charts	17-10
99 Nodes Support	17-11
Administrative Web Session	17-12
Basic Voice Mail	17-12
Caller ID Forwarding	17-13
Caller ID Propagation	17-14
CO [Local Exchange] Trunks	17-16
Database Change Log	17-20
Digital Endpoint Interface	17-20
Endpoints	17-21
Expansion Modules	17-27

Contents

File-Based MOH	17-28
Four-Port Single Line Module	17-29
Import Endpoints from CSV Files	17-30
IP Resource Application (IPRA)	17-32
IP Devices	17-32
IP Device Audio	17-35
IP Device Connection	17-36
IP Device Echo	17-38
IP Device VLAN Tagging	17-40
IP Networking	17-41
Licensing Issues	17-45
Loop Loss Measurement	17-45
Mini-DSS Unit	17-46
Multi-Protocol Endpoints	17-47
Network Node	17-51
Oversubscription/IP Resource-Sharing	17-52
Persistent Music-On-Hold Selection	17-53
Phantom Devices	17-54
Processor Module (PM-1)	17-56
Processing Server (PS-1)	17-57
Retry ARS Call If Call Rejected	17-58
Scheduled Backups – Warnings and Error/Failure Reasons	17-58
Scheduled Backups – Error Messages	17-65
Scheduled Backups – General Troubleshooting Tips	17-68
Single Line Endpoints	17-70
System Health Report	17-73
System Features	17-73
System-Level Issues	17-77
T1/E1/PRI Modules	17-80
Upgrade Process	17-82
UPS Monitoring	17-83
Voice Processing	17-83
VoIP Echo Canceller Troubleshooting	17-87
VPIM Networking	17-88
Customer Support	17-89
Technical Support	17-89
Emergency Assistance	17-89
Defective Equipment Return Policy	17-89

Index

I-1

Tables

Table 2-1	Toolbar Buttons	2-14
Table 2-2	Keystrokes for Navigating without a Mouse.	2-18
Table 3-1	Software License Descriptions	3-7
Table 3-2	Voice Data Save Locations	3-22
Table 4-1	Node Status Descriptions	4-21
Table 4-2	Example of Exporting an Extension from One Node to Another	4-22
Table 5-1	NANP and Overlap Flag Differences.	5-4
Table 5-2	Route Group Dial Patterns for U.S. Systems	5-18
Table 5-3	Route Group Dial Patterns for European Systems	5-18
Table 5-4	Toll String Wildcards for U.S. systems	5-23
Table 5-5	Toll String Wildcards for European Systems	5-23
Table 5-6	Special Characters for Dialing Patterns.	5-24
Table 6-1	Trunk Types and Feature Options.	6-11
Table 6-2	Call Routing Table Pattern Characters	6-24
Table 6-3	An Example of the Music-On-Hold (MoH) Profiles for Chained CRTs.	6-29
Table 6-4	AC Impedance Settings by Country.	6-33
Table 7-1	Substrings and Headers	7-8
Table 7-2	Endpoint Flags.	7-23
Table 7-3	DSS Button Types and Descriptions	7-46
Table 7-4	User-Keyed Extension Examples for Agent Help	7-52
Table 7-5	Call Logging Options and Descriptions	7-54
Table 7-6	Record-A-Call Operation	7-58
Table 7-7	Account Codes Available for U.S. and Europe	7-69
Table 7-8	Default DND Messages	7-72
Table 7-9	Default Reminder Messages	7-73
Table 9-1	IP Device Status Dialog Descriptions – License Category	9-4
Table 9-2	General IP Settings Fields.	9-7
Table 9-3	Base Server/Processing Server Connection Settings Fields.	9-11
Table 9-4	Web/SSH Settings Fields	9-13
Table 9-5	TFTP Settings Fields	9-14
Table 9-6	Advanced IP Settings Fields	9-15
Table 9-7	NTP Server Configuration Fields.	9-16
Table 9-8	Audio Stream Receive Port Ranges and Default Values.	9-19
Table 9-9	Reserved By Function Fields.	9-45

Tables

Table 9-10	Resource Types	9-49
Table 10-1	Trunk Echo Profiles	10-5
Table 10-2	Default Echo Profiles for Devices	10-7
Table 10-3	MOH Audio File Formats for Conversion.	10-9
Table 10-4	Other File Formats in the MOH Converter Utility.	10-10
Table 10-5	File-Based MOH Option Fields	10-13
Table 10-6	System Flags.	10-19
Table 10-7	System Timers.	10-24
Table 10-8	Trunk Access Codes	10-33
Table 10-9	Endpoint Feature Codes	10-34
Table 10-10	SIP and ITP Mode Functions for Show IP Feature	10-39
Table 10-11	SIP Default Feature Codes	10-39
Table 10-12	Inter-Tel Protocol IP Default Feature Codes	10-40
Table 10-13	System Administrator Default Feature Codes	10-41
Table 10-14	Diagnostics Mode Default Feature Codes.	10-42
Table 11-1	Sample Speech Recognition Combinations	11-23
Table 11-2	Transfer Destination Actions	11-35
Table 11-3	Voice Mail Application Programming Fields	11-42
Table 11-4	Voice Processor Timers and Limits	11-54
Table 11-5	E-Mail Gateway Fields Used for System Features	11-62
Table 12-1	Unified Messaging Levels for BVM and EM	12-11
Table 12-2	Programmable Fields for the Unified Messaging Folder	12-12
Table 13-1	Voice Processor Database Save/Restore Options	13-3
Table 13-2	Valid Characters for Path and Hostname Entries	13-11
Table 14-1	Database Test and Repair Utility File Menu Options.	14-8
Table 14-2	Database Test and Repair Utility Test Menu Options	14-8
Table 14-3	Database Test and Repair Toolbar Icon Shortcuts	14-8
Table 14-4	Database Test and Repair Utility Common Errors.	14-10
Table 14-5	DB Test and Repair Error Messages for Associated Mailboxes	14-11
Table 14-6	DB Test and Repair Error Messages for Modules.	14-12
Table 14-7	DB Test and Repair Error Messages for Devices	14-13
Table 14-8	DB Test and Repair Error Messages for Dynamic Enumerations	14-15
Table 14-9	DB Test and Repair Error Messages for Enumerations	14-16
Table 14-10	DB Test and Repair Error Messages for Extension Conflicts	14-16
Table 14-11	DB Test and Repair Error Messages for Hardware Addresses.	14-17
Table 14-12	DB Test and Repair Error Messages for Miscellaneous	14-18

Table 14-13	DB Test and Repair Error Messages for Referential Integrity	14-19
Table 14-14	DB Test and Repair Error Messages for Static Records	14-20
Table 16-1	Busy Out Statuses	16-5
Table 16-2	Audio Problem Codes	16-21
Table 16-3	EIA Standard Loop Length Line Settings and Descriptions.	16-26
Table 16-4	Alarms and Priorities	16-35
Table 16-5	Database Query Options	16-39
Table 16-6	Diagnostics Feature Codes	16-43
Table 17-1	Call Flow Troubleshooting Considerations	17-8
Table 17-2	99 Nodes Support Troubleshooting Issues	17-11
Table 17-3	Administrative Web Session Troubleshooting Strategies	17-12
Table 17-4	Basic Voice Mail Troubleshooting Strategies	17-12
Table 17-5	Caller ID Forwarding Support Troubleshooting Issues	17-13
Table 17-6	Caller ID Propagation Support Troubleshooting Issues.	17-14
Table 17-7	CO Trunk Troubleshooting Strategies	17-16
Table 17-8	Database Change Log Troubleshooting Issues.	17-20
Table 17-9	DEI Troubleshooting Strategies.	17-20
Table 17-10	Endpoint Troubleshooting Strategies.	17-21
Table 17-11	Expansion Module Troubleshooting Strategies	17-27
Table 17-12	File-Based MOH Troubleshooting Issues	17-28
Table 17-13	Single Line Module (SLM-4) Troubleshooting Strategies	17-29
Table 17-15	IP Endpoint System Limit.	17-30
Table 17-14	Import Endpoints from File Troubleshooting Strategies.	17-30
Table 17-16	IPRA Troubleshooting Strategies	17-32
Table 17-17	IP Devices Troubleshooting Strategies	17-32
Table 17-18	IP Device Audio Troubleshooting Strategies	17-35
Table 17-19	IP Device Connection Troubleshooting Strategies	17-36
Table 17-20	IP Device Echo Troubleshooting Strategies	17-38
Table 17-21	IP Device VLAN Tagging-Related Troubleshooting Strategies	17-40
Table 17-22	IP Networking Troubleshooting Strategies	17-41
Table 17-23	Licensing Troubleshooting Strategies	17-45
Table 17-24	Loop Loss Measurement Troubleshooting Issues.	17-45
Table 17-25	Mini-DSS Unit Troubleshooting Strategies	17-46
Table 17-26	Multi-Protocol Endpoint Troubleshooting Strategies	17-47
Table 17-27	Network Node Troubleshooting Chart	17-51
Table 17-28	Oversubscription/IP Resource-Sharing Troubleshooting Strategies	17-52

Tables

Table 17-29	Persistent Music-On-Hold Troubleshooting Issues	17-53
Table 17-30	Phantom Devices Troubleshooting Strategies.	17-54
Table 17-31	Processor Module (PM1) Modem Troubleshooting Strategies	17-56
Table 17-32	Processing Server Troubleshooting Strategies	17-57
Table 17-33	Retry ARS Call If Call Rejected Troubleshooting Strategies	17-58
Table 17-34	Voice Data Backup Failed Reasons	17-59
Table 17-35	Error/Failure Reasons and Troubleshooting Tips	17-61
Table 17-36	Scheduled Backups Error Messages and Troubleshooting Tips	17-65
Table 17-37	Scheduled Backups Troubleshooting Tips	17-68
Table 17-38	Single Line Endpoint Troubleshooting Strategies	17-70
Table 17-39	System Health Report Troubleshooting Issues	17-73
Table 17-40	System Features Troubleshooting Strategies	17-73
Table 17-41	System-Level Troubleshooting Strategies.	17-77
Table 17-42	T1/E1/PRI Troubleshooting Strategies	17-80
Table 17-43	Upgrade Process Troubleshooting Strategies.	17-82
Table 17-44	Troubleshooting Strategies for UPS Monitoring Issues	17-83
Table 17-45	Voice Processing Troubleshooting Strategies.	17-83
Table 17-46	VoIP Echo Canceller Troubleshooting Tips.	17-87
Table 17-47	VPIM Troubleshooting Strategies	17-88

Figures

Figure 1-1	Network Type.	1-11
Figure 1-2	Network Type.	1-12
Figure 1-3	Access Rights Dialog Box	1-13
Figure 2-1	Session Manager.	2-4
Figure 2-2	PPP IP Address Location	2-11
Figure 2-3	DB Studio.	2-12
Figure 2-4	Inactivity Messages	2-15
Figure 2-5	Selection Wizard	2-16
Figure 2-6	Description Column	2-17
Figure 2-7	Folder Name with Description	2-17
Figure 3-1	Password Directory	3-4
Figure 3-2	Software License Directory Display	3-6
Figure 3-3	About Software License.	3-9
Figure 3-4	Backup Database Parameters.	3-12
Figure 3-5	Scheduled Backups Summary.	3-16
Figure 3-6	System Database Files	3-21
Figure 3-7	Scheduled Backups History.	3-28
Figure 3-8	Reason Dialog Box	3-29
Figure 3-9	Sample Service Log.	3-32
Figure 3-10	System Maintenance	3-36
Figure 3-11	PS-1 System Health Report Information	3-41
Figure 3-12	Base Server System Health Report Information	3-42
Figure 3-13	Remote Configuration Wizard Check Box	3-54
Figure 4-1	DB Programming Local and Remote Nodes	4-2
Figure 4-2	Networking Wizard.	4-6
Figure 4-3	DB Programming Local and Off-Node Modems	4-23
Figure 5-1	Numbering Plan Options	5-3
Figure 5-2	Device Baseline Extensions	5-9
Figure 6-1	Trunks Location	6-4
Figure 6-2	Trunk Options (Loop Start Trunk)	6-11
Figure 6-3	System Call Routing Tables	6-22
Figure 6-4	Loop Loss Measurement Test Results	6-31
Figure 7-1	Create IP Device Options	7-6
Figure 7-2	Off-Node Device Options.	7-13

Figures

Figure 7-3	Default Keymap	7-27
Figure 7-4	Keymap Type Column	7-40
Figure 7-5	Programmable Keys	7-42
Figure 7-6	Keymap Group Location	7-49
Figure 7-7	Endpoint Options	7-50
Figure 8-1	Extension Lists	8-4
Figure 8-2	CO Trunk Groups	8-7
Figure 8-3	CO Trunk Group Options	8-11
Figure 8-4	Hunt Group and Options	8-32
Figure 8-5	Local Hunt Group Options	8-37
Figure 8-6	Node IP Connection Groups	8-54
Figure 9-1	Get IP Device Status	9-5
Figure 9-2	General IP Settings	9-6
Figure 9-3	Local Processor Module and Expansion Card IP Settings	9-17
Figure 9-4	IP Network Off-Node Connections	9-21
Figure 9-5	Call Configuration Options	9-24
Figure 9-6	Socket Options	9-34
Figure 9-7	Endpoint IP Settings	9-36
Figure 9-8	Reserved By Function Tab	9-44
Figure 9-9	Reserved By Device Tab	9-47
Figure 9-10	Resource Reservations Advanced Tab	9-48
Figure 10-1	System-Wide Parameters	10-2
Figure 10-2	VoIP Echo Canceller Setting	10-8
Figure 10-3	Local and Remote Page Zones	10-15
Figure 11-1	Network Settings	11-13
Figure 11-2	Voice Processor System Settings	11-17
Figure 11-3	Voice Processor Timers and Limits	11-53
Figure 11-4	E-Mail Gateway	11-66
Figure 11-5	E-Mail Gateway for SMTP	11-67
Figure 12-1	Mailbox Options	12-9
Figure 12-2	Remote Messaging Routing Example	12-19
Figure 13-1	Voice Processor Save/Restore Dialog Boxes	13-4
Figure 13-2	Database Save — Voice Processor	13-11
Figure 13-3	NFSD Process	13-20
Figure 14-1	Database Utility Menu	14-2
Figure 14-2	DB Programming Installation Wizard	14-3

Figure 14-3	Database Utilities Menu.	14-3
Figure 14-4	DB Test Dialog Box	14-7
Figure 15-1	Report Programming Location in DB Programming	15-2
Figure 15-2	EM Report Parameters	15-6
Figure 16-1	Busy Out Manager.	16-4
Figure 16-2	Busy Out Manager Programming	16-4
Figure 16-3	Audio Diagnostics Options.	16-20
Figure 16-4	Hybrid Balance Line Setting	16-32
Figure 16-5	Example of Get IP Device Status Window.	16-42
Figure 17-1	Troubleshooting Process Flow Diagram	17-3
Figure 17-2	Network Diagram Example	17-9

New Features

Introduction	1-3
New Features and System Changes Described in This Book	1-3
New Features for Hardware and Installation	1-3
Mitel Cordless Devices	1-3
Mitel 5000 v3.0 New Features in DB Programming	1-4
System Management	1-4
Trunks	1-4
Endpoints and Devices	1-4
Lists and Groups	1-4
IP Settings and Devices	1-5
System Settings	1-5
Voice Processor System Programming	1-5
Subscriber Mailboxes	1-5
Database Utilities	1-6
Diagnostics	1-6
Troubleshooting	1-6
Mitel NuPoint Messenger	1-6
SIP Peer Voice Mail	1-7
SIP Peer Operating State	1-7
SIP Peer Status	1-7
SIP Peer Keep Alive Functionality	1-7
SIP View Diagnostics Feature Code 9987 [9187]	1-8
New Dumps for SIP Peers in System Monitor	1-8
SIP Log Files Diagnostics	1-8
SIP Mailboxes	1-8
New Alarms and Messages	1-9
Licenses	1-9
OAI Caller ID Control	1-9
DB Programming Changes	1-10
General DB Programming Application Changes	1-10
DB Programming Supported Operating Systems	1-10
Mapped Devices No Longer Supported	1-10
Fax Encoding Setting Removal	1-10
License Changes	1-10
Session Manager	1-11

Voice Processing Changes	1-11
Voice Processor\Devices\Nodes	1-11
Voice Processor\Timers and Limits	1-12
Voice Processor\Devices\Applications	1-12
Voice Processor\Devices\Nodes	1-12
E-Mail Gateway	1-12
Call Configurations	1-12
Passwords\Edit Access Rights	1-13
New Features in Administrative Web Session (AWS)	1-14
New AWS Pages	1-14
System SIP Diagnostics Page	1-14
SIP Peer Diagnostics Page	1-16
Trunk Diagnostics Page	1-16
MOH Files Page	1-17
Modified AWS Pages	1-18
Home Page	1-18
Network Page	1-18
IP Resource Diagnostics Page	1-18
IPDRM Resource Diagnostics Page	1-18
Log Files Page	1-19
Application Logging Options Page	1-19
Onboard Modem Page	1-19
Digital Endpoint Interface Page	1-19
Session Information Details Page	1-19

Introduction

NOTE

The Inter-Tel 5000 system has been rebranded as the Mitel 5000 system. Over time, the supporting materials related to this product line will also be rebranded to reflect this name change.

This chapter lists new features related to the Mitel 5000 version 3.0 Database (DB) Programming application. This includes features used to complete system configuration and perform system adds, moves, and changes *after the system is installed*. For information about new features related to system hardware, licensing, or upgrades, refer to the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

Mitel 5000 system documentation includes the following resources:

- *Mitel 5000 Features and Programming Guide* (this book), part number 580.8006
- *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000
- *Mitel 5000 Reference Manual*, part number 580.8007 (new)
- *Mitel 5000 DB Programming Help*
- *Mitel 5000 Endpoint and Voice Mail Administrator Guide*, part number 580.8001

For additional system documentation, refer to the “Documentation” folder of the system software CD. You can also find all documentation on the [edGe Online Manuals and Guides Web site](http://www.inter-tel.com/techpublications) (www.inter-tel.com/techpublications).

New Features and System Changes Described in This Book

The following sections describe new features or system changes in this book:

- “Mitel 5000 v3.0 New Features in DB Programming” on [page 1-4](#)
- “Mitel NuPoint Messenger” on [page 1-6](#)
- “New Alarms and Messages” on [page 1-9](#)
- “OAI Caller ID Control” on [page 1-9](#)
- “DB Programming Changes” on [page 1-10](#)
- “New Features in Administrative Web Session (AWS)” on [page 1-14](#)

New Features for Hardware and Installation

Mitel 5000 version 3.0 includes the following new hardware and licensing features.

- Expanded DEI Capacity
- IP Enabler Unit License
- Liquid Crystal Display (LCD) Application Enhancements
- BVM Ports Capacity Increase

For more information about these features, refer to the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

Mitel Cordless Devices

The Mitel Models 5330 and 5340 endpoints now support a cordless handset and cordless headset. For more information, refer to the *Mitel Model 5330/5340 IP Endpoint User Guide*, part number 550.8123.

Mitel 5000 v3.0 New Features in DB Programming

NOTE

Throughout the book, version 3.0 new features or options are indicated by change bars, like the one shown in the margin to the left of this text.

Mitel 5000 v3.0 DB Programming includes the following new features, listed by chapter:

System Management

The following are new features and options system management:

- “Scheduled Backups” on [page 3-15](#)
- “System Health Report” on [page 3-40](#) (*reserved for controlled introduction*)
- “Display “T” for Two B-Channel Transferred Calls” on [page 3-52](#)

Trunks

The following are new features and options for trunks:

- “Persistent Music-On-Hold Selection” on [page 6-29](#)
- “Loop Loss Measurement Test” on [page 6-31](#)
- “ISDN PRI Two B-Channel Transfer” on [page 6-34](#)

Endpoints and Devices

The following are new features and options for endpoints and devices:

- “Creating Endpoints from CSV Files” on [page 7-8](#)
- “Propagate Original Caller ID on Transfer” on [page 7-26](#)
- “Calling Party Name” on [page 7-63](#)
- “Calling Party Number” on [page 7-64](#)
- “Emergency Party Calling Number” on [page 7-64](#)

Lists and Groups

The following are new features and options for lists and groups:

- “Send Station Caller ID to Attached PBX” on [page 8-26](#)
- “Propagate Original Caller ID” on [page 8-26](#)
- “Calling Party Name” on [page 8-26](#)
- “Calling Party Number” on [page 8-26](#)
- “Force Trunk Group Calling Party Name and Number” on [page 8-27](#)
- “Wait for ISDN Caller ID Information” on [page 8-27](#)

IP Settings and Devices

The following are new features and options for IP settings and devices:

- “Domain Name” on [page 9-9](#)
- “SIP Voice Mails for Call Configurations” on [page 9-26](#)
- “Fax Control-Messages Redundancy Count” on [page 9-31](#)
- “Fax Detection Sensitivity” on [page 9-31](#)
- “Fax Encoding Setting (Fax Transmission)” on [page 9-32](#)
- “Fax Maximum Connection Speed” on [page 9-32](#)
- “Supports RTP Redirect” on [page 9-33](#)

System Settings

The following are new features and options for system settings:

- “File-Based Music-On-Hold (MOH)” on [page 10-9](#)
- “Voice Over Internet Protocol (VoIP) Echo Celler” on [page 10-8](#)

Voice Processor System Programming

The following are new features and options for voice processing system programming:

- “Mitel NuPoint Messenger” on [page 1-6](#)
- “Voice Profile for Internet Mail (VPIM) Networking” on [page 11-9](#)
- “VPIM Home Domain” on [page 11-19](#)
- “Swap “7 for Save” and “9 for Delete” Message Keys” on [page 11-21](#)
- “BS-BVM System Recording Codec” on [page 11-26](#)
- “Propagate Original Caller ID on Transfer” on [page 11-46](#)
- “Calling Party Name and Number” on [page 11-46](#)
- “DTMF Generation Information” on [page 11-59](#)
- “Select the appropriate document (or None), and then click Finish. The selection appears in the Logo Document field.” on [page 11-73](#)

Subscriber Mailboxes

The following are new features and options for mailboxes:

- “Swap “7 for Save” and “9 for Delete” Message Keys” on [page 12-25](#)
- “Designate this Mailbox for Play Only” on [page 12-25](#)

Database Utilities

The “MOH Converter Utility” on [page 14-3](#) was added in v3.0 to support File-Based Music-On-Hold.

Diagnostics

The following are new features and options for diagnostics:

- “Database Change Log” on [page 16-6](#)
- Hybrid Balance Test improvements on [page 16-26](#)

Troubleshooting

The following are troubleshooting sections for v3.0 new features:

- “Persistent Music-On-Hold Selection” on [page 17-53](#)
- “Caller ID Forwarding” on [page 17-13](#)
- “I” on [page 17-16](#)
- “File-Based MOH” on [page 17-28](#)
- “Database Change Log” on [page 17-20](#)
- “System Health Report” on [page 17-73](#)
- “Import Endpoints from CSV Files” on [page 17-30](#)
- “VoIP Echo Cancellor Troubleshooting” on [page 17-87](#)
- “Scheduled Backups – Warnings and Error/Failure Reasons” on [page 17-58](#)
- “Scheduled Backups – Error Messages” on [page 17-65](#)
- “Scheduled Backups – General Troubleshooting Tips” on [page 17-68](#)

Mitel NuPoint Messenger

Mitel 5000 systems now support NuPoint Messenger, an external voice processing system that resides on the Mitel Application Suite® (MAS) server and uses Session Initiation Protocol (SIP) to communicate with the Mitel 5000 system. Mitel 5000 systems support NuPoint Messenger as the system voice processing application. For more information, refer to the following resources:

- *Mitel 5000 and NuPoint Messenger Integration Guide*, part number 580.8008
- *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000
- *Mitel 5000 DB Programming Help*
- *NuPoint Messenger Technical Documentation Help*

Mitel 5000 v3.0 DB Programming now includes SIP Voice Mail features (see [page 1-7](#)), which are required to integrate NuPoint Messenger with the Mitel 5000.

SIP Peer Voice Mail

SIP Peer Voice Mail provides access to a SIP messaging system. The following sections describe new SIP Peer Voice Mail options for v3.0. SIP voice mail options are located in System\Devices and Feature Codes\SIP Peers\SIP Voice Mails\<extension>.

SIP Peer Operating State

A SIP peer has an operating state that provides its availability. The SIP peer operating states are:

- **In Service (INS):** The SIP peer is available and in service.
- **Out-of-Service (OOS):** The SIP peer is temporarily unavailable. The SIP peer reaches this state due to one of the following reasons:
 - The outgoing call attempts failed consecutively for a configured number (Call Failure Threshold) of times.
 - The ping requests (SIP OPTIONS) timed out or failed for a configured number (Ping Failure Threshold) of times.
- **Out-of-Service-Maintenance (OOS-Maint):** The administrator manually put the SIP peer out of service to do maintenance.

Alarm 145 (SIP Peer Out-of-Service) generates when a SIP peer state changes from INS to OOS. This alarm clears automatically when the SIP peer state changes from OOS or OOS-Maint to INS.

SIP Peer Status

A SIP peer reports its status to any monitoring device. Each status includes the light-emitting diodes (LED) flash rate associated with a Direct Station Select (DSS)/Busy Lamp Field (BLF) button programmed for the corresponding SIP peer. The SIP peer statuses are:

- **Idle:** The operating state is INS and there is at least one available trunk or port for placing an outgoing or incoming call. The flash rate is off.
- **Busy:** The operating state is INS and there are no available trunks or ports for placing an outgoing or incoming call. The flash rate is solid.
- **Offline:** The operating state is OOS or OOS-Maint. The flash rate is solid.

SIP Peer Keep Alive Functionality

The SIP peer has keep alive functionality to refresh the NAT bindings for any firewall/NAT in the path and to determine if the SIP peer is reachable or not. You can enable or disable the SIP peer keep alive functionality in DB Programming for each SIP peer. When you enable the keep alive functionality, the Mitel 5000 system sends a SIP OPTIONS request to ping the SIP peer. When you disable the keep alive functionality, the Mitel 5000 does not send any SIP OPTIONS requests to the SIP peer.

If the SIP OPTIONS requests fail consecutively for a configured number of times, then the SIP peer changes to the OOS state and alarm 145 (SIP Peer Out-of-Service) generates. When subsequent SIP OPTIONS requests are successful, then the SIP peer state changes to INS and Alarm 145 (SIP Peer Out-of-Service) generates.

SIP View Diagnostics Feature Code 9987 [9187]

Use the existing diagnostics feature code 9987 [9187] “Diagnostics – SIP View” to view the incoming and outgoing SIP peer messages. This feature exists today for SIP trunks. This diagnostic code changes the SIP values system-wide which determines the output that appears in Message Print and diagnostic log files.

To change the SIP values system-wide through the administrator endpoint:

1. From an Administrator endpoint, dial feature code **9987 [9187]** to access the Diagnostics – SIP View feature.
2. Select an output from the following options:
 - No Output (OFF)
 - Headers (HEAD)
 - Full Output (FULL)

New Dumps for SIP Peers in System Monitor

New dumps are included with v3.0 in System Monitor:

- **Dump SIP Dialog Manager:** Contains information and statistics about SIP dialogs. You can also get these statistics from the Administrative Web Session Web page (for details, see “System SIP Diagnostics Page” on [page 1-14](#).)
- **Dump SID:** Contains dynamic information about a particular active SIP call. The extension number for each SIP call is a random non-dialable extension that you obtain by first performing a Dump Call Manager during the active call. After you obtain the extension for the current call, you can perform Dump Extension to get the SID information.
- **Dump SIP Peer:** Contains information about the SIP Peer, such as the IP address, UDP port number, host name, etc.

The Endpoint Administrator can use the existing diagnostics feature code 9933 (Diagnostics – Dump Extension) to perform these dumps.

SIP Log Files Diagnostics

The Log Files page now includes diagnostic log files for SIP Peers: CP SIP and CP History. The CP SIP log file includes SIP message and SIP peer information. The CP History log file includes SIP peer message information depending on the SIP View option (see “SIP View Diagnostics Feature Code 9987 [9187]” on [page 1-8](#)).

SIP Mailboxes

Because DB Programming does not provision NuPoint Messenger, it now manages associated and non-associated mailboxes differently than software versions earlier than v3.0. You now manage mailboxes in a new area of DB Programming.

In DB Programming you can equip a mailbox for an endpoint, off-node endpoint, hunt group, or off-node hunt group. Also, in DB Programming you can associate a non-associated mailbox to a newly-equipped endpoint, off-node endpoint, hunt group, or off-node hunt group.

Non-associated mailboxes that you create on the Mitel 5000 represent virtual mailboxes on NuPoint Messenger to track the use of the non-associated mailbox extensions. There is no way to configure associated or non-associated mailboxes on NuPoint Messenger. A device extension number cannot overlap with a non-associated mailbox extension.

New Alarms and Messages

There are new system alarms and messages for v3.0. For more information, refer to the *Message Print Diagnostics Manual*, part number 550.8018.

Licenses

The following are v3.0 new licenses:

- **Digital Expansion Interface # 3:** Indicates whether the Digital Expansion Interface # 3 software license is uploaded to the system.
- **Digital Expansion Interface # 4:** Indicates whether the Digital Expansion Interface # 4 software license is uploaded to the system.
- **File-Based MOH Sources:** Indicates how many File-Based MOH sources are uploaded to the system.
- **System IP Endpoint Capacity:** Indicates the maximum capacity for IP endpoints on the system (5200 - 75, 5400 -175, 5600 -250). If you do not have the IP Endpoints Enabled license, the System IP Endpoint Capacity corresponds to the number of Enable IP Endpoint Units license in the license generator. The System IP Endpoint Capacity value is determined in the following manner:
 - If the IP Endpoints Enabled license is enabled, the System IP Endpoint Capacity is either 75, 175, or 250 (depending on the system type 5200, 5400, or 5600 respectively).
 - If the IP Endpoints Enabled license is disabled, the System IP Endpoint Capacity is the lesser of the Enable IP Endpoint Units license (in the license generator) or the total of all category licenses.
- **System Health Report:** Indicates whether the System Health Report software license is uploaded to the system.
- **SIP Voice Mail Ports:** Indicates how many SIP Peer Voice Mail Ports licenses are uploaded to the system.

OAI Caller ID Control

System OAI Level 2 Toolkit v9.3 has been enhanced to support Caller ID Forwarding by adding the <Caller_ID_Number> and <Caller_ID_Name> fields to the syntax of the command string. For details, refer to the *System OAI Toolkit Specifications Manual, Issue 9.3*, July 2007, document part number, 835.2615.

DB Programming Changes

The following are Mitel 5000 v3.0 DB Programming changes.

- “General DB Programming Application Changes” below
- “Licenses” on [page 1-9](#)
- “Voice Processing Changes” on [page 1-11](#)
- “E-Mail Gateway” on [page 1-12](#)
- “Call Configurations” on [page 1-12](#)
- “Passwords\Edit Access Rights” on [page 1-13](#)
- “New AWS Pages” on [page 1-14](#)

General DB Programming Application Changes

The following sections describe general DB Programming changes.

DB Programming Supported Operating Systems

DB Programming continues to be installed on Windows computers as it has in the past. The only OS types that are currently supported by DB Programming are Windows XP and Windows Vista.

Mapped Devices No Longer Supported

DB Programming no longer supports using mapped drives. This includes manually mapping, automatically mapping, and also using “subst” to assign a drive letter to a folder path. All paths should be referenced via complete URL (for example, \\server\folder).

Fax Encoding Setting Removal

The Fax Encoding Setting (Fax Detection) option was removed from the IP Call Configuration folder for each IP Connection Group because the Mitel 5000 system does not support this functionality. The option was located under System/Devices and Feature Codes/Node IP Connection Groups/IP Call Configuration.

License Changes

The following changes are made in this release:

- **Voice Processor Messaging Networking:** This license name has changed from “Inter-Tel Messaging IP Networking.”
- **Voice Processor AMIS Networking:** This license was removed because AMIS networking was supported by VPU systems only.

The following entries have been added to the About Inter-Tel Software License dialog box:

- **File-Based MOH Licenses In Use:** The total number of licenses available for the File-Based MOH licenses that are currently consuming a license. This field is in the format XX of YY where XX indicates the number of licenses currently in use and YY indicates the total number of licenses available.
- **SIP Voice Mail Licenses In Use:** The total number of licenses available for the SIP Voice Mail licenses that are currently consuming a license. This field is in the format XX of YY where XX indicates the number of licenses currently in use and YY indicates the total number of licenses available.

Session Manager

Session Manager connection options were changed to support the following features:

- **Scheduled Backups** (see [page 3-15](#)): Allows periodic, automatic backups of the system database and voice mail.
- **Connection Log**: Allows you to store information for one node in each connection log.
- **Database Change Log** (see [page 16-6](#)): Provides details on user changes to DB Programming.

See “Session Manager Connection Tabs” on [page 2-7](#) for more information.

Voice Processing Changes

The following changes apply to voice processing options.

NOTICE

Voice Processing Unit (VPU) end of sale. VPU is no longer supported in v3.0. The VPU was discontinued in May 2007 and has reached its end of sale. Mitel recommends that current VPU installations upgrade to either Enterprise® Messaging (EM) or NuPoint Messenger. The two EM hardware platforms currently available, Base I and Base II, are separate system components and must be purchased from your local provider. Instructions for converting a VPU database to an EM database are included in the *Enterprise Messaging Installation and Maintenance Manual*, part number 780.8006. You cannot convert a VPU database to an NuPoint Messenger database. Contact your local provider for more information.

The discontinuation of VPU affected the following voice processing features and options:

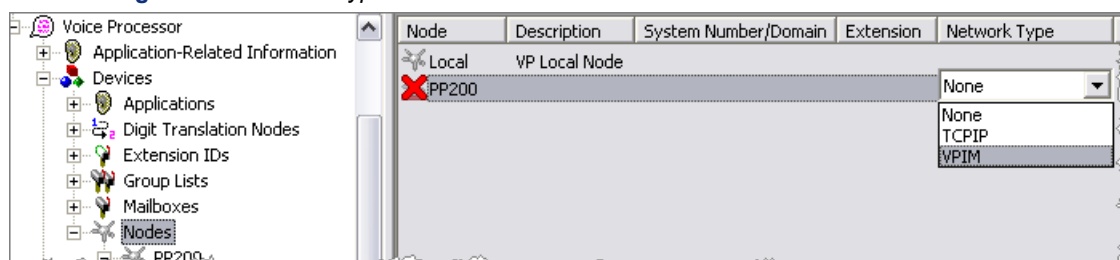
- The Accept AMIS Calls option has been removed from a Call Routing Announcement application because AMIS is only supported by the VPU. The VPU is no longer supported in the 3.0 release.
- The E-mail, AMIS, and ESMTP protocols are no longer supported and have been removed from the list. The Dial-Up Phone Number, Dial-Up Username, and Dial-Up Password fields in Voice Processor\Devices\Nodes\<node> have been removed because these fields apply to VPU AMIS only.
- The Windows Networking Username, Windows Networking Domain, and Windows Networking Password fields in Voice Processor have been removed because these fields apply to VPU only.

Voice Processor\Devices\Nodes

The networking options for EM are None, TCPIP and VPIM. The networking options for BVM are None, and VPIM.

Also, the System Number column has been renamed to System Number/Domain. The Domain name applies only to the VPIM Network Type.

Figure 1-1. Network Type



Voice Processor\Timers and Limits

Call Progress Delay: The default value has changed to **6000**.

Voice Processor\Devices\Applications

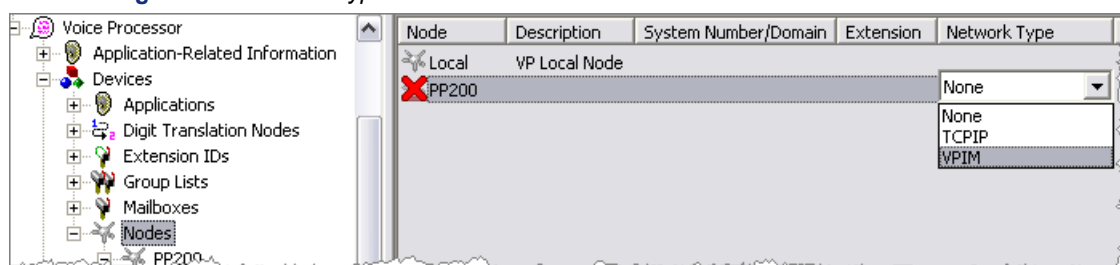
The Accept AMIS Calls option was removed from the Call Routing Announcement application because AMIS is only supported in the VPU.

Voice Processor\Devices\Nodes

To support VPIM Networking (see [page 11-9](#)), the VPIM protocol was added to the Network Type column. The networking options for EM are None, TCP/IP and VPIM. The networking options for BVM are None, and VPIM.

Also, the System Number column has been renamed to System Number/Domain. The Domain name applies only to the VPIM Network Type.

Figure 1-2. Network Type



The Dial-Up Phone Number, Dial-Up Username, and Dial-Up Password fields in Voice Processor\Devices\Nodes\<node> were removed because these fields apply to VPU AMIS only.

E-Mail Gateway

The E-mail Gateway folder was moved from Voice Processor\E-Mail Gateway to System\E-Mail Gateway. You can use this folder to configure the System Health Report feature (see [page 3-40](#)) in addition to existing features, such as Forward-to-E-Mail, VPIM Networking, and Unified Messaging (refer to the DB Programming Help).

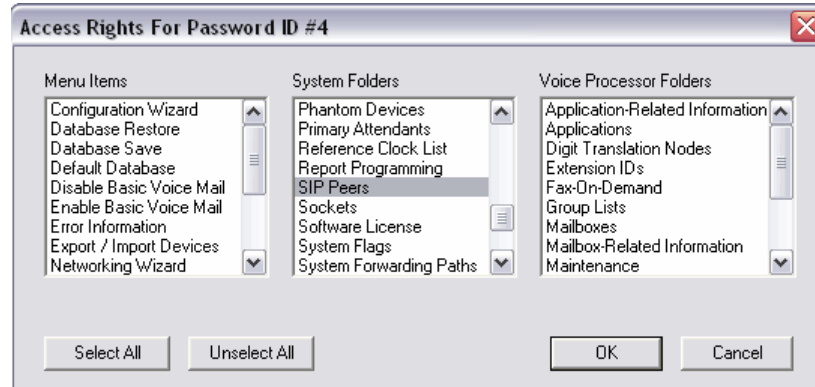
Call Configurations

The Fax Encoding Setting (Fax Detection) field was removed from the IP Call Configuration folder (System\Devices and Feature Codes\Node IP Connection Groups\IP Call Configuration) for each IP Connection Group because the Mitel 5000 system does not support this functionality.

Passwords\Edit Access Rights

The SIP Peers folder was added to the System Folders list in the Access Rights dialog box. For more information about SIP Peers, refer to the *Mitel 5000 Reference Manual*, part number 580.8007.

Figure 1-3. Access Rights Dialog Box



New Features in Administrative Web Session (AWS)

The Administrative Web Session (AWS) pages include a variety of changes for v3.0. Some changes include new pages and information to support SIP peers and file-based Music-On-Hold. The AWS pages provide statistical information for SIP peers and provide information about active SIP peer calls. For complete details, see the following sections:

- “New AWS Pages” below
- “Modified AWS Pages” on [page 1-18](#)

New AWS Pages

The following pages have been added to support new functionality such as diagnostic information for SIP peers and file-based management for Music-On-Hold:

- “System SIP Diagnostics Page” below
- “SIP Peer Diagnostics Page” on [page 1-16](#)
- “Trunk Diagnostics Page” on [page 1-16](#)
- “MOH Files Page” on [page 1-17](#)

System SIP Diagnostics Page

The System SIP Diagnostics page is new to v3.0. To locate the SIP System Diagnostics page, click **System SIP Diagnostics** from the IP Resource Info navigation tab in Advanced view. This page is available for Mitel CS-5200/5400/5600 systems. For a Mitel CS-5600 configuration, this page is available on the Processing Server (PS-1) AWS. This page provides statistical information for system-wide SIP calls and SIP peers, functionality to reset the system-wide SIP statistic counts, and a snapshot of existing SIP peer calls. When directed by Technical Support, you can also dump this information from System Monitor (see “New Dumps for SIP Peers in System Monitor” on [page 1-8](#)).

Statistic information displayed on the Web page includes counts for the following:

- **SIP Dialog Statistics**
 - *Total Created SIP Dialogs*: The total number of SIP dialogs created.
 - *Incoming SIP Dialogs*: The total number of SIP dialogs as a result of SIP messages received from all SIP peers.
 - *Outgoing SIP Dialogs*: The total number of SIP dialogs originating from the Mitel 5000 towards all SIP peers.
 - *Current Active SIP dialogs*: The number of currently active SIP dialogs.
- **SIP Message Statistics**
 - *Total Received SIP Messages*: The total number of SIP messages received from all SIP peers.
 - *Total Sent SIP Messages*: The total number of SIP messages sent to all SIP peers.

- **SIP Error Statistics**

- *Total Error Count*: The total number of errors including parse errors, transmission errors, invalid destination errors, SIP route errors, invalid state errors and SIP timer errors.
- *Parse Error Count*: The number of errors encountered while parsing incoming SIP messages.
- *Transmission Error Count*: The number of errors while transmitting SIP messages to peers.
- *Invalid Destination Error Count*: The number of errors while trying to send a SIP message towards an invalid SIP peer IP address or hostname. This could happen due to the misconfiguration of a SIP peer IP address, hostname, or port number.
- *SIP Route Error Count*: Not used.
- *Invalid State Error Count*: Not used.
- *SIP Timer A H Timeout Counter*: The number of SIP timeout events while sending SIP messages and/or expecting SIP responses.

- **SIP Call/Transaction Statistics**

- *Calls Received*: The total number of SIP calls received.
- *Remote Initiated Calls Established*: The number of SIP calls initiated and successfully established by remote SIP peers.
- *Remote Initiated Calls Rejected*: The number of SIP calls initiated by remote SIP peer, but rejected by the Mitel 5000.
- *Calls Initiated Locally*: The number of SIP calls initiated by the local host (Mitel 5000).
- *Initiated Calls Established*: The number of SIP calls initiated and successfully established by the local host (Mitel 5000).
- *Initiated Calls Rejected*: The number of SIP calls initiated by the local host (Mitel 5000), but rejected by a SIP peer.
- *Calls Terminated By Either End*: The total number of SIP calls terminated (by the local host or by remote SIP peers).
- *Transactions Received*: The total number of SIP transactions received from SIP peers.
- *Transactions Sent*: The total number of SIP transactions sent to SIP peers.

- **Clear Diagnostics**: Click **Clear Diagnostics** to zero out all of the fields. The “all diagnostics data will be lost” message appears.

The page refreshes every 30 seconds by default, but you may change the refresh interval with the buttons on the bottom panel:

- **Set Interval**: Sets the refresh rate of this page with the value in the Refresh Interval box. The minimum value of the Refresh Interval is 10 seconds.
- **Stop**: Stops refreshing the page. The Refresh Interval box is cleared automatically.
- **Refresh**: Immediately refreshes the page. Restores all information to the current values stored in the database.

“Diagnostics last cleared on” specifies the date and time when the last statistics were cleared or if the diagnostics have not been cleared since the last reboot.

SIP Peer Diagnostics Page

The SIP Peer Diagnostics page is new to v3.0. To locate the SIP Peer Diagnostics page, click **SIP Peer Diagnostics** from the IP Resource Info navigation tab. This page is available for Mitel CS-5200/5400/5600 systems. For a Mitel CS-5600 configuration, this page is available on the Processing Server (PS-1) AWS. This page provides statistical information for a specific SIP peer, such as NuPoint Messenger.

To view statistic information for a SIP peer:

1. Select an extension from the **SIP Peer Extension** list.
2. Click **Get Statistics**. The statistics for a given SIP peer includes counts for the following:
 - **SIP Messages Sent**: The total number of SIP messages sent to the SIP peer.
 - **SIP Messages Received**: The total number of SIP messages received from the SIP peer.
 - **SIP Requests Sent**: The total number of SIP request messages sent to the SIP peer.
 - **SIP Requests Received**: The total number of SIP request messages received from the SIP peer.
 - **SIP Responses Sent**: The total number of SIP response messages sent to the SIP peer.
 - **SIP Responses Received**: The total number of SIP response messages received from the SIP peer.
 - **Active Dialog Count**: The number of currently active SIP dialogs between the local host (Mitel 5000) and the SIP peer.
 - **Total Dialog Count**: The total number of SIP dialogs between the local host (Mitel 5000) and the SIP peer.

Trunk Diagnostics Page

To locate the Trunk Diagnostics page, click **Trunk Diagnostics** from the IP Resource Info navigation tab in Advanced view. This page is available for Mitel CS-5200/5400/5600 systems. For a Mitel CS-5600 configuration, this page is available on the Processing Server (PS-1) AWS. This page provides trunk call statistics over the past 24 hours. The current hour of the system time is highlighted on the page.

The page refreshes every 30 seconds by default, but you may change the refresh interval with the buttons on the bottom panel:

- **Set Interval**: Sets the refresh rate of this page with the value in the Refresh Interval box. The minimum value of the Refresh Interval is 10 seconds.
- **Stop**: Stops refreshing the page. The Refresh Interval box is cleared automatically.
- **Refresh**: Immediately refreshes the page. Restores all information to the current values stored in the database.

MOH Files Page

To locate the MOH Files page, click **MOH Files** from the System Management tab. This page is available for Mitel CS-5200/5400/5600 systems. For the CS-5600, you can access the Base Server AWS to find information about this feature. From this page you can upload, download, and delete music files for Music-On-Hold. The MOH files are stored on the compact flash-type memory card, but they are not included in the Database Save or Voice Processor Save. When you create your MOH files, make sure you create a backup of your local files.

The page includes information about the total music file space usage and the amount of available space left on the compact flash-type memory card. You cannot upload additional music files after the available memory drops below 20%. In that case, the Web server aborts the upload with notification.

The page also shows the file name, date, and size of the files that currently reside on the compact flash-type memory card of the Mitel 5000. The Web page supports the non-proprietary G.711 (.n64u) file format. You can only upload one music file concurrently. File names support the following characters: A-Z, a-z, 0-9, space (), exclamation mark (!), pound [hash] (#), hyphen (-), underscore (_), parenthesis (), and the plus sign (+).

NOTE

The power of all signal energy other than live voice cannot exceed -9dBm when averaged over a 3 second interval. With our default loss plan, worst case, this means that the File-Based MOH file cannot exceed -12 dBm0 when averaged over a 3 second interval. If any gain on the system (for example, the transmit gain on a loop start trunk) is increased, this maximum level must be decreased by the same amount.

To upload an MOH file:

1. Click **Browse** in the **MOH file to upload** text box. The **Choose File** dialog box opens.
2. Locate your file, and then click **Open**.
3. Click **Upload File**.

To download an MOH file:

1. Right-click a MOH file name, and then select **Save Target As**. The **Save As** dialog box opens.
2. Select or type a path for the location, and then click **Save**. The file is saved.

To delete an MOH file:

1. Click the check box next to the file name.
2. Click **Delete**.

Modified AWS Pages

The following pages have been modified for various reasons. Refer to the Help for complete details:

- “Home Page” below
- “Network Page” on [page 1-18](#)
- “IP Resource Diagnostics Page” on [page 1-18](#)
- “IPDRM Resource Diagnostics Page” on [page 1-18](#)
- “Log Files Page” on [page 1-19](#)
- “Application Logging Options Page” on [page 1-19](#)
- “Onboard Modem Page” on [page 1-19](#)
- “Digital Endpoint Interface Page” on [page 1-19](#)
- “Session Information Details Page” on [page 1-19](#)

Home Page

The Home page now includes the system alarm status. The following information appears:

- **Green:** Status says “Good.” The system is operational. Call Processing is running.
- **Yellow:** Status says “Fair.” The system is operational, but one or more modules are offline. A code appears. Refer to the *Message Print Diagnostics Manual*, part number, 550.8018 for details about the alarm.
- **Red:** Status says “Unstable.” Call Processing has reported a fault and it has not been cleared. A code appears. Refer to the *Message Print Diagnostics Manual*, part number 550.8018 for details about the alarm.

Network Page

The Network page now includes the following information:

- **DHCP Enabled:** Determines whether Dynamic Host Configuration Protocol (DHCP) is used for both the Base Server and the Processing Server. You can also program the DHCP Enable option in the Configuration Wizard. Refer to the DB Programming Help for details about the Configuration Wizard.
- **WINS Server IP Address:** Defines the IP connection’s WINS IP address provided by the IP network administrator. If there is no WINS Server, this field shows 0.0.0.0.

Refer to AWS Help for details.

IP Resource Diagnostics Page

The IP Resource Diagnostics page now includes static information for IP Voice Mail and File-Based MOH. Refer to the Help for details.

IPDRM Resource Diagnostics Page

The IPDRM Resource Diagnostics page now includes static information for IP Voice Mail. Refer to the Help for details.

Log Files Page

The Log Files page now includes diagnostic log files for SIP Peers: CP SIP and CP History. The CP SIP log file includes SIP message and SIP peer information. The CP History log file includes SIP peer message information depending on the SIP View option (see “SIP View Diagnostics Feature Code 9987 [9187]” on [page 1-8](#)).

The Log Files page also includes Database Change Logs and System Health Report Logs. The Database Change log is a log providing details on user changes to DB Programming. For more information, see “Database Change Log” on [page 16-6](#). The System Health Report log is a log that contains system information and statistics used to troubleshoot the Mitel 5000 system (see “System Health Report” on [page 3-40](#) for details).

From the AWS, you can view and save log files.

Application Logging Options Page

The Application Logging Options page now includes logging options for the following new logs:

- SIP Logs
- Database Change Logs

Refer to AWS Help for details.

Onboard Modem Page

To locate the Onboard Modem page, click Onboard Modem from the System Status tab in Advanced view. With v3.0, the 5000 is now able to connect to an external modem. To avoid confusion, the Modem page is now called the Onboard Modem page.

Digital Endpoint Interface Page

V3.0 now supports four digital endpoint interfaces and their bays. For more information, refer to the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000. The Digital Endpoint Information page now includes the bay information for those interfaces.

Session Information Details Page

The Session Information Details page includes two new fields for the new dual-filter Echo Canceller (ECAN) card. For more information, see “Voice Over Internet Protocol (VoIP) Echo Canceller” on [page 10-8](#).

- **Echo Canceller Type:**
 - *Basic*: The system is using the single-filter ECAN.
 - *Advanced*: The system is using the dual-filter ECAN.
 - *Specialized*: The system is using the dual-filter ECAN with advanced (non-user configurable) settings.
- **Minimum ERL Assumed (dB)**: The range is 0–18 dB.

About Database Programming

Introduction	2-2
Technical Support	2-2
Planning the Programming Session	2-2
Programming Wizards	2-2
Programming Checklist	2-3
Session Manager	2-4
Session Manager Interface	2-4
Session Menu	2-5
Settings Menu	2-6
Session Description	2-7
Session Manager Connection Tabs	2-7
Starting a DB Programming Session	2-8
Session Manager Connection Options	2-9
Local (Stand-Alone)	2-9
Network (Over IP)	2-10
Network (Using a Modem)	2-10
Modem Setup	2-11
Remote Modem Troubleshooting	2-12
DB Programming User Interface	2-12
DB Studio Elements	2-13
Menu Bar	2-13
File Menu	2-13
View Menu	2-13
Operations Menu	2-13
Tools Menu	2-14
Favorites Menu	2-14
Help Menu	2-14
Toolbar Buttons	2-14
Directory Folders	2-15
Status Bar	2-15
Programming the Inactivity Timer	2-15
Selection Wizards	2-16
DB Programming Tips	2-17
Viewing DB Studio Programming Panes	2-17
Changing Displayed Information in the Programming Window	2-17
Using a Keyboard Instead of a Mouse	2-18

Introduction

This guide provides descriptions and procedures for performing common administrative tasks using the Mitel 5000 Database (DB) Programming application. This includes instructions to complete system configuration and perform system adds, moves, and changes after installation.

The guide assumes that the system is installed and that test calls have been placed to verify that the system is properly connected to Central Office (CO) lines. It does not cover installation programming, which includes hardware programming, system upgrades, and licensing. For more information about installation programming, refer to the following resources:

- *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.
- *Mitel 5000 Reference Manual*, part number 580.8007.
- *Mitel 5000 DB Programming (context-sensitive) Help*.

To access Mitel 5000 DB Programming Help:

While in DB Programming, select Help – **Help Topics**, or press **F1** for context-sensitive help.

Technical Support

You can search the [Tech Central Knowledge Base Center](http://www.inter-tel.com/knowledgebasecenter) (www.inter-tel.com/knowledgebasecenter) on the [edGe Web site](http://www.inter-tel.com/portal/page/portal/us_edge) (http://www.inter-tel.com/portal/page/portal/us_edge) regarding DB Programming issues. The Knowledge Base is a current repository for resolved issues and common questions involving Mitel products. If the problem persists, contact Technical Support. For readers located in Europe, contact the Mitel Europe office for more information.

NOTICE

The following certification is required to install this equipment and to receive technical support:

- Mitel 5000 Basic certification
- Convergence Technology Professional (CTP) certification

Technical support is provided for authorized products only.

Planning the Programming Session

Before programming, determine the features that meet your organization's needs, and then refer to the specific programs and program planning sheets. Program planning sheets are included in the "Documentation" folder of the system software CD. You can also find all documentation on the [edGe Online Manuals and Guides Web site](http://www.inter-tel.com/techpublications) (www.inter-tel.com/techpublications).

Programming Wizards

DB Programming includes several wizards that allow you to quickly program different parts of the system without having to navigate to separate areas in DB Programming. Wizard details and instructions are included in the appropriate sections. For example, for Networking Wizard information, see "Using The Networking Wizard" on [page 4-6](#). For Configuration Wizard information, refer to the "Installation" chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

Programming Checklist

After all system hardware and software is installed, program the following:

- ☐ System management options such as passwords, database backup options, and system reset options. See “System Management” on [page 3-1](#).
- ☐ System nodes. See “Private Networking and System Nodes” on [page 4-1](#).
- ☐ Numbering plans for all system nodes.
 - a. Change the home area codes (does not apply to European systems).
 - b. Set up ARS route groups, dial rules, and facility groups.
 - c. Program toll restriction area flags, emergency number information, toll strings, classes of service, device baseline extensions, and user groups (area flags and user groups are not applicable to European systems).See “Numbering Plans” on [page 5-1](#).
- ☐ Trunk options for all system nodes. See “Trunks and Gateways” on [page 6-1](#).
- ☐ Endpoints and devices (including phantom devices) for all system nodes. For example, program endpoints, off-node devices, account codes, attendants, endpoint flags, keymaps, message centers, Do-Not-Disturb and Reminder messages, primary attendants, system forwarding paths, and System Speed Dial. See “Endpoints and Devices” on [page 7-1](#).
- ☐ Groups and lists. Program extension lists, trunk groups, network groups, and hunt groups. See “Extension Lists and System Groups” on [page 8-1](#).
- ☐ System and device IP settings and IP connections for system nodes. See “System and Device IP Settings” on [page 9-1](#).
- ☐ System settings.
 - a. Program system page zones, system flags, and system timers and limits.
 - b. Change any feature codes that conflict with extension numbers or that the customer wants to change. See “System Features” on [page 3-1](#).
- ☐ Voice processor system programming. See “Voice Processor System Programming” on [page 11-1](#).
 - a. Create voice processor applications such as Message Notification/Retrieval (MNR), Call Routing Announcements (CRAs), Record-A-Call, Schedule Time-Based Application Routing (STAR), and so on.
 - b. Create a voice mail administrator mailbox.
 - c. Program other voice processor applications and settings, extension IDs, group lists, voice processor options, timers, custom recordings, and system information.
 - d. Program feature-specific voice processor settings such as Fax-On-Demand and Unified Messaging.
 - e. Voice processor maintenance features such as Auto Reboot and Auto Scheduling options.
- ☐ Subscriber mailboxes. See “Subscriber Mailboxes” on [page 12-1](#).
- ☐ Maintenance system options. Program call cost, freeze zones, Message Print, and SMDR information, if applicable. See “System Management” on [page 3-1](#).
- ☐ Save the system database. See “Database Backup Options” on [page 3-12](#).

Session Manager

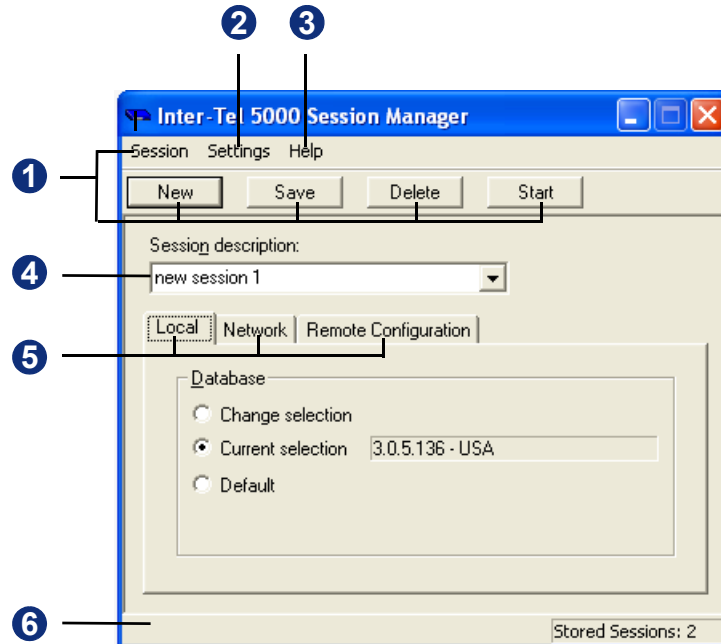
You must use Session Manager (shown in [Figure 2-1](#)) to start and select DB Programming sessions (see [page 2-12](#)). A session is a connection to a system node database.

Each session can then have unique connection settings, which allows you to enter and save information for each database that you are programming. For example, you may want to have a session stored for each node in a networked system. You can store an unlimited number of sessions. You can also export or import saved session settings from another computer. The Mitel 5000 Session Manager allows multiple sessions to run at the same time, provided each session interfaces with a different database. This allows you to program or view databases at numerous sites.

Session Manager Interface

You must start Session Manager to begin a DB Programming session. [Figure 2-1](#) shows an example Session Manager dialog box.

Figure 2-1. Session Manager



1	Session menu and buttons	Start, save, delete, or import session settings. For more information, see “Session Menu” on page 2-5 .
2	Settings menu	Select Language, Network Connection, Scheduled Backup, and Data Compression settings. For more information, see “Settings Menu” on page 2-6 .
3	Help menu	View Help or Session Manager version information.
4	Session description	Select the session name and number.
5	Connection tabs	Select the connection type. For more information, see “Session Manager Connection Tabs” on page 2-7 .
6	Status bar	Shows menu option descriptions and the total number of sessions saved.

Session Menu

The Session menu includes the following options:

- **New** (from the Session menu or button): Creates a new session. The session boxes show default values and the latest system version installed.
- **Save** (from the Session menu or button): Saves new session information.
- **Delete** (from the Session menu or button): Removes the currently displayed session. If a local database exists for this session, it is also deleted.
- **Start**: (from the Session menu or button): Starts a new session or the session shown in the Session Description box. See the following section, “Session Description”.
- **Export Session Settings File** (Session menu only): Select if you have sessions that you want to save for use on another computer. Then select the desired name and location of the file. Click **Save** to save the session settings is saved as a `.txt` file.
- **Import Session Settings File** (Session menu only): Select to import existing session information. Then select the name of the `.txt` file that you want to import. When you click **Open**, the sessions are automatically added to the registry (that is, existing sessions are **not** overwritten) and available for use. You cannot export or import individual session settings. Information for all sessions is saved to or imported from the same file.
- **Exit**: Exits Session Manger.

Settings Menu

The Settings menu includes the following options:

Language: Select the language for programming the system database. The default is American English for the USA and British English for Europe.

Network Connections: Change IP connection settings. These settings should only be changed if the link to Call Processing goes down while DB Programming is receiving large amounts of data, when saving a database, or when accessing mailbox or endpoint folders. The Network Connection parameters include:

- **Remote Proxy Server Connect Timeout:** *Remote Configuration is reserved for controlled introduction.* Indicates the number of seconds that the Session Manager waits for the connection to be made with the remote Mitel 5000 system. The range is 30–9999 seconds; the default is 120 seconds. See “Remote Configuration” on [page 3-54](#).
- **Read Timeout:** *This field applies to IP connections only.* This option applies to IP connections that are made using the Network tab, including a modem connection. Select the number of milliseconds (msec) that DB Programming waits to receive data packets from Call Processing. If DB Programming does not receive data before this timer expires, a warning message appears and DB Programming may shut down. If this occurs, check the link with Call Processing. If the link is valid, ping the network. If the network connection appears to be slower than the current Read Timeout value, increase this setting. The default setting is 5 seconds.

NOTE

Mitel recommends that you use the default setting. If you set this value too high, it may slow down other operations.

- **Receive Buffer Size:** *This field applies to IP connections only.* This field applies to IP connections that are made using the Network tab, including a modem connection. Select the number of bytes that are used as a buffer when DB Programming is receiving data from Call Processing. If DB Programming is shutting down when receiving large amounts of data, ping the network. If the network connection is faster than the current Read Timeout value, increase this setting. In the default state, this setting is 10000 bytes.
- **View IP Port:** *Remote Configuration is reserved for controlled introduction.* View or edit the following Remote Configuration connection ports. See “Remote Configuration” on [page 3-54](#).
 - **Proxy Server IP Port** (Remote Configuration tab): Identifies the port that is used on the network (proxy). The default port setting is 1194.
 - **Inter-Tel 5000 IP Port** (Remote Configuration tab): Identifies the port that is used on the Inter-Tel (Mitel) 5000 for the remote connection. The default port setting is 4000.
 - **IP Port** (Network tab): Identifies the recommended port to connect to Session Manager. The default port setting is 4000.
- **Scheduled Backups:** Schedule system database backups. For more information, see “Scheduled Backups” on [page 3-15](#) or refer to *Mitel 5000 DB Programming Help*.
- **Use Data Compression:** When selected, DB Programming information going through Call Processing to the voice processing computer is compressed to speed up data transfers.

NOTE

Do not disable the Use Data Compression flag unless instructed to do so by Mitel personnel.

Session Description

You can enter a new session description in the Session Description box, or you can select a previously saved session from the list.

Session Manager Connection Tabs

You can select one of the following Session Manager connections:

- **Local:** Allows you to use the following options.
 - *Change selection:* When a local session is started, you are prompted to select the database for this session. If a Current Selection exists for this session, it is deleted.
 - *Current selection:* This option uses the same database from the previous local session. If a previous selection was made, the database version appears next to the current selection option.
 - *Default:* When you start a local session, you are prompted for the system type.
- **Network:** Connects you to other system nodes. For a network connection, you must enter the IP address of the system associated with the session.
 - *Hostname/IP Address:* The hostname or IP address of the system. You can enter the IP or browse for an existing system IP address.
 - *System version:* The system version in which you are connecting to with Session Manager. If Session Manager connects to the system and the version is incorrect, Session Manager attempts to reconnect with the correct version if it is installed on the computer. Updating the system version on this tab also updates the version on every other tab in which it appears.
 - *IP Port:* Identifies the recommended port to connect to Session Manager. The default is set to 4000. You must enable this option from the Settings menu (see [page 2-6](#)).
 - *Use Modem:* To set up a modem connection, you must enter the number and type of the modem device before beginning the session. Enable this option, and then click **Properties** to configure RAS settings. Click **OK** when finished. For additional information on setting up a modem connection, see “Network (Using a Modem)” on [page 2-10](#).
- **Remote Connection:** *Remote Configuration is reserved for controlled introduction.* If authorized, you can use the Remote Configuration feature to configure a remote system database using a Virtual Private Network (VPN) connection. See “Remote Configuration” on [page 3-54](#).

Starting a DB Programming Session

You must start a session before configuring DB Programming. See “Session Manager Connection Options” on [page 2-9](#) for information about selecting a database connection type.

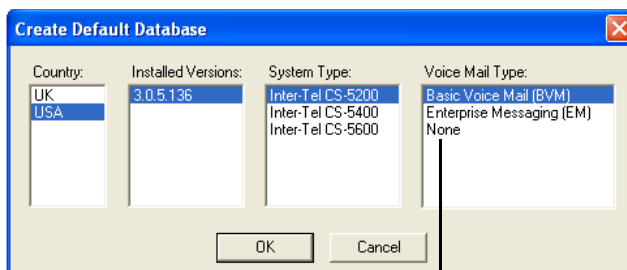
To start a session:

1. From the **Session description** list, select a session, or click **New** and enter the new session description.
2. Click **Start**. If a password is required, enter the password, and then click **OK**. By default, DB Programming passwords are not enabled. To program a system password, see “Programming a Password” on [page 3-4](#).

NOTES

If you do not select or create a session, or if you try to connect to a non-Mitel 5000 system or a remote Inter-Tel Axxess® platform, an error message appears and the session terminates.

3. Do one of the following:
 - If you are using the *Local* tab to create a new database or use a default database, the following dialog box below appears.




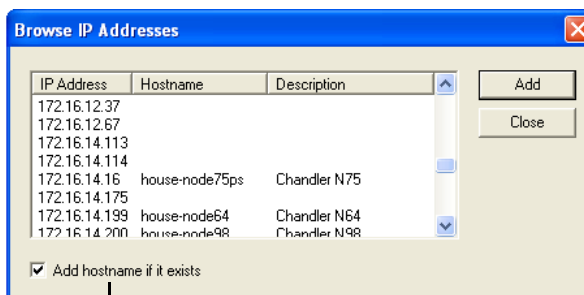
Select “None” if you are using a NuPoint Messenger voice processor

Select the options for your system, and then click **OK**.

- If you using the **Network** tab to connect to another system node:

Do one of the following:

- In the **Hostname/IP Address** box, type the IP address for the system node.
- Click  (Browse) to select the IP address from the list. The following dialog box appears. Click **Add** to select the IP address.



If the “Add hostname if it exists” check box is selected and a hostname is programmed for the system, the hostname assigned to the IP address is populated in the IP Address box instead of the IP address.

- If you are using the *Remote Configuration* tab to use a Remote Configuration connection, See “Remote Configuration” on [page 3-54](#).

After you make the Session Manager connection, the DB Programming interface (DB Studio) appears. See “DB Programming User Interface” on [page 2-12](#).

Session Manager Connection Options

The following sections describe the several different methods that you can use to connect to a system database.

Remember the following when connecting to sessions with Session Manager:

- You can only have one remote and one local session to be active at a time for each session name.
- You cannot edit the session data while an associated session is active.
- You cannot open multiple local databases under a single session name.

The following Session Manager connection scenarios result in warning messages:

- **Current Selection:** If you click **Start** when the Current selection in the Local tab is set to a session name that is already active, an override message appears. If you override the message, you are prompted to start a new or different session.
- **Default:** If you click **Default** in the Local tab, and then click **Start**, a message appears indicating that the session is already active. If you override the message, you are notified that performing the operation deletes the working database copy for the session. If desired, click **Yes** to select the version information. When you click **OK**, if the session is active or the database copy is in use, a message appears prompting you to create a new session or select a different session. If the session is not active, the override proceeds successfully.
- **Change Selection:** If you click **Change Selection**, and then click **Start**, a message appears indicating that the session is already active. If you override this message, another message appears notifying you that the operation will delete the working database. If desired, click **Yes** to select the database. When you double-click the database or click **Open**, if the session is active or the database copy is in use, a message appears prompting you to create a new session or select a different session. If the session is not active, the override proceeds successfully.
- **Edit Sessions Parameters:** If you change session parameters while the viewed session is active and attempt to click **Save** or **Start**, a message appears notifying you that changes cannot be saved.
- **Change Session Name:** If you attempt to change the session name while the viewed session is active, either local or remote, a message appears notifying you that changes cannot be saved.
- **Delete Session:** If you attempt to delete a session that is active, either local or remote, the following message appears, "This session cannot be deleted at this time because it is currently active. If you are certain this is not true, you may try again after restarting the Sessions Manager or restarting your PC."

Local (Stand-Alone)

To use a computer for stand-alone programming, the proper version of DB Programming must be loaded on a computer that has an IP connection to the Mitel 5000 Base Server. The system database can then be saved to the programming computer or any storage devices available on that computer. If you are saving the voice mail database or Basic Voice Mail, then a USB 2.x-compatible flash drive must be inserted in the USB-A port on the front of the Base Server.

Network (Over IP)

If you know the system IP address, you can access the system database over the network through an IP connection. Because the system initially uses Dynamic Host Configuration Protocol (DHCP) to assign the system IP address, you must get the IP address from the LCD panel on the front of the system chassis before you can access the system from a remote location.

For more information about finding the IP address from the LCD panel, refer to the Installation chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000. You can then provide a static IP address (recommended) in DB Programming. The system is then available for programming over an IP connection.

Network (Using a Modem)

When you cannot access the system over the public Internet, use modem access to the system database to program the system or perform maintenance and diagnostics tasks (see “Modem Setup” on [page 2-11](#)). This allows flexibility in making database changes without visiting the site and, in system trouble situations, the service personnel may perform preliminary investigations before going on site. You can connect directly to the system using the built-in modem. For more information and complete modem kit instructions, refer to the *Modem Kit Installation and Troubleshooting for Mitel® 5000 and Inter-Tel® Axxess®*, part number 835.1621-11.

To use the remote programming feature, a user dials the number that directly rings in to the modem, is transferred to the modem, or dials the modem extension number using DISA or an endpoint. When the modem circuit rings, the modem automatically answers the call and generates modem tone. The calling party may then connect the programming computer modem and proceed with the programming session. When the session is completed, the calling party hangs up or disconnects the call from the modem. When this happens the system modem no longer hears modem tone and disconnects.

Use the IP port for remote programming. To set up or check the modem parameters, use the Windows Settings/Control Panel as you would for any computer modem application. If a remote programming session is active on a system with an external voice processing system, and the communications connection fails, the remote programming session is terminated.

If used, Save/Restore will take longer to perform through a modem than through a direct connection due to the slower bit rate. If the Restore function is used, the associated system reset, when completed, will disconnect all calls including the modem connection. If the modem connection is lost during the programming session, allow a minute for the system modem to reset, and then re-establish the call. All changes that were saved by a system update before the connection was lost will be retained in system memory.

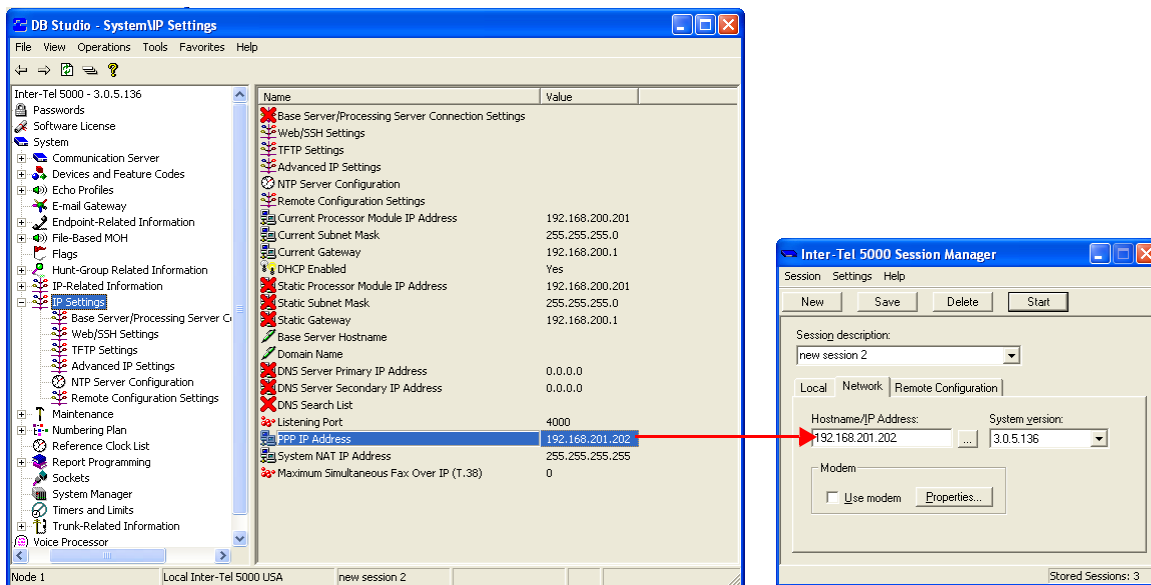
Modem Setup

For more information and complete modem kit instructions, refer to the *Modem Kit Installation and Troubleshooting for Mitel® 5000 and Inter-Tel® Axxess®*, part number 835.1621-11.

To set up a modem:

1. Make sure the modem is configured correctly for the system. If necessary, refer to the modem documentation.
2. From the Session Manager dialog box, click the **Network** tab.
3. In the Session Manager **Hostname/IP Address** box, type the PPP IP Address (the default PPP IP address is 192.168.201.202). To find the PPP IP address, you can start a local session, and then view the PPP IP address under Communication Server – IP Settings, as shown [Figure 2-2](#).

Figure 2-2. PPP IP Address Location



4. Select the **Use modem** check box.
5. Click **Properties**. The <session> Modem Properties dialog box appears.
6. In the **Phone number** box on the **General** tab, type the phone number to connect to the Mitel 5000. The default modem phone number is located under System – Devices and Feature Codes – Modems – **Local**.
7. Select the **Show icon in notification area when connected** check box.
8. Click **OK**.
9. In Session Manager, click **Start** to begin the DB Programming session. You may be prompted for a PPP username/password. Leave the options blank (click **Cancel** or **OK**). When prompted for the DB Programming password, enter it if applicable.
10. Click **Dial**, and then click **OK** at the Connection Complete screen. The modem connection is established and you are ready to begin programming.

Remote Modem Troubleshooting

If the modem is not connecting to the system, try the following:

- Try running the Windows Hyperterminal program under Start – Accessories – Communications – **HyperTerminal**. The modem may not be configured properly if Hyperterminal is unable to dial out.
- In the **Bits per second** box, type **9600**.
- Check that the DB Programming modem is enabled (System – Devices and Feature Codes – Modem – **Local**).
- The modem connected to the system may need to be reprogrammed.

For more information and complete modem kit instructions, refer to the *Modem Kit Installation and Troubleshooting for Mitel® 5000 and Inter-Tel® Axxess®*, part number 835.1621-11.

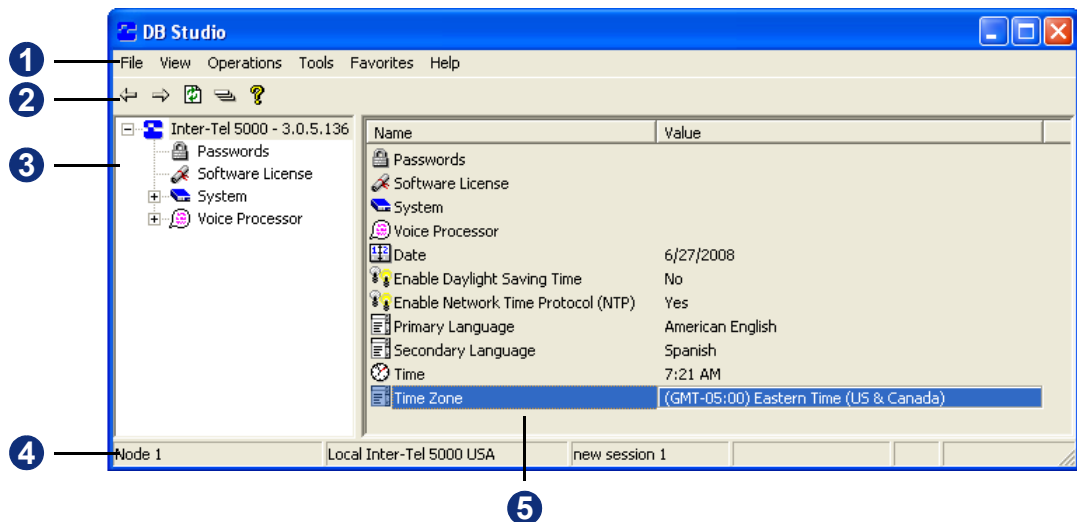
DB Programming User Interface

The DB Programming user interface, DB Studio (as shown in [Figure 2-3](#)), allows you to quickly move between programming options. For more information about DB Studio elements, see [page 2-13](#). You can see both the hierarchy of the database and all the items in each programming area. When you click an element or folder in the left pane, the contents appear in the right pane.

NOTE

If the DB Programming session is slow to respond, shut down any other programs—including antivirus programs—that may be running. If this action does not improve response speed, make sure the computer meets the minimum requirements. For more information about computer requirements, refer to the Specifications chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

Figure 2-3. DB Studio



1	Menu bar	Shows menu options. See page 2-13 .
2	Toolbar buttons	Provide viewing options. See page 2-14 .
3	Left pane	Shows Directory folders. See page 2-15 .
4	Status bar	Shows system and connection information. See page 2-15 .
5	Right pane	Displays options available for feature settings.

DB Studio Elements

The following sections describe DB Studio elements.

Menu Bar

Menus include the File, View, Operations, Tools, Favorites, and Help menus.

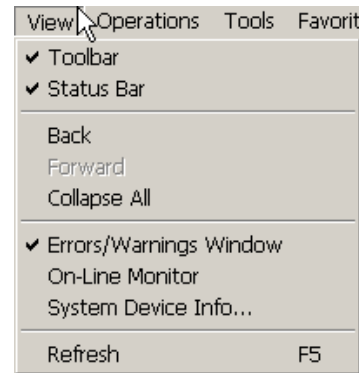
File Menu

This menu contains the Exit option only, which ends the DB Programming session.

View Menu

The View menu includes the following options:

- **Toolbar:** Shows or hides the toolbar at the top of the window.
- **Status Bar:** Shows or hides the status bar at the bottom of the screen. The status bar shows the name of the session.
- **Back and Forward:** Allow you to move Back and Forward between views. You can also use the **Back** and **Forward** arrow buttons. See Figure 2-3 on [page 2-12](#).
- **Collapse All:** Collapses all expanded folders in the left pane. You can also use the Collapse all button. See Figure 2-3 on [page 2-12](#).
- **Errors/Warning Window:** Enables or disables the errors and warnings window that appears at the bottom of the screen.
- **On-line Monitor:** Enables or disables online Monitor (OLM) mode. OLM is used for troubleshooting system problems. Use the OLM mode only when authorized by Mitel personnel.
- **System Device Info:** Displays all of the system devices. The Time Division Multiplexing (TDM) and IP devices appear at the top of the list, followed by the system non-physical devices at the bottom.
- **Refresh:** Refreshes the screen.



Operations Menu

The Operations menu provides several options to help manage the system, as described in the following sections:

- “System Software Licenses” on [page 3-6](#)
- “Database Backup Options” on [page 3-12](#)
- “System Error Information” on [page 3-35](#)
- “System Resets” on [page 3-44](#)
- “Uploading the System Manager CA Certificate” on [page 4-27](#)
- “Node Devices – Importing and Exporting” on [page 4-19](#)
- “Saving and Restoring Voice Processing Databases” on [page 13-3](#)
- “Printing System Reports” on [page 15-5](#)

Tools Menu

The Tools menu includes the following options:

- **Configuration Wizard:** Used to configure new systems. For more information about the Configuration Wizard, refer to the Installation chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.
- **Networking Wizard:** Used to configure IP networking or T1/E1 PRI networking parameters. For more information, see “Using The Networking Wizard” on [page 4-6](#).
- **Resource Reservation Tool:** For detailed information about the Resource Reservation Tool, see [page 9-42](#).
- **Shortcut Tool (CTRL+T):** Allows you to quickly jump to a specific programming area. For shortcut descriptions, refer to the *Mitel 5000 DB Programming Help* (press F1).

Favorites Menu

From the Favorites menu, you can add shortcuts to your most frequently visited folders. The menu also has options for sorting the list and deleting entries.

Help Menu





The Help menu includes the following options:

- **About DB Studio:** Shows DB Studio version and copyright information.
- **Help Topics:** Starts online Help.
- **About Inter-Tel Database Programming:** Shows DB Programming version and copyright information. For option descriptions and instructions, refer to Help (press F1).
- **About Inter-Tel Software License:** Shows licensed features on the system. Additional software license information is available in the Software License directory. For option descriptions and instructions, refer to Help (press F1).
- **About Inter-Tel Software Release and Packages:** Shows system software release and package information while connected in a remote-mode session. For option descriptions and instructions, refer to the Help (press F1). Not available for local-mode sessions.

Toolbar Buttons

[Table 2-1](#) shows DB Studio toolbar buttons.

Table 2-1. *Toolbar Buttons*

Icon	Name	Description
	Back and Forward	Move backward and forward between views. You can also use the Back or Forward options in the View menu.
	Refresh	Refreshes the display. You can also use the Refresh option in the View menu or the F5 button.
	Collapse All	Collapses all expanded folders in the left pane and returns the focus to the root folder. You can also use the Collapse All option in the View menu.
	About DB Studio	Shows DB Studio version information.

Directory Folders

The following subdirectories are shown in the Directory:

- **Passwords directory:** For more information about assigning system passwords, see “Passwords” on [page 3-4](#).
- **Software License directory:** For more information about software licensing, see “System Software Licenses” on [page 3-6](#).
- **System directory:** The System directory features include most of the Mitel 5000 system features and are discussed throughout this guide.
- **Voice Processor directory:** For more information about voice processor features, see “Voice Processor System Programming” on [page 11-1](#).

Status Bar

The status bar at the bottom of the window shows the description and number of the Node being programmed, the type of programming session, and the name assigned to the programming session in Session Manager. It also displays status and error messages when applicable. The status bar also displays a description if you click and hold the cursor over the menu or menu option.

Programming the Inactivity Timer

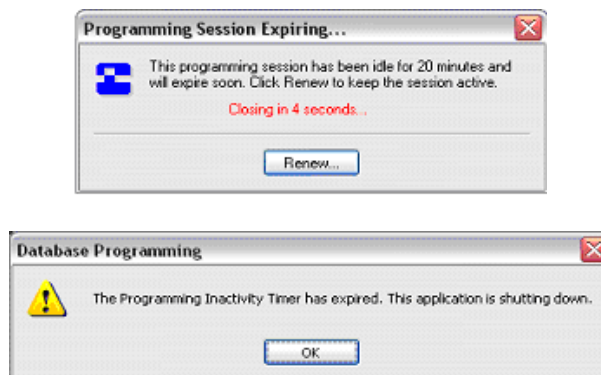
DB Studio has an inactivity timer that automatically shuts down the application when it has been idle for a specified amount of time. The programmable idle period is a field in the main folder and can be modified only in the online Monitor (OLM) mode. The valid range is 10–120 minutes; the default is 20 minutes.

NOTE

Do **not** use OLM mode unless you are instructed to do so by Mitel technical support personnel.

Inactivity messages are shown in [Figure 2-4](#).

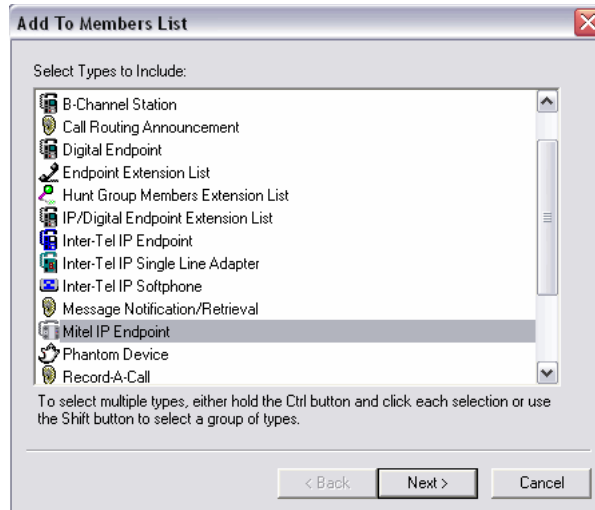
Figure 2-4. *Inactivity Messages*



Selection Wizards

Any list in DB Programming that you use to add or move items through the shortcut menu uses a Selection Wizard (for example, adding members to a hunt group). [Figure 2-5](#) shows an example Selection Wizard.

Figure 2-5. Selection Wizard



DB Programming Tips

The following sections describe general tips when using DB Programming.

Viewing DB Studio Programming Panes

Remember the following when you view the left and right programming panes (see [page 2-12](#)):

- While programming, it is best to display the information in Details view to make the input fields visible.
- Click the column headings to sort a list of items. To sort files in reverse order, click the column heading once more. The tree view does not get sorted until you restart DB Programming.
- In many programming areas, click the right mouse button to see a menu of available commands.
- Several feature options instruct you to “click in a blank area of the right pane.” If there is not a blank area available, you can also press CTRL+N.

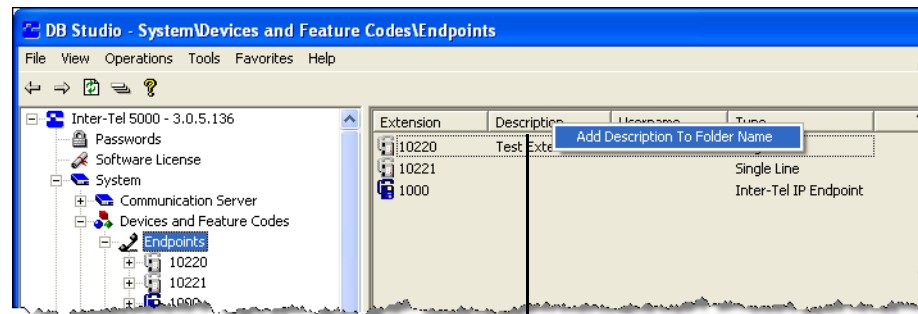
Changing Displayed Information in the Programming Window

For identification purposes, you can add information to the left pane of the system folders.

To add the information:

1. Right-click the option that you want to display in the folder name, as shown in [Figure 2-6](#).

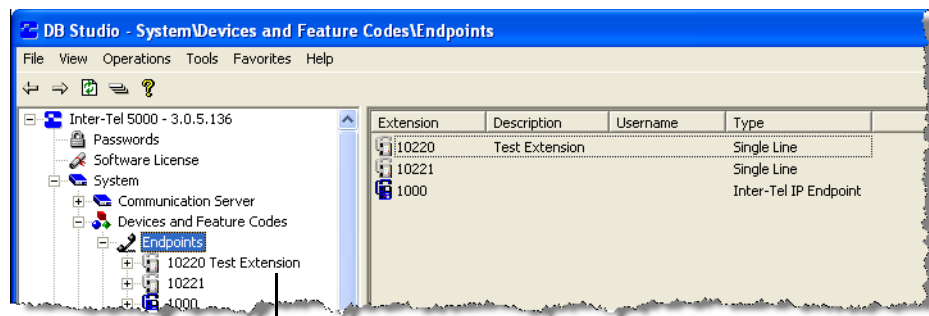
Figure 2-6. Description Column



Right-click to add
a description to the left pane.

2. Click **Add <option> To Folder Name**. The option name now appears in the folder name in the left pane, as shown in [Figure 2-7](#). To remove the field, repeat the procedure and select the option to remove the field. (The recommended limit is three fields.)

Figure 2-7. Folder Name with Description



Description
Appears Here

Using a Keyboard Instead of a Mouse

You can use the keyboard to program feature options, without using a computer mouse. [Table 2-2](#) shows keystroke assignments.

Table 2-2. *Keystrokes for Navigating without a Mouse*

Key	Action
TAB SHIFT + TAB	Moves the selection between left and right pane or between lists (immediately below Menu Bar) and the left pane.
ALT + TAB	Switches between open programs in Windows.
Left or Right Arrow	Moves programming focus to left or right.
Up or Down Arrow	Moves programming focus up or down. Scrolls up or down in lists.
SPACE BAR	Changes status of a flag when the flag is selected for programming.
ENTER	Equivalent to a single click. Also used to accept a selected item in lists.
CTRL + N	Opens “Create” or “Add” dialog boxes.
CTRL + ENTER	Equivalent to a double-click.
ESC	When programming an item, it restores the original value (no change made) and removes focus from that item. If a list is open, it closes the list with no change.

System Management

Introduction	3-3
Passwords	3-4
Programming a Password	3-4
Assigning Administrator Access Rights	3-5
System Software Licenses	3-6
About Software License	3-9
Software License Operations – Upload Software License	3-10
Comparing or Uploading a Software License	3-11
Database Backup Options	3-12
Backup Database Save	3-14
Scheduled Backups	3-15
Setting Scheduled Backups for a Session	3-16
Setting Scheduled Backups for All Sessions	3-30
Scheduled Backup Diagnostic Logs	3-31
Default Database	3-34
System Error Information	3-35
System Maintenance Options	3-36
Call Costs	3-37
Selecting a Call Cost Rate	3-37
Calculating Call Costs	3-38
Freeze Zones	3-39
Programming Freeze Zones	3-39
Adding Nodes to Freeze Zones	3-39
Deleting Nodes from Freeze Zones	3-39
System Health Report	3-40
CS-5600 Report Example	3-41
Programming	3-42
System Resets	3-44
Immediate System Resets	3-44
Call Processing Resets	3-44
Major Reset Scheduling	3-44
System Requires Reset	3-45
Scheduled Reset Time	3-45
Force Reset If Not Idle	3-45
Days of the Week	3-45
Always Reset On Days Of Week	3-46
Reset System Dialog Box	3-47

Message Print	3-48
Output Port And Local Backup Port	3-48
Message Print Output Active	3-49
Output Device Line Width	3-49
Print Options	3-49
Station Message Detail Recording	3-50
Devices	3-50
Output Port and Local Backup Port	3-50
SMDR Output Active	3-51
Output to System Manager	3-51
Display Elapsed Time in Seconds	3-51
Display “O/I” for Operator and International Calls	3-51
Display Redirected Station.	3-52
Display “T” for Two B-Channel Transferred Calls	3-52
Record Calls.	3-52
Suppress Digits Options.	3-53
Remote Configuration	3-54
Enabling Remote Configuration in DB Programming.	3-54
DB Programming Remote Configuration Options	3-54
Enabling an On-Demand Remote Connection.	3-55
Enabling an On-Demand Remote Connection from an Endpoint	3-56

Introduction

This chapter describes features that you can use to manage and maintain your Mitel 5000 system. System management options include:

- “Passwords” on [page 3-4](#)
- “System Software Licenses” on [page 3-6](#)
- “Database Backup Options” on [page 3-12](#)
- “Scheduled Backups” on [page 3-15](#)
- “System Maintenance Options” on [page 3-36](#)

NOTICE

System Performance. Perform the following system management options after hours, when system usage is at a minimum.

- DB backup saves (with a large database, especially with off-node devices).
- Paging to a large number of endpoints.
- All-ring hunt groups to a large number of endpoints.
- Change extension logic. (DB Programming performs a batch modify or delete extension (the larger the database, the slower the action).

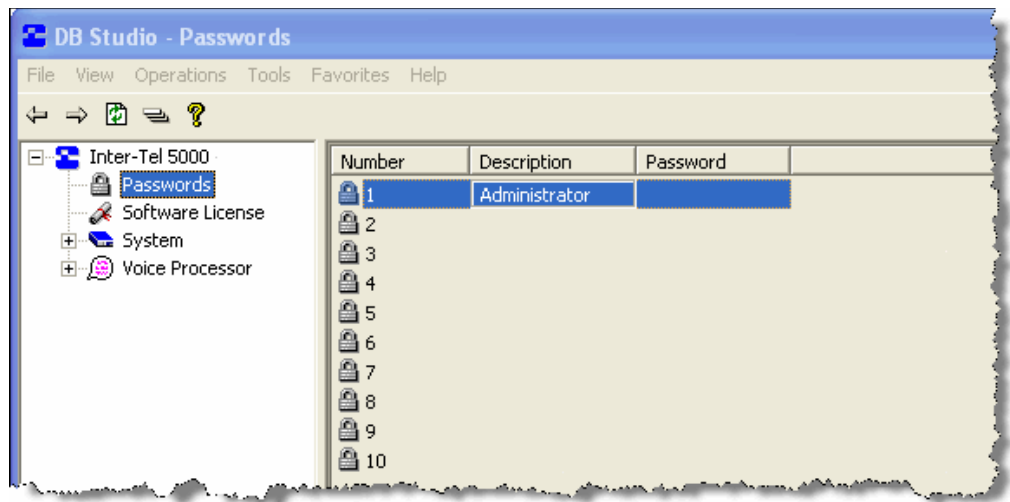
Passwords

System password and access rights are located in the Passwords directory (PASS). The Passwords folder contains 10 password entries that allow you to set the description (up to 20 characters) and define the password. You can program access rights for passwords 2–10. The first password is the administrator password. This selection cannot have its access rights customized, and the administrator can always use everything in DB Programming.

Administrators can use their password (password #1) as the old password when changing other passwords (such as network, socket, and so on). For example, if changing a socket connection password, the administrator password is accepted as a valid entry in the Old password text box. This capability allows administrators to change passwords that may have been forgotten.

When you right-click a password, the **Edit Password** and **Edit Access Rights** options display.

Figure 3-1. Password Directory



Programming a Password

To program a password:

1. Right-click the password number you want to set, then select **Edit Password**. The Edit Administrator Password dialog box appears.
2. In the **New Password** box, type the new password (up to 8 characters). Typed characters appear as asterisks (***).
3. Retype the password in the Confirm password box.
4. Click **OK** to exit and save the password. If the entered passwords match, you will return to the Password field. If not, you must re-enter the new password and verify it again. If you make a mistake while entering the password or want to leave it unchanged, click **Cancel**.

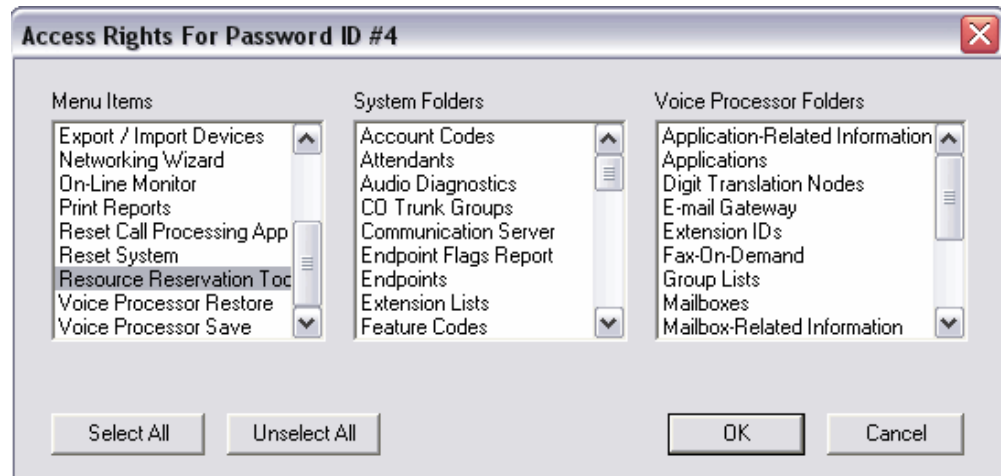
A system password will be requested at the start of each programming session, unless there are no passwords in the database. Passwords can be programmed in any order or left blank. If one or more passwords are left blank, pressing **ENTER** when the Request System Password dialog box is displayed allows access to the highest level containing a blank password.

Assigning Administrator Access Rights

You can assign administrator access rights for each administrator. You cannot program access rights for the administrator—password #1.

To assign administrator access rights:

1. Right-click the password number that you want to program, and then select **Edit Access Rights**. The following dialog box appears.



2. Select the menu items, system folders, and voice processor folders to which the password user will have access. Or, click **Select All/Unselect All** to select or to clear every item in every list. To select or clear multiple items listed consecutively, press **SHIFT** while selecting the first and last item within a list. To select or clear multiple items **not** listed consecutively, press **CTRL** while making the selections.

NOTE

There are two special cases to note.

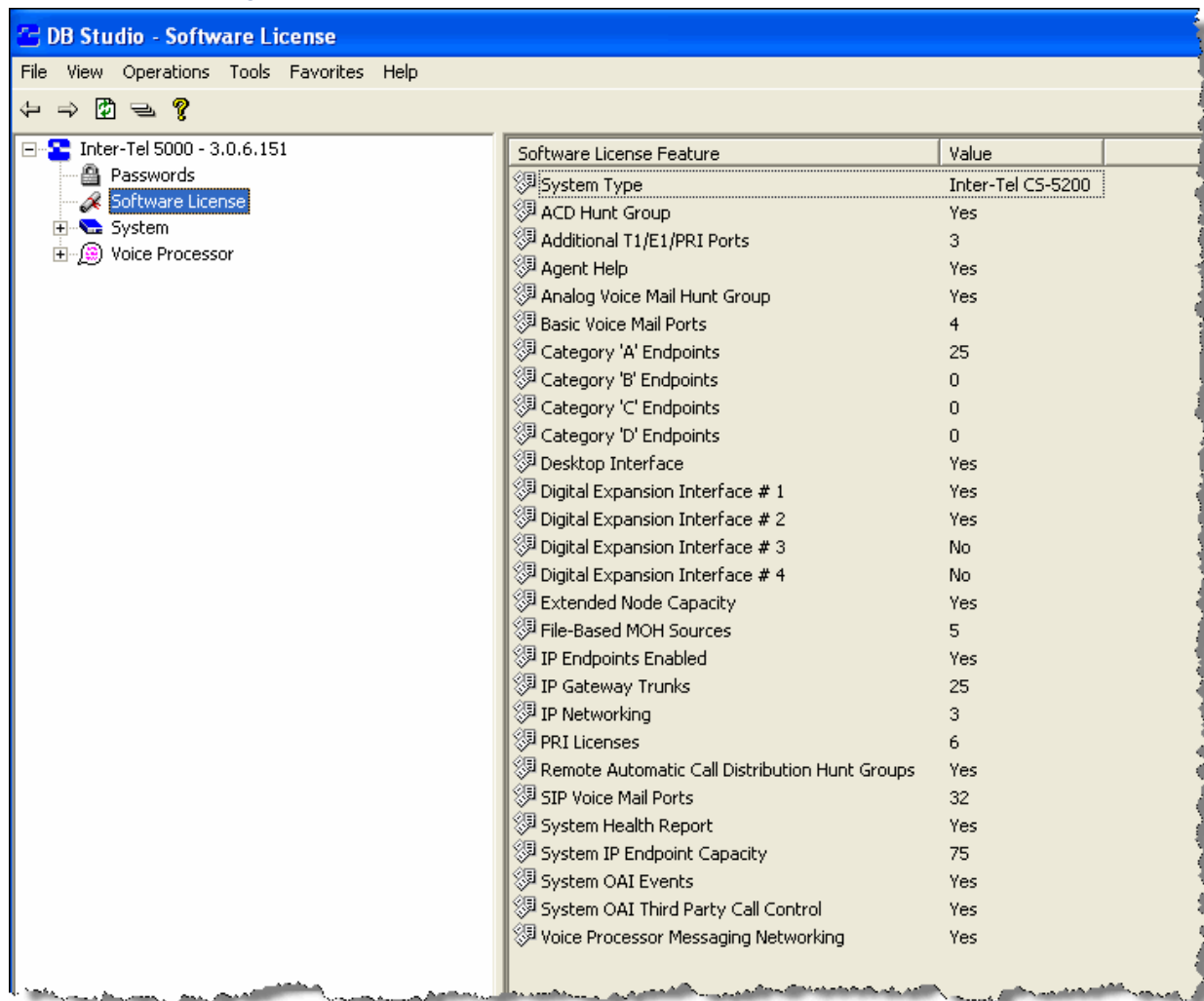
- To gain access to the items in the System root folder, select Communication Server in the System Folders.
- To gain access to the items in the voice processor root folder, you must select Networking in the Voice Processor Folders.

3. Click **OK**. Although a user can be given access to the Password folder, the user is allowed to edit only their own description and password. The user is **not** allowed to edit other passwords or descriptions.

System Software Licenses

You can view the software licenses and values currently uploaded to the system, including features common to all licenses. Software licenses are read-only, as shown in [Figure 3-2](#).

Figure 3-2. Software License Directory Display



To view software licenses:

Select **Software License**. Software licenses are shown in the right pane.

The detailed information about software license features is shown in [Table 3-1](#). The values shown are for local mode. In remote mode, the values match the software license that is loaded. If there is no license loaded or the current license on the system is invalid, the fields display with a red "X."

Mitel 5000 systems require a version-specific license. You can install and run DB Programming, but you are prompted to upload the license file. For information about uploading a software license and for a list of features that require licenses, see "Software License Operations – Upload Software License" on [page 3-10](#).

NOTICE

You must upgrade system software *before* loading the license.

Table 3-1. Software License Descriptions

Field	Description
System Type	Displays the system type associated with the license that is loaded to the system. This field should match the system type of the About Software License dialog on page 3-9 .
ACD Hunt Group	Indicates whether or not the ACD Hunt Groups software license is uploaded to the system.
Additional T1/E1/PRI Ports	Indicates how many additional Dual T1/E1/PRI port licenses are uploaded to the system.
Agent Help	Indicates whether or not the Agent Help software license is uploaded to the system.
Analog Voice Mail Hunt Group	Indicates whether or not the Analog Voice Mail Hunt Group software license is uploaded to the system.
Basic Voice Mail Ports	Indicates how many Basic Voice Mail port licensed are uploaded to the system.
Category A Endpoints	Indicates how many Category A endpoint licenses are uploaded to the system.
Category B Endpoints	Indicates how many Category B endpoint licenses are uploaded to the system.
Category C Endpoints	Indicates how many Category C endpoint licenses are uploaded to the system.
Category D Endpoints	Indicates how many Category D endpoint (Mitel Models 5212, 5224, 5330, and 5340) licenses are uploaded to the system.
Desktop Interface	Indicates whether or not the Desktop Interface software license is uploaded to the system.
Digital Expansion Interface #1	Indicates whether or not the Digital Expansion Interface # 1 software license is uploaded to the system.
Digital Expansion Interface #2	Indicates whether or not the Digital Expansion Interface # 2 software license is uploaded to the system.
Digital Expansion Interface #3	Indicates whether or not the Digital Expansion Interface # 3 software license is uploaded to the system.
Digital Expansion Interface #4	Indicates whether or not the Digital Expansion Interface # 4 software license is uploaded to the system.
Extended Node Capacity	Indicated whether or not the IT-5000 License Enable 99 Nodes software license is uploaded to the system. For more information about 99 Nodes requirements, refer to the Specifications chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
File-Based MOH Sources	Determines how many File-Based MOH sources can be used on the system.
IP Endpoints Enabled	Indicates whether or not the IP Endpoints Enabled software license is uploaded to the system.
IP Gateway Trunks	Indicates how many IP gateway trunk licenses are uploaded to the system.
IP Networking	Indicates how many IP networking trunk licenses are uploaded to the system.
PRI Licenses	Indicates how many PRI licenses are uploaded to the system.

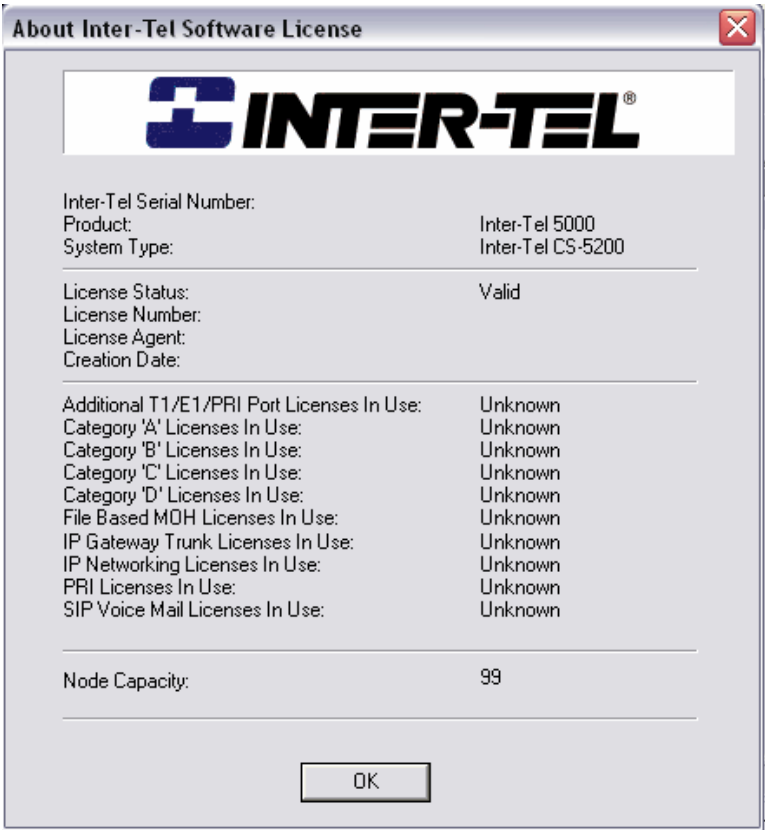
Table 3-1. Software License Descriptions (Continued)

Field	Description
Remote Automatic Call Distribution Hunt Groups	Indicates whether or not the Remote Automatic Call Distribution Hunt Groups software license is uploaded to the system.
SIP Voice Mail Ports	Determines how many SIP Peer Voice Mail Ports can be used on the system.
System Health Report	Enables the System Health Report feature.
System IP Endpoint Capacity	<p>This feature determines the maximum capacity for IP endpoints on the system (75 on a CS-5200, 175 on a CS-5400, 250 on a CS-5600). If you do not have the IP Endpoints Enabled license, the System IP Endpoint Capacity corresponds to the number of Enable IP Endpoint Units license in the license generator.</p> <p>The System IP Endpoint Capacity value is determined as follows:</p> <ul style="list-style-type: none"> • If the IP Endpoints Enabled license is enabled, the System IP Endpoint Capacity is either 75, 175, or 250 (depending on the system type 5200, 5400, or 5600 respectively). • If the IP Endpoints Enabled license is disabled, the System IP Endpoint Capacity is the lesser of the Enable IP Endpoint Units license (in the license generator) or the total of all category licenses.
System OAI Events	Indicates whether or not the System OAI Events software license is uploaded to the system.
System OAI Third Party Call Control	Indicates whether or not the System OAI Third Party Call Control software license is uploaded to the system.
Voice Processor Messaging Networking	Indicates whether or not the Voice Processor Messaging Networking software license is uploaded to the system.

About Software License

The About Software License dialog box shows current licenses allocated for your system, as shown in [Figure 3-3](#).

Figure 3-3. About Software License



Software License Operations – Upload Software License

You must upload a software license to the Mitel 5000 system. If you do not upload a software license, the system considers the license invalid and issues Alarm 125. For a complete list of alarm messages, refer to the *Message Print Diagnostics Manual*, part number 550.8018.

NOTE

The USB security key and secure socket layer (SSL) serial number is stored on the USB security key. The license must match the serial number on this key or the upload fails.

If for any reason you need to replace the USB security key, make sure you upload the latest license file *before* replacing the key.

Attempting to upload a license file after changing the USB security key results in an error and the system does not function. If the USB security key is not installed when the system reboots, the software license needs to be uploaded.

To upload a software license:

1. From the DB Programming menu bar, select Operations – Software License Operations – **Upload Software License**.
2. Enter the path and name of the license file (.isl) or click Browse to search for the file.
3. Click **Start**. The system compares the new software license to the existing license, if applicable.

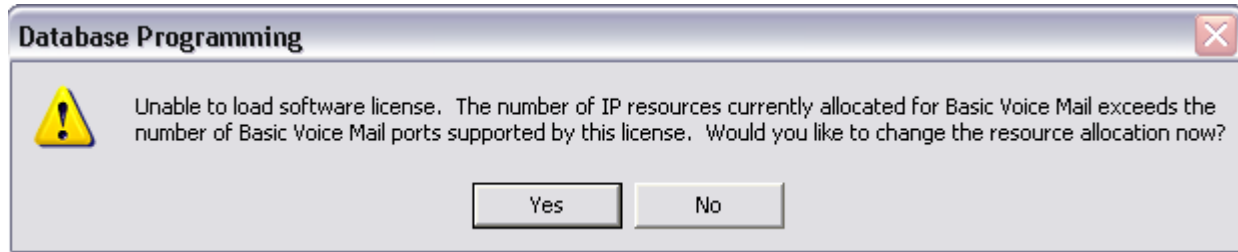
NOTE

If you click Start before selecting a license (.isl), a message displays, informing you that you have not identified a file name.

4. Click **Finish** at the Compare Software License screen. If you upload a software license that does not support your current programming, a warning message appears.

Comparing or Uploading a Software License

When you upload a software license, the system checks the Basic Voice Mail (BVM) ports available in the new license and the current resources allocated to BVM. If the current resources allocated exceed the number of licensed BVM ports, you are prompted to change the resource allocation.



If you click **Yes**, the view is changed to the System – Communication Server – IP Settings – IP Resource Allocation folder so you can change the IP resources allocated to BVM.

If you click **No**, you return to the folder you were viewing, prior to the software license upload, and the upload is canceled.

You must license additional BVM ports. If you downgrade a license to support fewer BVM ports, DB Programming performs a check on the Time Slot Groups (see "Time Slot Groups" on [page 11-27](#)). If the Time Slot Groups currently have a Maximum Channel Allocation greater than the new license supports, a warning message appears, preventing you from uploading the license. You are prompted to go to the Time Slot Groups folder and change the Maximum Channel Allocation fields to a value that is supported in the new license. If you do not go to the Time Slot Groups or you click **Cancel**, you are returned to DB Programming and the new license is not loaded.

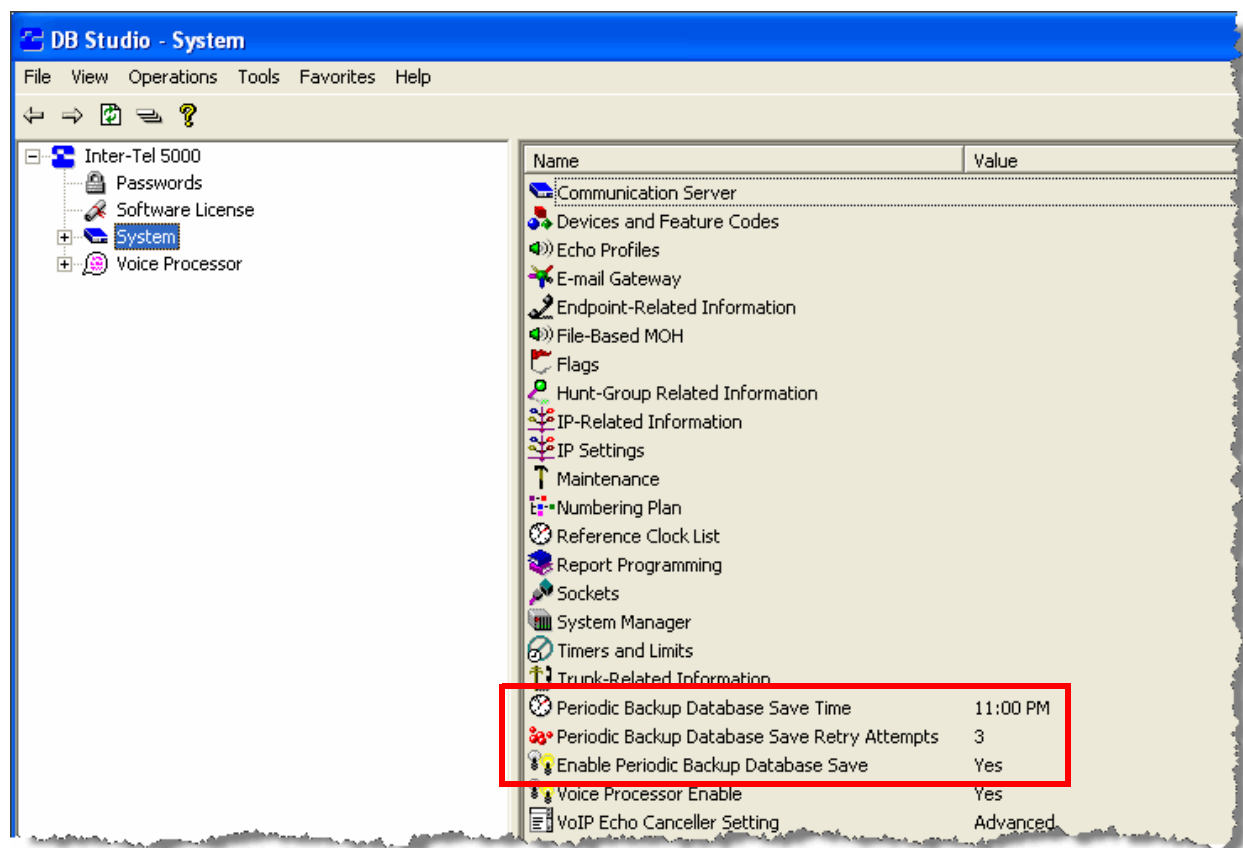
BVM ports, IP Endpoint Categories, and Node Capacity are displayed in the Compare License dialog box.

Database Backup Options

A backup copy of the system database is automatically stored on the compact flash-type Mitel memory card located on the front of the Mitel 5000 Base Server. This backup remains available, even if the system experiences a power failure or if the battery backup loses power. If the system is powered up and a corrupt database file is detected, the backup file in flash memory or on the compact flash (CF) drive is restored. You can program an automatic backup as described below. Database Backup options are located in the System folder, as shown in [Figure 3-4](#). For information about voice processing database maintenance, see “Saving and Restoring Voice Processing Databases” on [page 13-3](#).

NOTE The voice processor database is not stored in flash memory.

Figure 3-4. Backup Database Parameters



The following are database backup options:

- **Periodic Backup Database Save Time:** The time of day when a scheduled database backup occurs. This must be at least 15 minutes after the Scheduled Reset Time; otherwise, the backup may not occur. If you enter a time that is less than 15 minutes after the Scheduled Reset Time, a message appears, requesting a new value. By default, this is 11:00 P.M.

NOTE

If Daylight Saving Time is enabled, Mitel recommends that you do *not* program the backup to occur at 2:00 PM. If you do, the backup may not occur on the day that the time changes.

- **Periodic Backup Database Save Retry Attempts:** The number of times that DB Programming attempts to save the database. If the database is not saved before the system retries the number of times specified in this field, the database is not saved until the next day. The range is 0–10; the default is 3.
- **Enable Periodic Backup Database Save:** Enable this option to save the database at the time indicated in the Periodic Backup Database Save Time option. This option must be enabled to backup the database at the scheduled time. By default, the option is enabled.

To disable the Enable Periodic Backup Database Save option:

1. Select **System**. Backup options are shown in the right pane.
2. In the **Value** column, clear the check box. The field changes to **No**. To enable the option, select the check box.
3. Click out of the field or press **ENTER** to save the change.

NOTE

If the system detects that the database has not changed since the last backup, the save is not performed.

Backup Database Save

A backup copy of the database is automatically stored on the system memory card. This backup remains available, even if the system experiences a power failure or if the battery backup loses power. If the system is powered up and a corrupt database file is detected, the backup file in flash memory is restored.

NOTE The voice processor database is *not* stored in flash memory.

This backup database is designed to recover in the event of a total power failure—it is not designed to replace the static database. Changes made to the static database are, not reflected in the backup database until the database is automatically or manually backed up. For example, if you default the database, the static database is defaulted, not the backup database.

The backup database allows the system to automatically convert databases when the software is upgraded. For example, if the system is upgraded from v2.4 to v3.0, the v2.4 static database is detected and considered corrupt. When this occurs, the system restores the backup database and converts the information to a v3.0 static database. The backup database version, however, does not change until a backup is performed (it remains a v2.4 database).

The system repeatedly attempted to restore a backup database but was interrupted by power-ups. If the static database is corrupted, the system attempts to restore the backup database. If the system detects problems with the backup database, it may default the static database instead of restoring the backup database. The database is defaulted if one of the following occurs:

- There is no backup database available.
- The system was saving the backup database when the power down occurred.
- The system repeatedly attempted to restore a backup database but was interrupted by power ups. The system defaults the database after it has exceeded the number of restore attempts, as specified in DB Programming. If this occurs, the backup database remains in flash memory for troubleshooting purposes.

If desired, you can force DB Programming to save the backup file immediately, as described below or schedule a backup (see [page 3-15](#)). To set Backup Database Save parameters, see [page 3-12](#).

To force a backup database save:

1. Select Operations – Database Operations – **Backup Database Save**.
2. Click **Start** to create the backup. The backup file is saved and stamped with the new date and time.

Scheduled Backups

The Mitel 5000 system contains a significant amount of data. This data includes the system configuration database as well as voice data (messages, prompts, custom recordings, etc.). The system database is automatically backed up daily, but this is within the phone system on the same media. In the event of a media failure, the system database and voice mail recordings will all be lost back to the point of the last manual backup (see [page 13-3](#)). In the field, months may elapse between manual backups.

With Scheduled Backups, you can configure the frequency and times at which automatic backups will be performed and the locations in which to store the backups. The backups contain the system database and (optionally) voice processor data.

A software license is not required for this feature. Scheduled Backups are supported for both standard IP connections and modem connections.

For modem connections, note the following:

- You may enable or disable the modem speaker as desired. If left turned on, it just makes noise while the scheduled backup is running. If turned off, it is off for both scheduled and manual database programming operations.
- During Scheduled Backups, the “Redial attempts” and “Time between redial attempts” settings programmed for the modem connection through the standard Windows Properties\Options dialog are not used. Rather, retries and the wait between retries are governed by the programming for Scheduled Backups.

Scheduled Backups automates the exact same process followed to do a manual System Database and Voice Processor Save. DB Programming has much control over the System Database Save. It queries the Mitel 5000 for the database information and creates an archive in the indicated folder. The archive file holds the database description and content. Then, if options are selected to include Voice Processor data in the Save, Database Programming commands the Voice Processor (either BVM or EM) to save its data to the indicated folder. DB Programming has no further control over the Voice Processor Data Save once the command is sent. It will receive status back from the Voice Processor indicating the resulting status.

Currently, Scheduled Backups are not supported for Remote Configuration connections.

Session Manager Service Configuration: There is a new “Scheduled Backups” menu option in the Session Manager. You can program backup configuration settings per session in the Scheduled Backups dialog box. These settings include enable or disable backups, backup frequency and time, backup location, and other parameters.

You can also program global settings through the Scheduled Backups Settings dialog box, such as the maximum number of simultaneous backup sessions allowed, maximum number of retries, duration between retries, etc. The Scheduled Backups programming is stored by the System Manager in the registry, along with all of the other Session Manager data. See [page 3-16](#) for programming information.

Windows Task Scheduler: The Session Manager enters and maintains the backup task scheduling information in the Windows Task Scheduler. After a backup is programmed and scheduled, a backup is performed at the appointed time by the Windows Task Scheduler. Each time changes to Scheduled Backups are made and saved with the Session Manager, the associated task in the Windows Task Scheduler is deleted (if it exists) and re-created with the new programming.

NOTICE

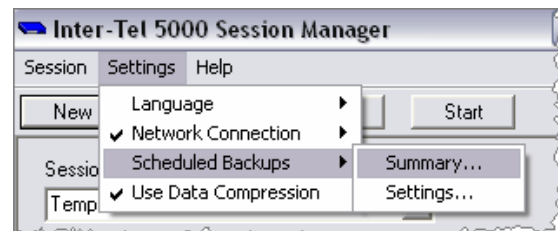
Possible Data Corruption. Although you have the ability to view, modify, and delete the scheduled task(s) directly in the Windows Task Scheduler, do **not** change the scheduled tasks information in the Windows Task Scheduler. If you modify the tasks in the Windows Task Scheduler, Scheduled Backups may fail.

Service Log: A Service Log file is maintained for each session for diagnostic purposes. Entries are made by the Session Manager and DB Programming during each backup attempt, including specific information about the operation, any warning and error messages, and completion status. See [page 3-32](#) for details.

Setting Scheduled Backups for a Session

The Scheduled Backups feature contains the following options:

- “[Viewing the Scheduled Backups Summary](#)” below
- “[Setting Scheduled Backups for All Sessions](#)” on [page 30](#)



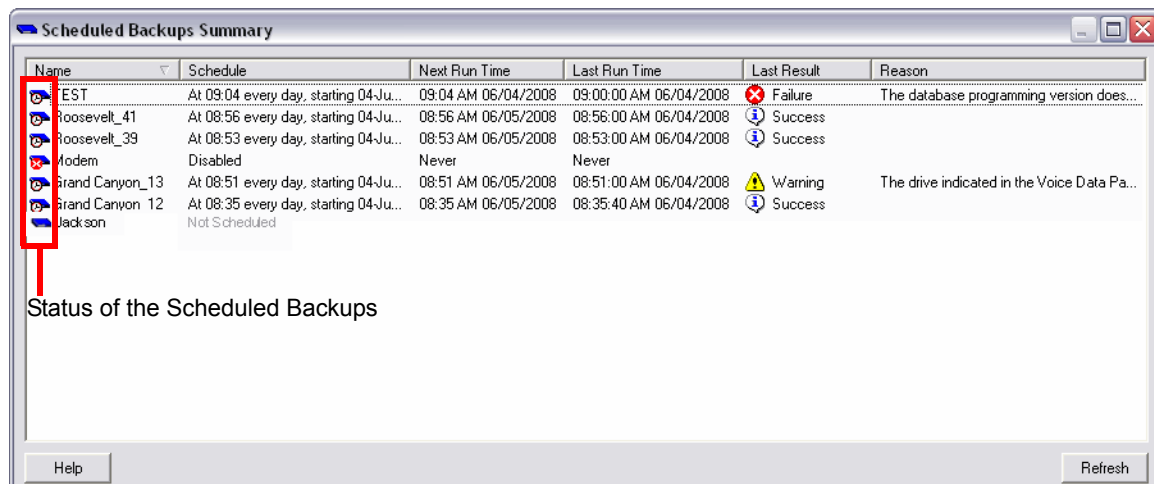
Viewing the Scheduled Backups Summary

The Scheduled Backups Summary dialog box shows a summary of the Scheduled Backups for all programmed remote sessions that have v3.0 or later systems. This dialog box also has the option to program Scheduled Backups settings for a session (see [page 3-16](#)). To program Scheduled Backups settings for all sessions, see “[Setting Scheduled Backups for All Sessions](#)” on [page 30](#).

To view the summary:

Select Session Manager – Settings – Scheduled Backups – **Summary**. The Scheduled Backups Summary dialog box appears as shown below.

Figure 3-5. Scheduled Backups Summary



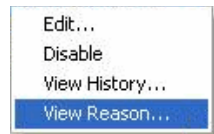
When there is no session created, the dialog box is blank. When a new session is created or started, the session name appears in the dialog box with the current scheduling programmed, the time the backup was last attempted, and the result from that last backup attempt. If the backup did not complete successfully, the Reason column includes a brief description of the warning or failure reason. See “Scheduled Backups – Warnings and Error/Failure Reasons” on [page 17-58](#) for a detailed list of failure reasons and warnings.

Status of the Scheduled Backups: The icon next to each session name indicates whether the Enable Scheduled Backups check box (see [page 3-19](#)) for the session is:

- enabled (🕒, timer),
- disabled (🚫, red “X”), or
- not yet scheduled (🔲, plain blue box).

Refresh Button (F5): Re-reads all information from the registry and refreshes the display.

You can take one of the following actions on a per-session basis by right-clicking a session:



- **Edit:** Opens the Scheduled Backups dialog box to program backup configuration settings for a session (see “[Scheduled Backups Configuration Outlines](#)” below).
- **Enable/Disable:** Shows “Enable” when backups are disabled for the session, and “Disable” when backups are enabled for the session. Selecting this option enables or disables backups for the session. This option is unavailable if no scheduled backups or Scheduled Backup configuration test have yet been programmed for the session.
- **View History:** Opens the Scheduled Backups History dialog box to view the scheduled backups results for a session (see [page 3-28](#)). This option is unavailable if no scheduled backups or Scheduled Backup configuration test have yet been programmed for the session.
- **View Reason:** Opens the Reason dialog box to view the full reason of a failure or warning status (see [page 3-29](#)). This option is unavailable if the Reason column is blank.

Scheduled Backups Configuration Outlines

This section provides the outlines for preparing and programming Scheduled Backups for a session.

To prepare scheduled backups for a session:

1. Designate and prepare the “Save system database to” folder (or use the default, recommended).
2. Determine whether or not Voice Data is to be saved, and if so, designate and prepare the “Save voice data to” folder.
3. Determine the Windows Login Username and Password to be used for the Scheduled Backups.
4. Procure the Database Programming Password, if needed, to gain Database Save privilege to the target Mitel 5000.

5. If E-mail Notification is to be used:
 - a. Designate a Scheduled Backups Administrator to receive the e-mail notifications for Scheduled Backups attempts. Note the desired e-mail address(es).
 - b. Prepare the Sender information:
 - If the Username entered for Scheduled Backups has a default profile that you want to use for e-mail authentication, you just need the name of the server. You can read this from the default profile account properties.
 - If there is no default profile or you do not want to use that account for e-mail authentication, you need a valid e-mail account for sending the e-mail, along with the Username, Password, and Server.
 - Determine the Name and Address you want to specify for the Sender. This is the name that appears in the e-mail client. The Address can be anything as well, but if you want to allow for Recipients to reply to this e-mail notification (not necessary), you can use a valid e-mail address and associated name.
6. Determine the desired scheduling for the backups.
7. Review the Scheduled Backups Settings defaults and determine if different values are needed.

To program scheduled backups for a session:

1. At the computer used for the Scheduled Backups, program the Session Manager as needed to set up a Network Session for the target Mitel 5000.
2. Perform a manual Database Save from the Mitel 5000 to the designated location, including voice data, if designated, to the designated voice data location.
3. Address any problems with the Network Session and manual Database Save.
4. Program Scheduled Backups as described in “Programming Scheduled Backups” on [page 3-19](#).
5. Make sure the Enable Scheduled Backups check box is selected (see [page 3-19](#)).
6. When finished, click **OK**. If all entries are valid, any changes made are saved in the registry.
 - If there are any invalid entries, an error message appears, and you are moved to the offending tab to make the entries valid. See “Scheduled Backups – Error Messages” on [page 17-65](#) for a list of programming error messages and troubleshooting tips.
 - If the Enable Scheduled Backups check box is selected, the Scheduled Backup Task for the session is created (or re-created, if it existed before).
 - If the Enable test of Scheduled Backup at: START TIME check box is selected in the Test tab, that test is also scheduled at this time (see [page 3-27](#)).
 - You can click **Cancel** to leave the dialog at anytime. If there are any changes that are not yet saved, a warning message appears.
7. Before the test of the Scheduled Backup configuration starts:
 - Log off from the computer. This is not required, but it ensures that the Authorization programming is tested.
 - Reboot the computer. This is not required, but it simulates the worst case scenario of a power outage occurring prior to a scheduled backup.

8. When the backup has had time to complete, log on to the computer and monitor the following results:
 - If E-mail Notification was programmed and the Notify only if Scheduled Backups fails check box was selected, there should only be an e-mail message posted if there was a problem. Check for this first and take action accordingly. If the check box was cleared, there should be a success message.
 - There should be a posting in the Windows Event Viewer, indicating success or failure (and reason). See [page 3-33](#) for details.
 - The Service Log should contain entries for the backup attempt. See [page 3-32](#) for details.
 - If the attempt succeeded, the new backup file(s) should now exist in the programmed location(s).

The programming is completed. Make sure the computer is left powered-up with supporting equipment allowing it to connect to the Mitel 5000 at any time.

Programming Scheduled Backups

The Scheduled Backups dialog box contains the following tabs to organize the programming:

- “[Location Tab](#)” below
- “Authorization” on [page 3-23](#)
- “Notification” on [page 3-24](#)
- “Scheduling” on [page 3-25](#)
- “Test” on [page 3-27](#)

Enable Scheduled Backups: The Enable Scheduled Backups option applies to all of the tabs and indicates whether or not backups are enabled for the session. When v3.0 or later DB Programming is installed, backups are automatically disabled for all pre-existing sessions. The Summary column in the Scheduled Backups Summary dialog box displays “Not Scheduled” (see Figure 3-5 “Scheduled Backups Summary” on [page 3-16](#)). This is the case also, when a new session is created.

However, as soon as you open the Scheduled Backups dialog box for the first time for a session, backups for the session are automatically enabled. That is, the Enable Scheduled Backups check box is automatically selected. From that point on, this check box will not be automatically selected or cleared. If you clear it, it will not be selected again until you select it.

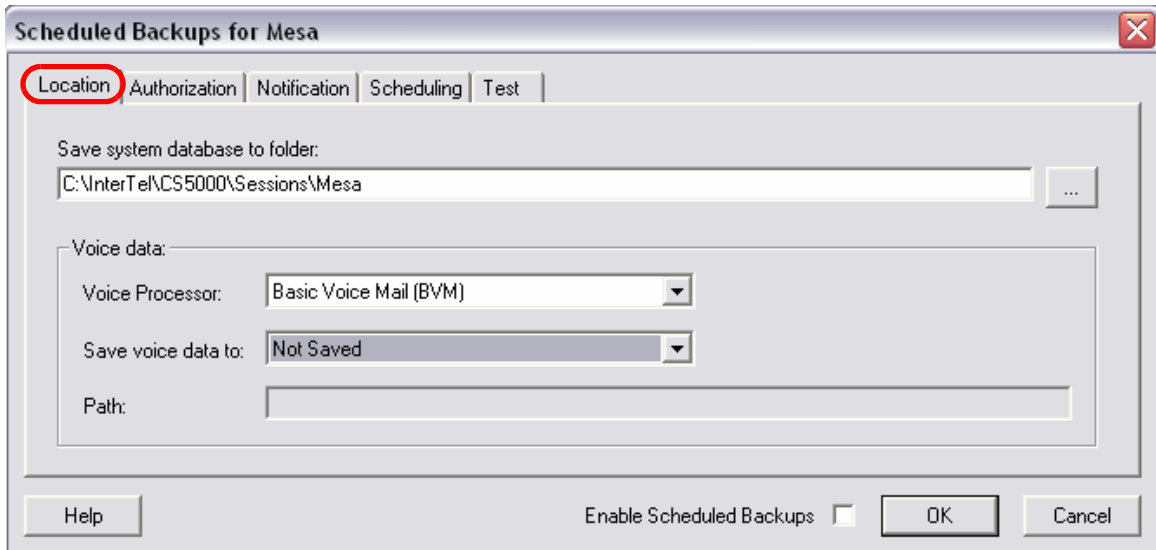
The status of this option is displayed in the icon used in the Scheduled Backups Summary dialog box (see Figure 3-5 “Scheduled Backups Summary” on [page 3-16](#)).

Location Tab

The Location tab allows for programming what is backed up and where the backups are stored. If you encounter an error, see “Scheduled Backups – Error Messages” on [page 17-65](#) for a list of possible programming error messages and troubleshooting tips.

To open the **Location** tab, do one of the following:

- Double-click a session name in the **Name** column on the Scheduled Backups Summary dialog box.
- Right-click a session name in the **Name** column, and then select **Edit**.
- Right-click an entry on the Scheduled Backups Summary dialog box, select **Edit**, and then click the **Location** tab, as shown in the following example.



The Location tab contains the following options:

- **Save system database to folder:** Determines the folder for the system database backup file. If desired, use the default provided: a folder named after the session, created under the Sessions folder in the installation location (as shown above).

NOTE

Do not use a mapped drive for the location because a mapped drive becomes disconnected when you log off of the system. Program your backup to use the full definition of the path.

To change the path, do one of the following:

- Type a different path.
- Use the browse button to the right of the text box to navigate to the folder you want. This allows for storing of backups on a different hard drive or even a network drive.

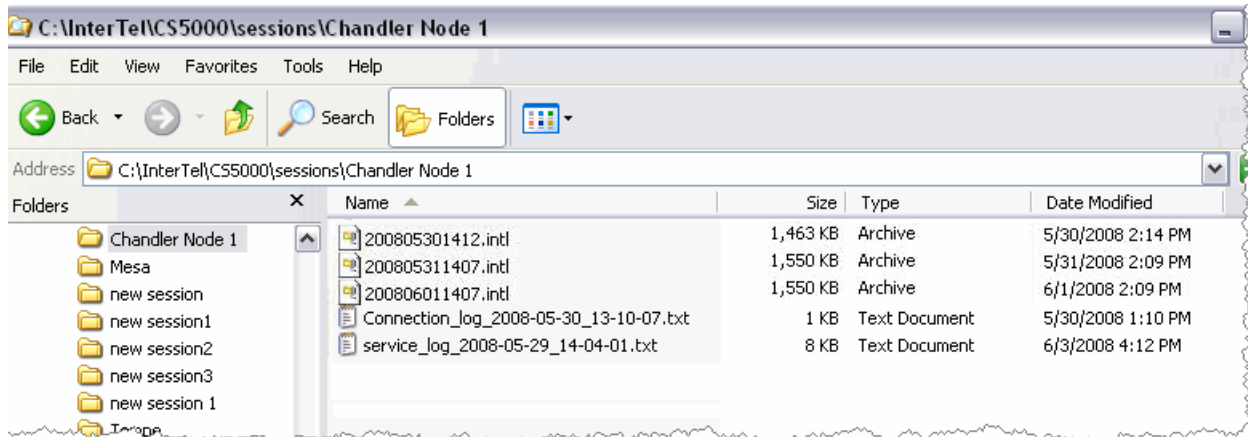
The backed up system database files are named simply with a date/time stamp and the intl suffix: `yyyymmddHHMM.intl`.

Because the Schedule Backup Feature keeps only a limited number of files (as specified in the Settings dialog box on [page 3-30](#)), direct backups for each session to a new folder that includes the session name. Any existing database backups in the directory are subject to the file limit, so keep scheduled backups separate from manual backups.

The full path is limited to up to 60 characters, and the path does not include a session name in the file name. You must store the files in separate folders named for each session. See "Scheduled Backups – Error Messages" on [page 17-65](#) for the related error event log.

Figure 3-6 on [page 3-21](#) shows an example of the system database files in the sessions folder. To configure a global setting to indicate how many backups per session to keep, see [page 3-30](#).

Figure 3-6. System Database Files



- **Voice Data:** Consists of all store voice mail recordings (messages, prompts, names, fax documents, etc.). These are stored in the voice processing unit. If there is a voice processing unit attached to the system, you can back up voice data in one of the following voice processing units along with the system database:

NOTE

NuPoint Messenger is not backed up as part of this automatic backup procedures. For information about how to backup NuPoint Messenger voice data, refer to the NuPoint Messenger documentation.

- *Voice Processor:* Specifies the Voice Processor type:
 - None (default)
 - Basic Voice Mail (BVM)
 - Enterprise Messaging (EM)
 - Processing Server Basic Voice Mail (PS-BVM)

When “None” is selected, no voice data is saved with the Scheduled Backup and the other fields in the Voice data frame are disabled. When a Voice Processor is anything other than “None,” the applicable fields become enabled. At this point, voice data may or may not be saved, depending on the selection in the Save voice data to box (see below).

- **Save voice data to:** Specifies a location for the voice data file. [Table 3-2](#) shows the available options, along with the Voice Processor types for which they are offered. Whenever the Voice Processor type is changed, the selection in this box is changed back to “Not Saved.”

Table 3-2. Voice Data Save Locations

Location	Indicates:	Voice Processor Type:		
		BVM	EM	PS-BVM
Not Saved (default)	Voice data is not backed up. In this case only, the Path field is disabled.	✓	✓	✓
USB Port	Voice data is backed up through the USB port, either on the Mitel 5000 itself (BVM, PS-BVM) or on the EM unit.	✓	✓	✓
EM Local	Voice data is backed up on the local hard drive in the EM unit.		✓	
Windows Server	Voice data is backed up to a Windows network location. In this case, the Path must contain a valid Windows network address.			✓
NFS (Network File System) Server	Voice data is backed up to an NFS (Unix/Linux) network location. In this case, the Path must contain a valid NFS network address.			✓

- **Path:** When the Save voice data to box is set to anything other than “Not Saved,” the Path is defaulted according to the selection:
 - **USB Port:** Type a folder or subfolder name in which to store the voice data. For BVM and PS-BVM, the path must always begin with `U: /`. For EM, the path must always begin with `F: \`.
 - **EM Local:** Type a folder or subfolder name in which to store the voice data. The drive letter must always be `D: \`, and the default is `D: \Backup`.
 - **Windows Server** and **NFS Server:** Type a valid network address including the server name and folder.

NOTE When saving voice data in PS-BVM, type `\\<hostname>\<path>`. When saving voice data in NFS Server, type `/<hostname>/<path>`. If the host name does not exist in the path, the Voice Data Backup fails (see “Viewing Failure or Warning Reasons” on [page 3-29](#)).

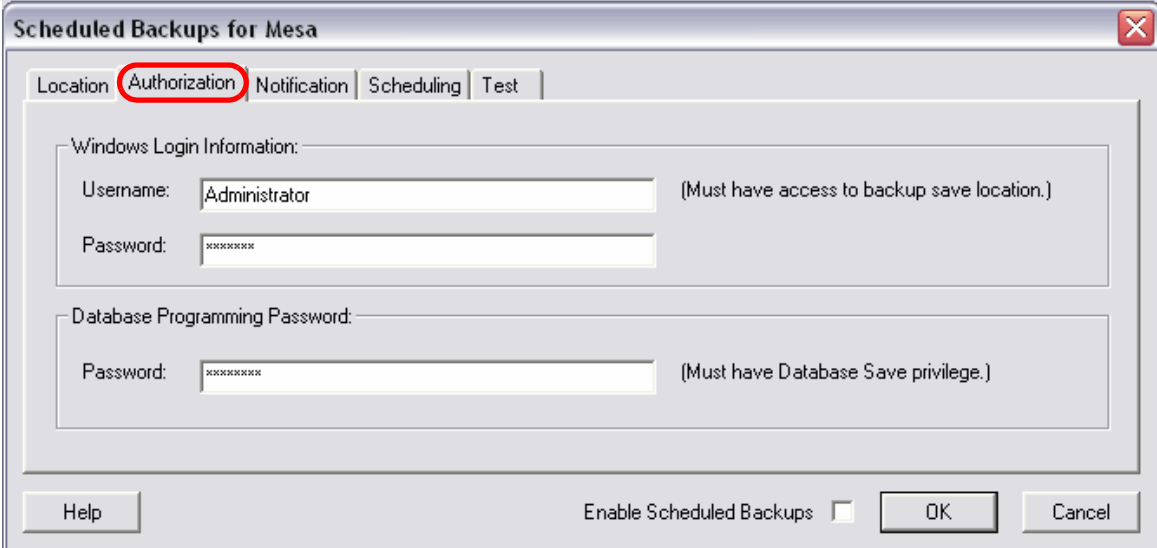
At the time of programming in the Session Manager, the Path cannot be validated. Make sure the Path is valid by scheduling a Scheduled Backup configuration test (see [page 3-27](#)). When the Scheduled Backup (or test) runs, if the Path is invalid, an error message is recorded and the voice data backup fails.

Authorization Tab

You can view and modify the backup authorization programming in the Authorization tab. If you encounter an error, see “Scheduled Backups – Error Messages” on [page 17-65](#) for a list of possible programming error messages and troubleshooting tips.

To open the Authorization tab, do one of the following:

- Double-click an entry on the Scheduled Backups Summary dialog box, and then click the **Authorization** tab.
- Right-click an entry on the Scheduled Backups Summary dialog box, select **Edit**, and then click the **Authorization** tab, as shown in the following example.



The screenshot shows the 'Scheduled Backups for Mesa' dialog box with the 'Authorization' tab selected. The 'Location' tab is also visible. The 'Authorization' tab contains two sections: 'Windows Login Information' and 'Database Programming Password'. The 'Windows Login Information' section has a 'Username' field with 'Administrator' and a 'Password' field with asterisks. The 'Database Programming Password' section has a 'Password' field with asterisks. At the bottom, there is a 'Help' button, an 'Enable Scheduled Backups' checkbox, and 'OK' and 'Cancel' buttons.

The Authorization tab contains the following options:

- **Windows Login Information:** A user name and password must be programmed to execute scheduled backups successfully even when you are not logged into the system (for example, after a system reboot, during the night when no user is logged in to the computer, etc.)
 - *Username:* The user name must be associated with the required privileges to access the destination location(s) for the backup file(s). When a session is created, the user name is defaulted to that of the person creating the session. To change the user name, type the user name that you want to use.
 - *Password:* When backups are scheduled for the first time, or whenever the user name is changed, the Password box is blank. Type the Windows Login Password in the Password box. Characters appear as asterisks (*).
- **Database Programming Password:** A Database Programming Password may be required in order for DB Programming to access the Mitel 5000 to perform the database save. The password programmed must have the Database Save privilege. Characters appear as asterisks (*). It is set to blank by default.

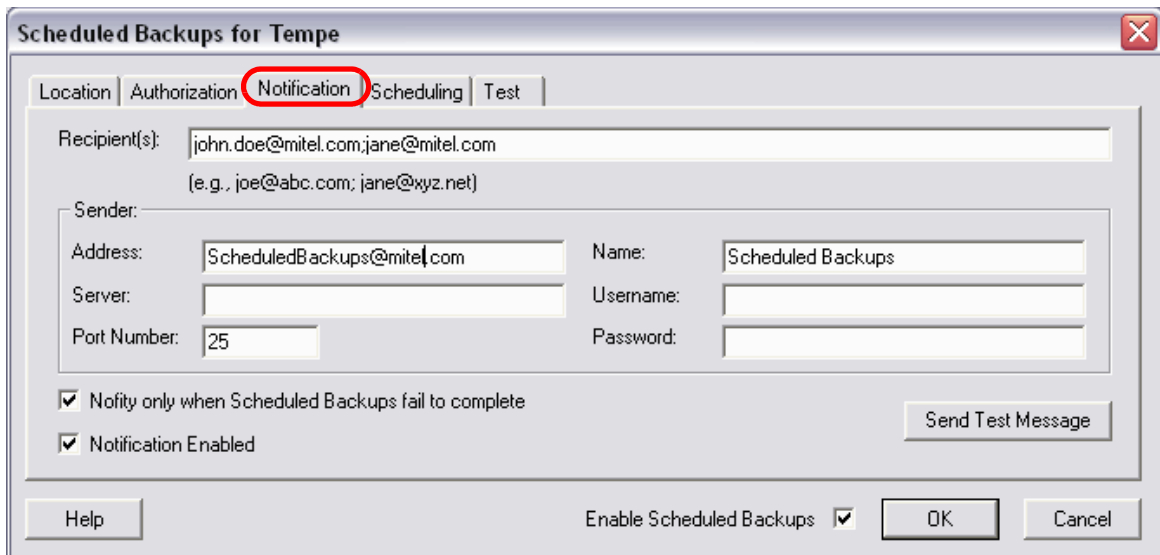
When the Scheduled Backups actually take place, if the Username or Password is invalid, this failure is recorded and the backup is not performed. Perform a test of the Scheduled Backup configuration (see [page 3-27](#)) to ensure the proper authorization has been programmed. To run a test to test the Authorization programming, you must be logged out.

Notification Tab

You can view and modify the e-mail notification parameters in the Notification tab. If you encounter an error, see “Scheduled Backups – Error Messages” on [page 17-65](#) for a list of possible programming error messages and troubleshooting tips.

To open the Notification tab, do one of the following:

- Double-click an entry on the Scheduled Backups Summary dialog box, and then click the **Notification** tab.
- Right-click an entry on the Scheduled Backups Summary dialog box, select **Edit**, and then click the **Notification** tab, as shown in the following example.



The Notification tab contains the following options:

- **Recipient(s):** Type one or more e-mail addresses that can receive notification e-mails for each Scheduled backups attempt. To type multiple e-mail addresses, separate them by semi-colons (;). If this box is blank, notification e-mail is not sent.
- **Sender:** The only entries that are required are the Server and Port Number. You can type more or all of the Sender information to be more descriptive about the sender.
 - *(Optional) Address:* Type the e-mail address of the sender (for example, John.Doe@mitel.com). It is set to ScheduledBackups@mitel.com by default.
 - *Server:* Type the server to be used for sending the notification e-mail.
 - *Port Number:* Change the e-mail port number, if needed. It is set to **25** by default.
 - *(Optional) Name:* Type the name of the sender (for example, John Doe). This is the name appears in the e-mail client. It is set to **Scheduled Backups** by default.
 - *(Optional) Username:* Type the user name of the sender (for example, JohnDoe).
 - *(Optional) Password:* Type the password for the Username, if any.

NOTE

When authentication is required by the server, the following authentication modes are supported: NTLM, CRAM-MD5, LOGIN, and PLAIN. In this order, each method supported by the server is tried with the given Username and Password, until authentication succeeds or there are no more methods to try. The first of these observed to be supported by the server is used. If the server supports no authentication modes, the Username and Password are not used. If the server requires authentication and it does not support any of these modes, the authentication fails and e-mails are not sent (this will be logged).

- **Notify only when Scheduled Backups fail to complete:** By default, the Notify only when Scheduled Backups fail to complete check box is selected, so that the e-mail Recipient(s) do not receive countless success messages. To receive success messages, select this box.
- **Notification Enabled:** When the Notification Enabled check box is selected, E-mail Notification is enabled, and when cleared, E-mail Notification is disabled. By default, this check box is not selected. As soon as a Recipient is entered in the Recipient(s) box, if the box was previously blank, this box is automatically selected.

When finished programming, click **Send Test Message** to verify that the Notification programming is valid. When this button is clicked, the system sends a test message to the programmed recipient(s).

You must then verify that the message is in fact received by the programmed recipient(s). If the message is not received in a timely manner, you must address this problem before Notification can function properly.

Scheduling Tab

You can view and modify the scheduling for backups in the Scheduling tab. If you encounter an error, see “Scheduled Backups – Error Messages” on [page 17-65](#) for a list of possible error messages and troubleshooting tips.

To open the Scheduling tab, do one of the following:

- Double-click an entry in the **Schedule** or **Next Run Time** or **Last Run Time** column on the Scheduled Backups Summary dialog box.
- Right-click an entry in the **Schedule** or **Next Run Time** or **Last Run Time** column, and then select **Edit**.
- Right-click an entry on the Scheduled Backups Summary dialog box, select **Edit**, and then click the **Scheduling** tab. The following dialog box appears.

The screenshot shows the 'Scheduled Backups for 3.0.4.37 US' dialog box with the 'Scheduling' tab selected. The 'Perform Backups' dropdown is set to 'Weekly' and the 'Start Time' is '12:00 AM'. Under the 'Backup Weekly' section, 'Every 1 week(s) on' is selected, and the 'Sunday' checkbox is checked. The 'Enable Scheduled Backups' checkbox at the bottom is unchecked. The 'OK' and 'Cancel' buttons are visible at the bottom right.

The Scheduling tab contains the following options:

- **Start Time:** Indicates the start time of the monthly, weekly, or daily scheduled backups. Type the time that you want to start backups. It is set to **12:00 AM** by default.

NOTE

Because multiple start times are not supported by the Windows XP Task Scheduler interface, you can only program a single start time.

- **Perform Backups:** Backups can be performed monthly, weekly, or daily. Different parameters appear in the area immediately below according to the setting. It is set to **Monthly** by default.
 - **Monthly Backups:** The Monthly Backups contains the following options:
 - *On Day (date) of the Month(s) or On the x Day of the Week of the Month(s):* If you select the day (date) of the month(s), type or select the date of the month. If you select the day of the week and week of the month(s), select the month (first, second, third, fourth, or last) and the day of the week (Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, or Sunday) that you want the backups to occur.
 - *Month(s):* Select the month or months in which you want the backups to occur. You must select at least one month.

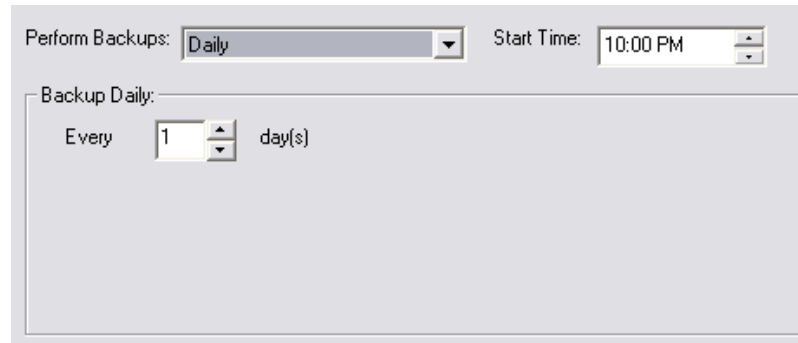
The screenshot shows the 'Perform Backups' dialog box. The 'Perform Backups' dropdown is set to 'Monthly'. The 'Start Time' is set to '12:00 AM'. Under the 'Backup Monthly:' section, the 'On the' radio button is selected, with 'first' in the day dropdown and 'Sunday' in the week dropdown. Below this, there is a grid of checkboxes for each month of the year, all of which are checked: January, February, March, April, May, June, July, August, September, October, November, and December.

The defaults set up when Monthly is selected for Schedule Backups are for the monthly backups to occur on the first Sunday of every month, at the Start Time.

- **Weekly Backups:** In the Every x week(s) on box, type or select the number of week(s), and then select the day(s) on which you want the backups to occur. You must select at least 1 week (up to 99 weeks). By default, it is set to **1**, and the selected day is set to **Sunday**. This means that the backups occurs once every week, on Sunday, at the Start Time. If Every x week(s) is changed to 2, and Wednesday and Saturday are selected instead of Sunday, backups occurs once every two weeks, on Wednesday and Saturday, at the Start Time.

The screenshot shows the 'Perform Backups' dialog box with 'Weekly' selected in the 'Perform Backups' dropdown. The 'Start Time' is set to '10:00 PM'. Under the 'Backup Weekly:' section, the 'Every' box is set to '1' and the 'week(s) on:' section has checkboxes for each day of the week. The 'Sunday' checkbox is checked, while Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday are unchecked.

- **Daily Backups:** In the Every x day(s) box, type or select the number of frequency in days (1 to 999) that you want the backups to occur. For example, setting this control to 7 would cause backups to occur once every week. It is set to 1 by default, indicating that the backups are scheduled to occur every single day.



Perform Backups: Daily Start Time: 10:00 PM

Backup Daily:

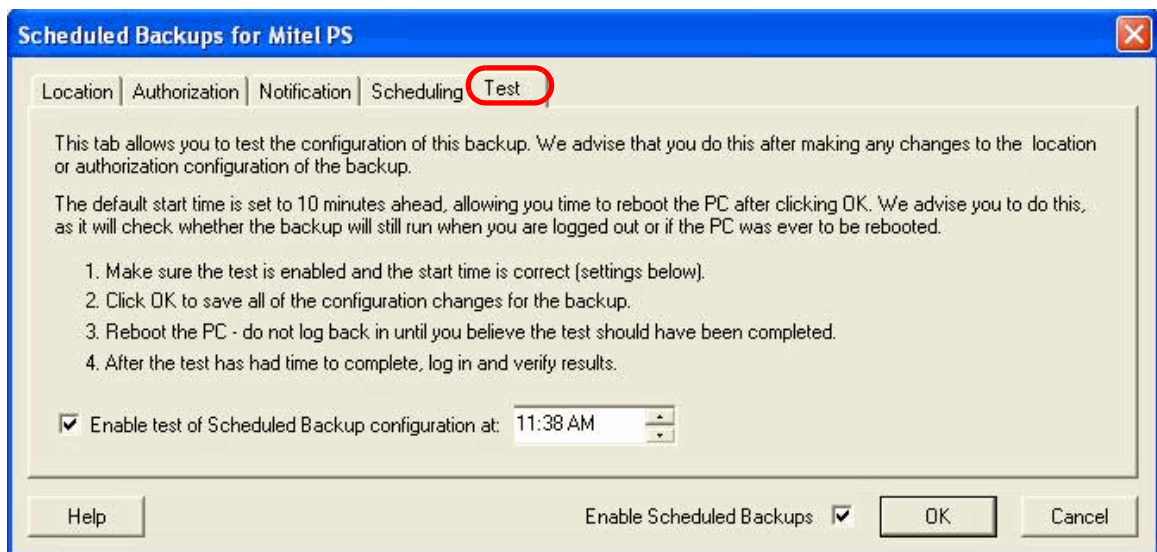
Every 1 day(s)

Test Tab

You can test the configuration of a backup in the Test tab. Perform this test after making any changes to the Location or Authorization configuration of the backup.

To open the Test tab, do one of the following:

- Double-click an entry on the Scheduled Backups Summary dialog box, and then click the **Test** tab.
- Right-click an entry on the Scheduled Backups Summary dialog box, select **Edit**, and then click the **Test** tab.



Scheduled Backups for Mitel PS

Location | Authorization | Notification | Scheduling | **Test**

This tab allows you to test the configuration of this backup. We advise that you do this after making any changes to the location or authorization configuration of the backup.

The default start time is set to 10 minutes ahead, allowing you time to reboot the PC after clicking OK. We advise you to do this, as it will check whether the backup will still run when you are logged out or if the PC was ever to be rebooted.

1. Make sure the test is enabled and the start time is correct (settings below).
2. Click OK to save all of the configuration changes for the backup.
3. Reboot the PC - do not log back in until you believe the test should have been completed.
4. After the test has had time to complete, log in and verify results.

☒ Enable test of Scheduled Backup configuration at: 11:38 AM

Help Enable Scheduled Backups ☒ OK Cancel

The Test tab contains the **Enable test of Scheduled Backup configuration at:** option. Type or select the time that you want to schedule a test run of the backups. By default, it is set to the current time plus 10 minutes. The 10 minutes gives you enough time to set up a one time test, close out all windows, log off, and then reboot the computer. Logging out and rebooting the computer is not required, but recommended to perform the most thorough test (see step 7 on [page 3-18](#)). This check box is automatically selected whenever you access this tab. (Prior to accessing this tab, the Scheduled Backup configuration test is not enabled.) Make sure the check box is selected to schedule to run the one-time test at the time shown. This one-time task is deleted after it runs.

When you schedule a test successfully, a message similar to the one below appears.



If there is a problem scheduling the test when you click **OK**, an error message appears. You must remedy the situation before you can schedule a test. See “Scheduled Backups – Error Messages” on [page 17-65](#) for a list of possible programming error messages and troubleshooting tips.

Viewing the Backup History

You can view the results of the scheduled backups for a session. This dialog box is read-only. The dialog box lists the most recent at the top of the list. Click the headers to re-sort the entries as desired.

To view the Backups History, do one of the following:

- Right-click on an entry, and then click **View History**.
- Double-click an entry in the **Last Result** column on the Scheduled Backups Summary dialog box.

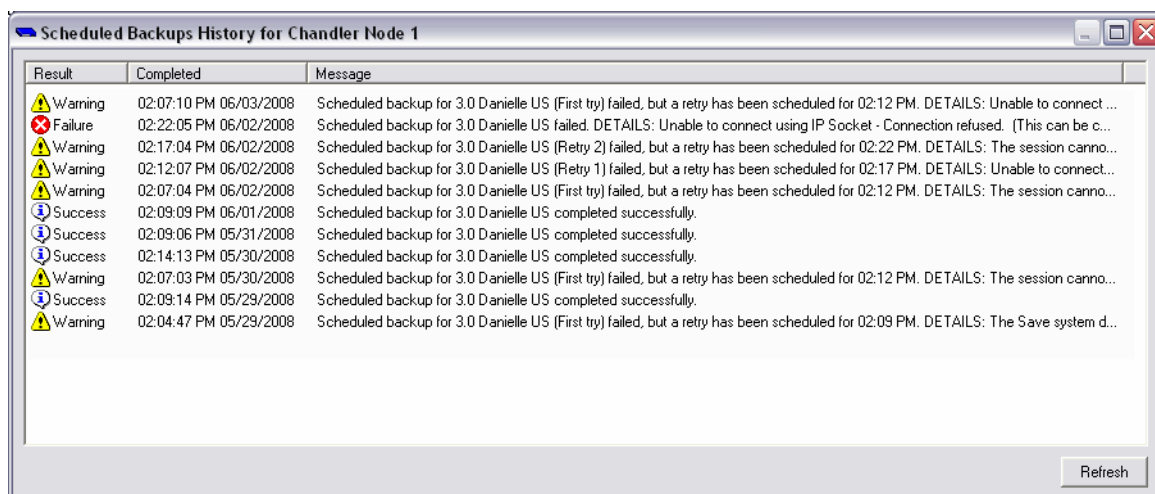
[Figure 3-7](#) shows a sample of each type of result. See [page 3-31](#) for a detailed list of failure reasons and warnings.

Refresh Button (F5): Re-reads all information from the registry and refreshes the display.

To view the whole message in a box, do one of the following:

- Double-click anywhere in the dialog box.
- Right-click on a message, and then select **View Message**.

Figure 3-7. *Scheduled Backups History*



Viewing Failure or Warning Reasons

You can view the full reason of a failure or warning status after a backup attempt has run and failed.

To view the full failure or warning reason:

- Double-click an entry in the **Reason** column on the Scheduled Backups Summary dialog box.
- Right-click an entry in the Scheduled Backups Summary dialog box, and then select **View Reason**.

Figure 3-8 shows a sample of the full reason of a failure status. See “Scheduled Backups – Warnings and Error/Failure Reasons” on [page 17-58](#) for a detailed list of failure reasons and warnings.

Figure 3-8. Reason Dialog Box



Setting Scheduled Backups for All Sessions

You can view and edit the settings that apply to all sessions in the Scheduled Backups Settings dialog box.

To set scheduled backups:

1. Select Session Manager – Settings – Scheduled Backups – **Settings**. The Scheduled Backups Settings dialog box appears.

Scheduled Backups Settings

Session options:

Maximum simultaneous Scheduled Backups: 3

Maximum backup databases saved per session: 3 (System databases only)

Retry options:

Time before retry: 45 (Minutes)

Retry attempts: 4

Time between retry attempts: 15 (Minutes)

Logging options:

Maximum file size: 250 (Kbytes)

Maximum number of files: 3

Help OK Cancel

2. Program the following options:
 - **Maximum simultaneous Scheduled Backups:** Shows the maximum number of backup sessions that is allowed to run simultaneously. Program this value depending on the bandwidth available/needed for backup sessions. If too many backups are allowed, the backups will take too long and may not complete successfully. Type or select the new value. The range is 1–3; the default is 3.
 - **Maximum backup database saved per session:** Shows the maximum number of system database files saved in each session's backup folder. The backup folder for the session is defined in the Save system database to folder option in the Location tab (see [page 3-19](#)). The Any file with the `intl` suffix stored in the backup folder is considered a backup file for the session.

When the maximum number of files exists in the folder and another backup runs, the oldest system database file is deleted. Note that this applies only to system database backup files, not to voice data backup files. Only one voice data backup file is maintained. Type or select the new value. The range is 1–99; the default is 3, indicating that the 3 most recent system database backup files in the folder are maintained.
 - **Time before retry:** Shows the maximum time allowed for completion of the Database Save. If it takes longer than this time for the Database Save operation to complete, the system assumes that the save attempt has failed and the session is terminated with timeout failure status. Type or select the new value. The range is 1–99 minutes; the default is 45 minutes. The lower limit allows ample time for the current task to complete its shutdown, before the retry is started.

- **Retry attempts:** Shows how many retries can be performed for a backup session when the backup session fails for any reason. Type or select the new value. The range is 0–99; the default **4**.
- **Time between retry attempts:** Shows how many minutes to wait before beginning a retry after failure. This duration is also used when a session must be postponed because the maximum number of simultaneous sessions is already running. Type or select the new value. The range is 5–99 minutes; the default is **15** minutes.

The following two options are for Service Logs (see [page 3-32](#) for details):

- **Maximum file size:** Shows the maximum file size allowed for Service Logs. Type or select the new maximum file size. The range is 10–999 KB; the default is **250** KB.
- **Maximum number of files:** Shows the maximum number of Service Log files maintained. Type or select the new value. The range is 1–9; the default is **3**.

3. Click **OK**.

Scheduled Backup Diagnostic Logs

You can monitor Scheduled Backup events in the following logs for diagnostic purposes:

- **Service Logs:** Events are logged during each Scheduled Backup attempt (see [page 3-32](#)).
- **Windows Event Logs:** Events are logged at the completion of each Scheduled Backup attempt.
 - “Viewing the Scheduled Backups Summary” on [page 3-16](#)
 - “Event Viewer” on [page 3-33](#)
- **E-Mail Notification:** If E-Mail Notification of Scheduled Backups is enabled, the same statement recorded in the Event Viewer is sent as an e-mail message to a programmed server/address (see [page 3-24](#)). An e-mail message is sent for each failed attempted backup (and successful attempts as well, if programmed).

Other logs produced by DB Programming are not being changed at this time, except for the fact that some new messages relating to the scheduled backups may appear in these logs.

To monitor Scheduled Backups:

1. If E-mail Notification is used, review the notifications received. If not, or in addition, access the computer to review the Windows Event Logs.
2. If a failure is indicated, access the computer to examine the Service Log.
3. Use the Service Log to troubleshoot the situation to determine the cause of the problem:
 - If the problem appears to be the way Scheduled Backups are set up, review the programming and settings, making adjustments as needed.
 - If the problem appears to be with hardware or connections, or if there is a problem with Database Save itself, go back to the manual Network Session and Database Save to diagnose the problem(s).
 - If the event logs do not address the concern, see “Scheduled Backups – Error Messages” on [page 17-65](#) for additional troubleshooting tips.
4. If E-mail Notification is not received when it should be, or messages do not appear in the Windows Event Log, see “Scheduled Backups – Error Messages” on [page 17-65](#) for additional troubleshooting tips.

Service Logs

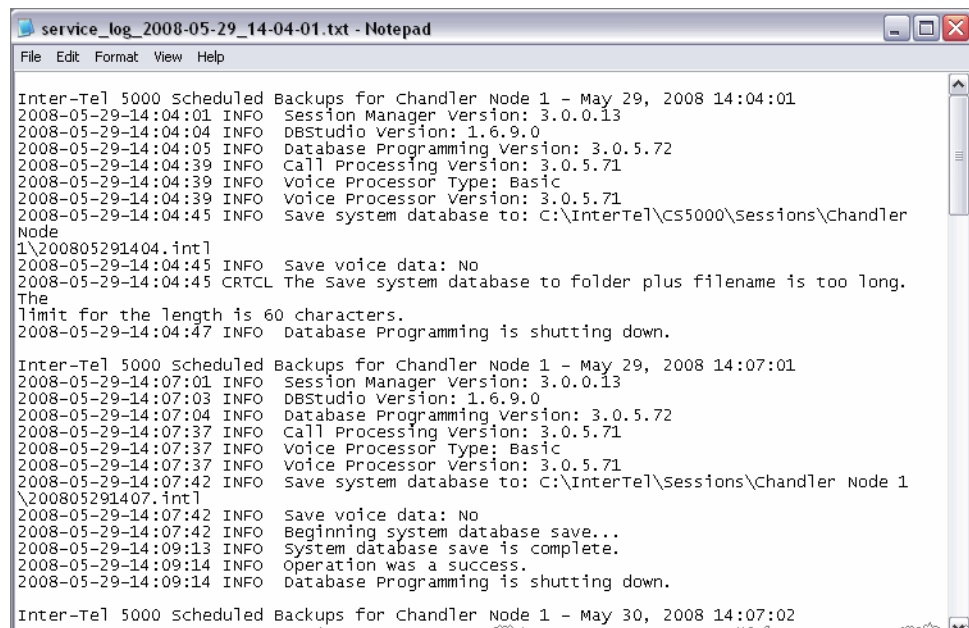
DB Programming logs all attempts to perform backups, as well as failure and success conditions, in a special Service Log. The Service Log provides a step by step indication of what occurred during the backup attempt. Each message box, question, error, warning, etc., is logged.

The following information describes how the Service Log is handled:

- One Service Log is maintained separately for each session.
- Scheduled Backup attempts for the session are logged sequentially in the Service Log file for that session.
- The Service Log files are named according to the following syntax:
`service_log_YYYY-MM-DD-HH-MM.txt`
- The Service Log files are stored under “sessions” in the install folder, in a subfolder named for the session. For example:
`C:\InterTel\CS5000\sessions\Chandler Node 1\database_log_YYYY-MM-DD-HH-MM.txt`
- Each entry in the log is date/time stamped.
- Each backup attempt includes a header to clearly delineate it from the other backup attempts.
- When the Service Log reaches the maximum file size programmed on the Scheduled Backups Settings dialog box (see [page 3-31](#)), the file is backed up. Entries are logged to the active Service Log file until it reaches the maximum file size. As soon as that is reached, a new empty Service Log file is created and further changes are logged in the newly active file. The maximum number of files is used to determine how many backups to maintain. If creating the new active log file would cause the maximum number of files to be exceeded, before it is created, the oldest Service Log file is deleted.

Figure 3-9 shows an example Service Log.

Figure 3-9. Sample Service Log

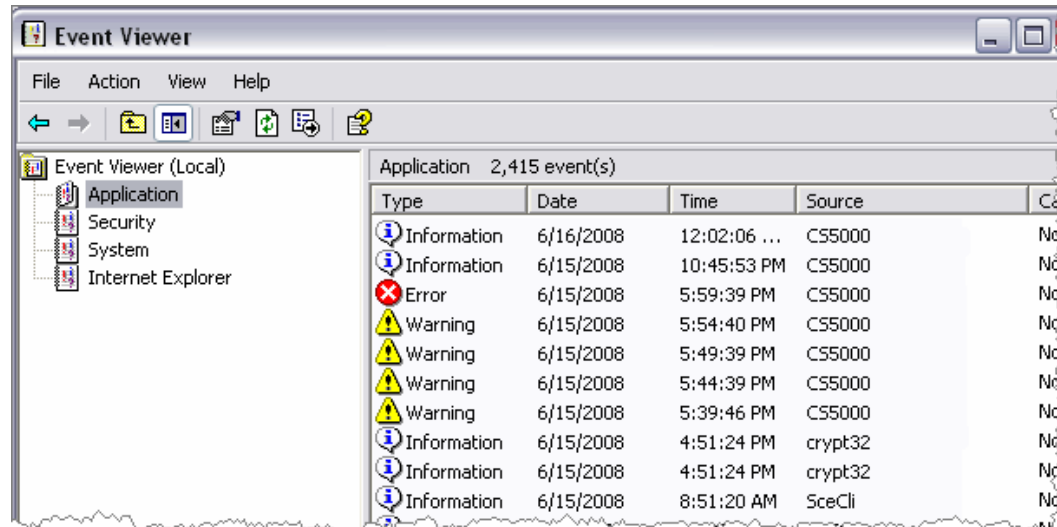


Event Viewer

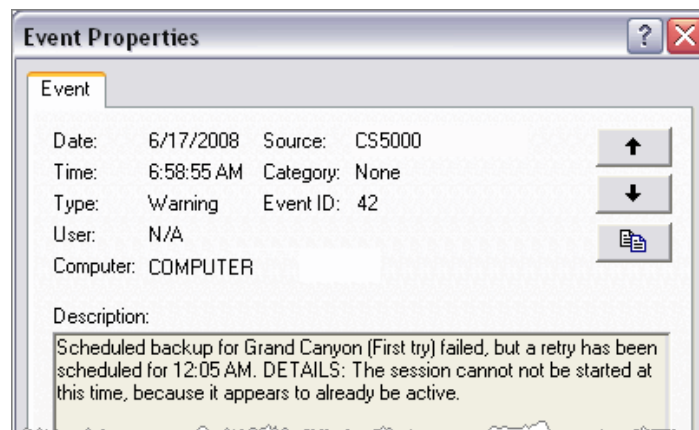
Backup attempts are logged in the Event Viewer. An entry is recorded under the Application folder in the Event Viewer for every backup attempt. This entry indicates whether or not the attempt was completely successful.

To view the Event Viewer:

Select Start – Control Panel – Performance and Maintenance – Administrative Tools – **Event Viewer**, as shown in the following example.



Double-clicking an event log opens the Event Properties dialog box as shown below. This box shows a brief description of the event. For example, if the backup did not complete successfully, it includes a brief description of the warning or error reason.



Default Database

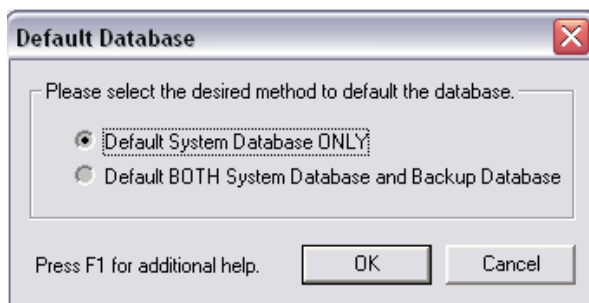
On a Windows-based EM voice processing unit, you can default the database to return the call processing and voice processor databases to default values. When you select **Default Database**, a window appears, as shown below, that warns that defaulting the database overwrites the current database and prompts you to continue.

NOTE

Defaulting the database ends the programming session and drops all calls. It also causes voice processing to stop. Voice processing restarts after the database default operation is complete. However, the EM unit does not reset.

From the DB Studio menu, select Operations – Database Operations – **Default Database**. The dialog box at right appears.

The default option is set to Default System Database ONLY. The second option defaults both the System database and the Backup database if one has been saved. Either option causes DB Programming to close, as expected.



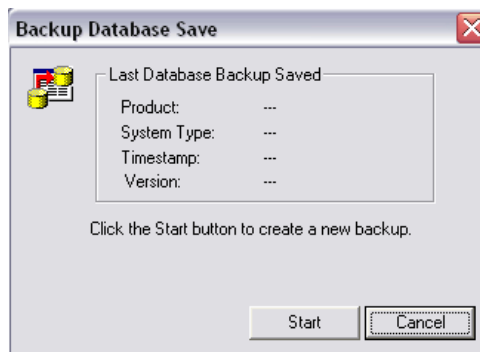
To default both System Database and Backup Database:

NOTE

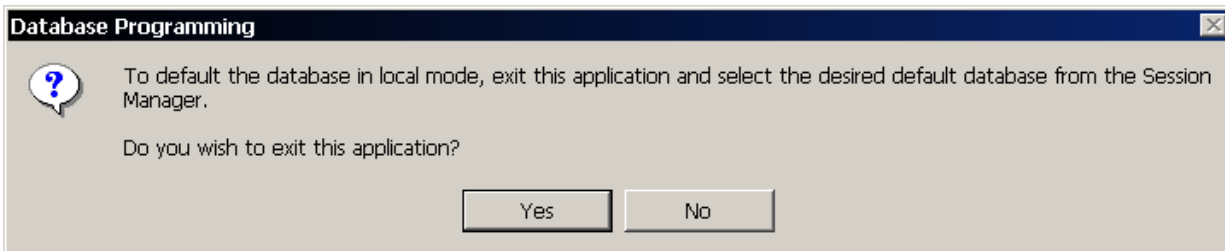
Mitel recommends that you do **not** delete the "Backup Database." The "Backup Database" is created as a safety net in rare situations where the system loses its primary database.

1. Select **Default BOTH System Database and Backup Database**.
2. Click **OK**. System Database and the Backup Database are defaulted, and the application shuts down.

To verify that the Backup Database has been defaulted, from the DB Studio menu bar, select Operations – Database Operations – **Backup Database Save**. The Backup Database Save dialog box appears, showing particulars about the last database backup saved.



If you are programming in Local Mode when you select **Default Database**, the following warning message appears.



You can also default the database using the LCD panel. Refer to the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000, for more information.

System Error Information

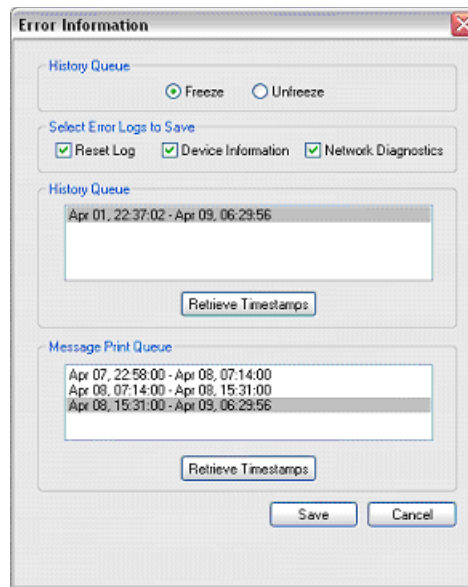
For system troubleshooting, you can freeze and unfreeze the system history queue and save error information.

NOTE

The history and Message Print queues are stored in RAM, not battery-backed RAM. If the system loses power, the queue information is lost. Retrieve history and Message Print information before powering down when troubleshooting the system. Queue files, however, are not affected by minor or major resets

To retrieve history and Message Print queue blocks:

1. Start Session Manager.
2. From the DB Programming menu bar, select Operations – **Error Information**. The following dialog box appears.



When you select Network Diagnostics option before you complete a system freeze, the freeze includes a Network Diagnostics Log file with an .ndl extension. This log file captures settings call processing, IP resource, and IP settings, as well as insufficient bandwidth alarms. This information can be obtained using Diagnostics Monitor. For more information, refer to the *Mitel 5000 Reference Manual*, part number 580.8007.

3. If the system is not already frozen, select **Freeze**. Otherwise, continue to the next step.
4. Click **Retrieve Timestamps** to view the timestamps associated with the history and Message Print queues. The blocks are listed based on the time intervals.
5. Select the timestamps that you want to save (you can use the SHIFT and CTRL key to select more than one item).
6. Click **Save**. The standard Windows browse screen appears.
7. Select the destination for the files (maximum 65 characters, including the freeze file names), and then click **OK**.

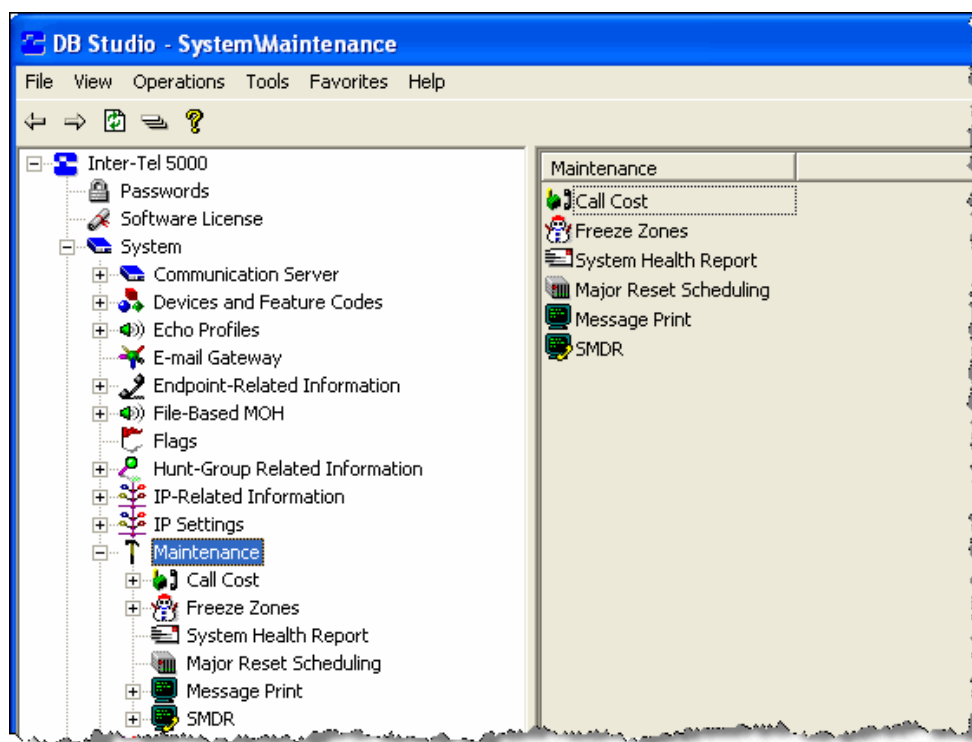
System Maintenance Options

System maintenance options include the following:

- “Call Costs” on [page 3-37](#)
- “Freeze Zones” on [page 3-39](#)
- “System Health Report” on [page 3-40](#)
- “Major Reset Scheduling” on [page 3-44](#)
- “Message Print” on [page 3-48](#)
- “Station Message Detail Recording” on [page 3-50](#)

System Maintenance options are under System – Maintenance, as shown in [Figure 3-10](#).

Figure 3-10. *System Maintenance*



Call Costs

You can use the Call Cost feature to estimate and display call costs while the calls are in progress. For more information about the Call Cost feature, refer to the “System Features” chapter in the *Mitel 5000 Reference Manual*, part number 580.8007. When using Call Cost, the following daytime rates and multiplication factors are displayed:

For U.S. Systems:

- Local calls
- Toll – local calls
- Toll – long distance calls
- Operator-assisted calls
- International calls
- Incoming calls
- Free calls
- Network calls

For European Systems:

- Local calls
- Toll (National) calls
- Operator calls
- International calls
- Incoming calls
- Free calls
- Network calls

Selecting a Call Cost Rate

To select a Call Cost a rate:

1. Select System – Maintenance – **Call Cost**. Call Cost options are shown in the right pane.
2. In the **Rate/Factor** column, select the current value, and then type the new value in the box.
3. Click out of the field or press **ENTER** to save the change.

Calculating Call Costs

You can use the following procedure to calculate call costs.

To calculate call costs:

1. Determine the daytime rates, in dollars [pounds in Europe] per minute, for the following types of calls (all default values are 0.00). Use several service provider bills from months with typical usage to calculate the average cost per minute of each type of call. Record the charges in dollars [pounds] and cents [pence] from 00.00–99.99. You may need to adjust the calculations later to more accurately estimate actual call costs. (This program is to be used as an estimate only.
2. Determine the multiplication factors that adjust the daytime (peak) per-minute call cost for evening (standard) and weekend (cheap) rates.

For U.S. systems: The multiplicative factor adjusts the daytime per-minute call cost for evening and weekend rates of outgoing calls. For example, the evening call cost multiplier is 0.65 if calls are 35% less expensive after 5:00PM. The evening (E) multiplicative factor and night/weekend (N/W) multiplicative factors are used on the following schedule:

	SUN	MON	TUE	WED	THU	FRI	SAT
8 AM TO 5 PM	N/W	No Multiplication Factors Apply					N/W
5 PM TO 11PM	E	E	E	E	E	E	N/W
11PM TO 8 AM	N/W	N/W	N/W	N/W	N/W	N/W	N/W

For European systems: The multiplicative factor adjusts the peak per-minute call cost for standard and cheap rates of outgoing calls. For example, the call cost multiplier is 0.65 if calls are 35% less expensive after 6:00PM. The standard (S) and cheap (C) multiplicative factors are used on the following schedule:

	SUN	MON	TUE	WED	THU	FRI	SAT
9 AM TO 1 PM	C	No Multiplication Factors Apply					C
1 PM TO 6 PM	C	S	S	S	S	S	C
6 PM TO 9 AM	C	C	C	C	C	C	C

Freeze Zones

You can freeze the system to “lock” the current state of the system fault history queue, which is a sequential list of all system commands and inputs. You can use this list, when decoded, to determine a series of events which may have resulted in an error. Unfreezing the system “unlocks” the current state of the history queue, and resumes event collection.

Using freeze zones, you can determine which nodes in the network are frozen during each freeze request. There can be up to 10 freeze zones in the database.

Programming Freeze Zones

To program a freeze zone:

1. Select System – Maintenance – **Freeze Zones**. Freeze Zone options are shown in the right pane.
2. *Optional.* In the **Description** column, type a name for the freeze zone in the box.

Adding Nodes to Freeze Zones

Double-click an individual zone to view nodes, if any, assigned to the freeze zone.

To add nodes to the freeze zone:

1. Select System – Maintenance – **Freeze Zones**. Freeze Zone options are shown in the right pane.
2. Use one of the following methods:

Method A

- a. In the **Value** column, select the current value, and then type the new value in the box.
- b. Press **ENTER**. A screen appears displaying what is associated with the number entered.
- c. Click **OK**. The new number appears in the field.

Method B

- a. Right-click anywhere in the right pane, and then select **Add To List**. A window appears prompting for the device type to include.
- b. Select the node types (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
- c. Select the appropriate nodes, then select **Add Items**.
- d. When you have added all the necessary nodes, click **Finish**. The selections appear in the list. To view programming options, double-click the extension number.

Deleting Nodes from Freeze Zones

To delete nodes from a freeze zone:

Select one or more nodes from the list, right-click, and then select **Remove Selected Items**.

System Health Report

This feature is reserved for controlled introduction.

The System Health Report is a report with Mitel 5000 system information and statistics that is e-mailed to the desired location daily. This feature is intended for support center personnel. The information in this report helps the recipient diagnose and troubleshoot problems with the Mitel 5000 system. This feature requires a software license (see “System Software Licenses” on [page 3-6](#)).

Information in the report includes a summary of the overall status of the Mitel 5000, system release information, system topology, call traffic, and alarms. Alarm messages are categorized by severity (Critical, Alert, Info, Debug). Refer to the *Message Print Diagnostics Manual*, part number 550.8018 for details about the alarms.

There is a new “System Health Report” folder in DB Programming (System – Maintenance). If the feature is not enabled in the license, the fields in DB Programming are disabled (appear with a red “x”). You can configure the time the report is sent and a recipient e-mail address (for example, the customer’s local provider or some type of centralized customer care center). The e-mail recipient receives the report in text format in addition to Extensible Markup Language (XML).

In a CS-5600 configuration, the text formatted report lists the PS-1 information followed by the Base Server information. Attached in the e-mail is a one .xml file for the PS-1 and another .xml file for the Base Server.

You can view the System Health Report Logs in the Administrative Web Session (AWS) session. For more information, refer to AWS Help. Daily logs are rotated and up to seven logs are stored on the Mitel 5000 compact flash-type memory card for up to seven days.

The report provides a system summary of the Mitel 5000 system consisting of the following information:

System Summary

- Alarm Status:
 - **Green:** The system is operational. Call Processing is running. There are no active alarms.
 - **Yellow:** The system is operational but one or more modules is offline. These are minor alarms (A000-A039).
 - **Red:** Call Processing reported a fault and it has not been cleared. These are critical alarms (A100-A244).
- System up time:
 - Days
 - Hours and minutes
 - Number of users
 - Load Average
- Release information:
 - Software release
 - Software version
 - License (system type 5200/5400/5600)
 - Build date
 - Listening port
- System modules with status

Call Activity (detail for the previous 24 hours):

- Number of active PSTN trunks
- Number of calls per hour

System Events:

- Memory usage, disk usage, file integrity check of main system files, and checksum check on low-level firmware files
- Alarm information
 - Call Processing Component
 - Trunk usage statistics (incoming and outgoing PSTN calls for each hour of the day)
 - Reset information
 - Voice channel errors
 - Software exceptions
 - Device timeouts/dumps
 - Digital Endpoint Interface Component
 - Firmware release in each DEI
 - Firmware release in each DEM
 - Number of calls per DEM (by hour of day)

CS-5600 Report Example

In a 5600 configuration, the text formatted report lists the PS-1 information (see [Figure 3-11](#)) followed by the Base Server information (see [Figure 3-12](#) on [page 3-42](#)).

Figure 3-11. PS-1 System Health Report Information

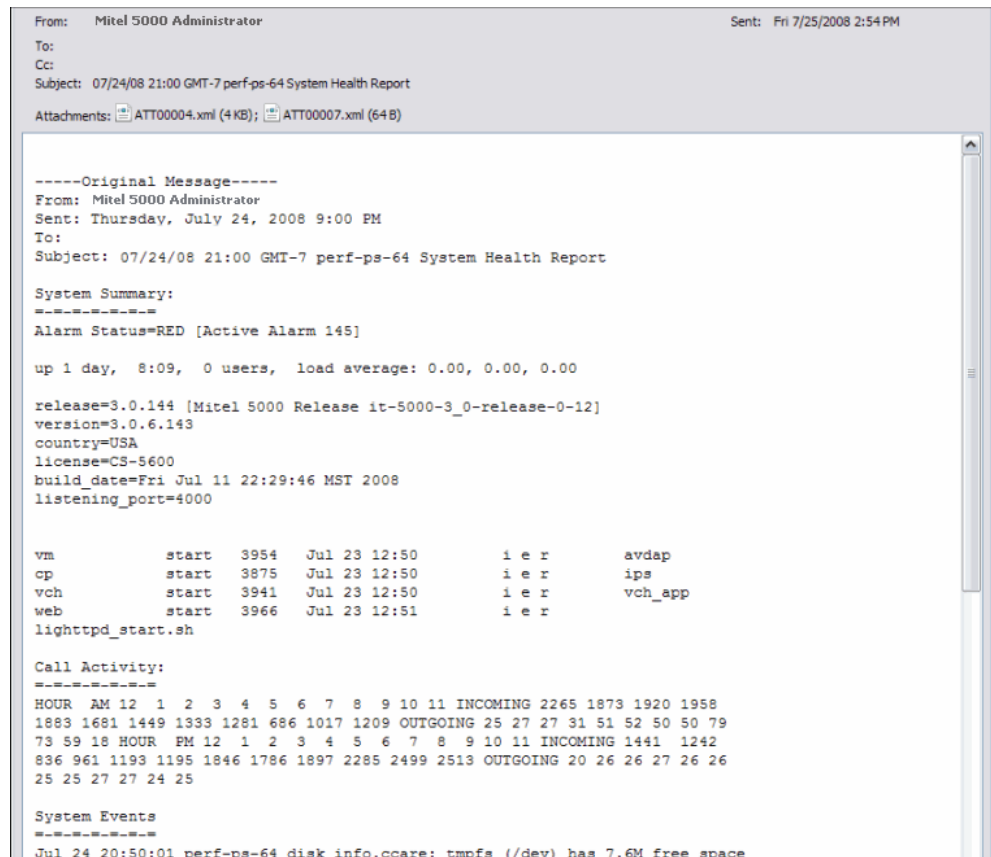


Figure 3-12. Base Server System Health Report Information

```
Base Server Log Information
=====
System Summary:
=====

up 1 day, 8:00, 0 users, load average: 0.02, 0.05, 0.05

release=3.0.144 [Inter-Tel 5000 Release it-5000-3_0-release-0-12]
version=3.0.6.143
country=USA
license=CS-5200
build_date=Fri Jul 11 22:14:03 MST 2008
listening_port=4000

t1_slot2      start   630    Jul 23 12:51      e r      t1_app
dt1_slot3      start   718    Jul 23 12:51      e r      dt1_app
del           start   557    Jul 23 12:50      i e r      del
ipra7         start   545    Jul 23 12:50      i e r      ipra_app
ipra9         start   471    Jul 23 12:50      i e r      ipra_app
vm            none
cp           start   462    Jul 23 12:50      i e r      ro
ls           start   483    Jul 23 12:50      i e r      ls_app
sl           start   484    Jul 23 12:50      i e r      sl_app
rch          start   429    Jul 23 12:50      i e r      rch_app
ppp          start   541    Jul 23 12:50      i e r      setsid
tftp         none
web          start  1005    Jul 23 12:51      i e r
lighttpd_start.sh

System Events
=====
Jul 24 20:40:02 perf-bs-64 disk_info.ccare: /dev/hda1 (/) has 235M free space - 48% used
(214M/473M) Jul 24 20:40:02 perf-bs-64 disk_info.ccare:
/dev/ram0 (/var/log/intl) has 3.1M free space - 14% used (526k/3.9M) Jul 24
20:40:02 perf-bs-64 disk_info.ccare: /dev/ram1 (/var/log/diag) has 3.6M free space - 1% used
(19k/3.9M) Jul 24 20:41:21 perf-bs-64 file_check.ccare:
[/usr/local/intl/etc/romd.conf] differs from backup Jul 24 20:41:22
perf-bs-64 mem_info.ccare: 98MB RAM - 69MB used - 28MB free - 2MB buffers - 42MB cached Jul 24
20:41:22 perf-bs-64 norflash_check.ccare: [armboot.bin] norflash checksum does not match Jul 24
20:41:23 perf-bs-64
norflash_check.ccare: [fpga.bin] roclock checksum does not match Jul 24
20:41:23 perf-bs-64 norflash_check.ccare: [hdvoice.axf] norflash checksum does not match Jul 24
20:41:23 perf-bs-64 norflash_check.ccare: [zImage] norflash checksum does not match
```

Programming

In DB Programming, you must enable the report for delivery and configure the e-mail gateway settings.

To support System Health Report, you must first program the SMTP server in the E-mail Gateway folder. If you attempt to enable the Enable E-mail Delivery option in the System Health Report folder without setting the SMTP server, an error message appears.

To set the SMTP server:

1. Select System – **E-mail Gateway**.
2. Set the E-mail System to **SMTP**.
3. Program the following fields:
 - E-mail SMTP Server
 - E-mail Address
 - E-mail Username
 - Gateway Password
 - E-mail Real Name

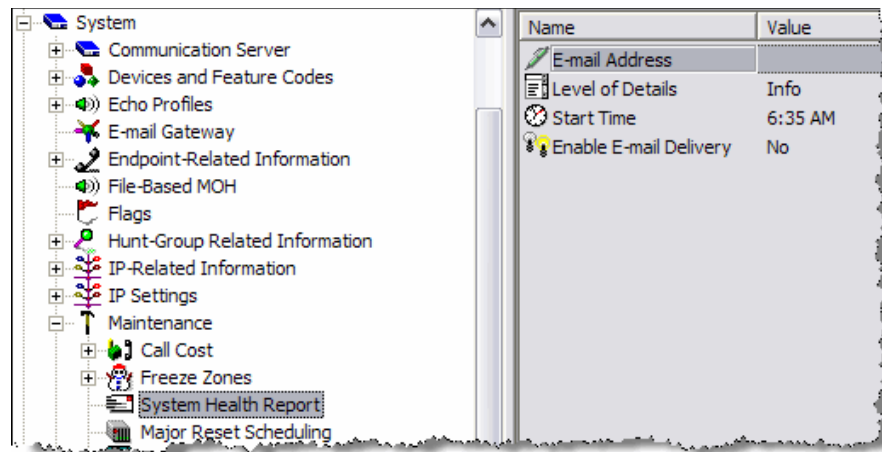
For details about these fields, refer to the DB Studio Help.

To enable the System Health Report delivery:

1. Select System – Maintenance – **System Health Report**.
2. Configure the following fields:
 - **E-mail Address:** Type an e-mail address of the recipient to which the report is sent.
 - **Level of Details:** This value indicates the level of detail that is included in the report. Click the **Value** column, and then select the alarm information level (Critical, Alert, Info, Debug) to include in the report. The default is **Info**.
 - **Start Time:** The time the report starts to generate, and then is sent. Click the **Value** column, and then select the time for the report e-mail delivery to begin. The default is 6:35 A.M.
 - **Enable Email Delivery:** Set this option to **Yes**. The report is e-mailed to the recipient on a daily basis according to the start time. The default is set to **No**.

NOTE

To enable the Enable E-mail Delivery option, you must first program the E-mail Address field in this folder. If you attempt to enable this option without an e-mail address programmed, an error message appears.



To configure the E-Mail Gateway options:

Select System – **E-Mail Gateway**, and then follow the instructions in the DB Programming Help to configure the options. The e-mail gateway settings are shared with other system features including BVM Forward-to-E-mail and BVM VPIM. For more information, see [page 11-62](#).

System Resets

This section describes system resets and how to reset the system on demand or to schedule a reset.

NOTICE

Possible Service Interruption. A system reset terminates all calls in progress. Schedule resets to occur after normal business hours.

Immediate System Resets

You manually reset the system. You can also use the LCD panel on the Base Server to immediately reset the system. For more information, refer to the Installation chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

To perform an immediate system reset:

1. From the DB Programming menu bar, select Operations – **Reset System**.
2. Click **OK** to reset the system and end the programming session.

Call Processing Resets

To reset Call Processing:

1. From the DB Programming menu bar, select Operations – **Reset Call Processing Application**.
2. Click **OK** to reset call processing and end the programming session.

Major Reset Scheduling

A system reset is required to ensure proper system operation after you make any of the following changes:

- Equipping or unequipping modules or devices
- Changing extension lists
- Changing trunk group lists

The following operations do not require a major reset:

- Changing ACD agent IDs.
- Changing extension numbers (this includes any extension number, not just UCD/ACD, such as endpoint, trunk group, and so on.)

A major system reset terminates all calls and ends the programming session. However, a delayed system reset checks system activity at the scheduled time and waits for the system to become idle and any active programming session to end before allowing the reset to occur.

A Call Processing reset affects call processing and all related applications. To avoid Call Processing issues, you can schedule a delayed reset, as described in the following sections.

NOTE

If Daylight Saving Time is enabled, Mitel recommends that you do not schedule resets to occur at 2:00 AM. If you do, the system may not perform the reset when the time changes.

Make sure the Scheduled Reset Time value (it defaults to 12:01AM) is AFTER the Periodic Backup Database Save Time (it defaults to 11:00PM); otherwise any Database changes since the previous backup database save will be lost.

System Requires Reset

(Read Only) Indicates if Call Processing requires a reset. If the field shows *Yes*, the system resets at the time indicated in the System Delayed Major Reset field. If the field shows *No*, a delayed major reset does not occur, even if one is scheduled.

Scheduled Reset Time

If the System Requires Reset option is turned on, this field determines the default time for *scheduled* system resets. Scheduled major resets can be scheduled when system administrators program the database or when Reset Now is selected from the Operations menu.

To program the default time for delayed system resets:

1. Select System – Maintenance – Major Reset Scheduling – **Scheduled Reset Time**.
2. In the **Value** column, select the time for the scheduled reset (AM/PM). The default value is 12:01 AM.
3. Click out of the field or press **ENTER** to save the change.

Force Reset If Not Idle

Normally, the system does not perform a major reset if there are any active calls. However, if this option is turned on, the system forces a major reset at the specified time, as programmed in the previous section. A major reset causes all active calls on the system to be dropped. The option should be used only on systems which are busy 24 hours each day and, therefore, do not have a consistent time when all resources are idle and a normal delayed major reset can be performed. This option affects any request to perform a major reset, whether it be by the system itself for resource reconciliation, or requested through DB Programming.

NOTE

When enabled, this option drops all active calls at the specified time, should a major reset be necessary. This does not happen every day, but it does happen occasionally. Be aware of this so you do not mistake the reset for a system failure.

To enable the Force Reset If Not Idle option:

1. Select System – Maintenance – Major Reset Scheduling – **Force Reset If Not Idle**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Press **ENTER** or select another field to save the change.

Days of the Week

Select the days of the week on which you want automatic resets to occur. Resets occur on the days of the week that are selected, provided the **Always Reset On Days Of Week** option is turned on. By default, all days of the week are turned off.

To select days:

1. Select System – Maintenance – Major Reset Scheduling – **<day>**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To deselect the day, clear the check box.
3. Press **ENTER** or select another field to save the change.

Always Reset On Days Of Week

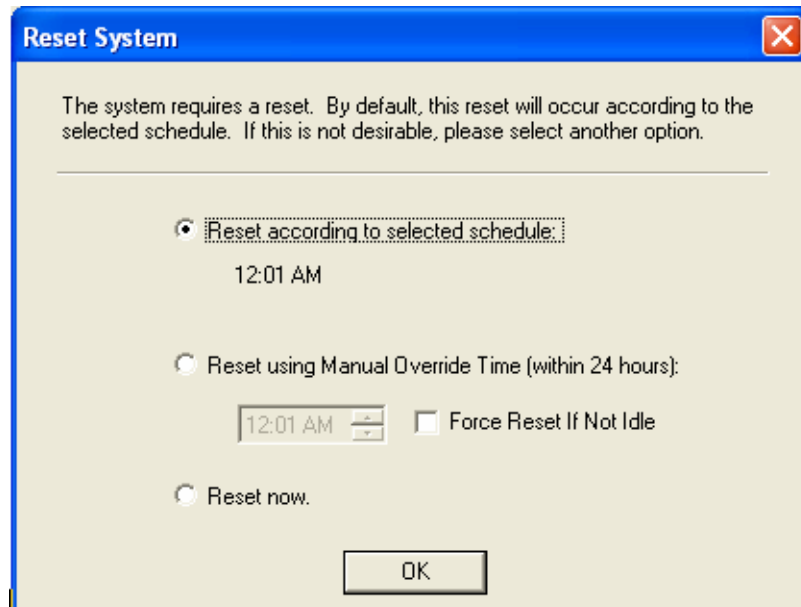
Set this option to Yes to have resets occur on the specified days of the week. If this option is disabled, resets do not occur on the specified days. By default, this option is set to No. If a red "X" appears next to **Always Reset On Days Of Week**, you have not selected any of the days of the week. You must have at least one day of the week selected; otherwise, resets do not occur. When finished, the system resets as programmed.

To enable Always Reset on Days of Week:

1. Select System – Maintenance – Major Reset Scheduling.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Press **ENTER** or select another field to save the change.

Reset System Dialog Box

When you make a change that requires a reset, the Reset System dialog box appears when you exit DB Programming.



1. Select one of the following options:

- **Reset according to selected schedule:** Resets the system according to the schedule that the user selected in the Major Reset Scheduling folder (System\Maintenance). The reset schedule that is currently selected appears here.
- **Reset using Manual Override Time (within 24 hours):**

NOTE

The Reset using Manual Override Time (within 24 hours) value must be at least 15 minutes before the programmed Periodic Backup Database Save Time value (under System); otherwise, the backup may not occur. If you select a value that is less than 15 minutes before the Periodic Backup Database Save Time, an error message is displayed, requesting a new value

You can use the scroll box to change the scheduled reset time to a different time (within 24 hours). For example, if the system is programmed to reset on Wednesdays at 11:30 PM, and you schedule a manual override time for 10:00 PM on a Wednesday, the system resets at 10:00 PM and then again at 11:30 PM. By default, this is 12:01 AM. Note that the Manual Override Time is only used when the system requires a reset. This option can also be accessed from the Major Reset Scheduling folder in OLM mode.

- **Force Reset If Not Idle:** Turn on this option to force a reset, even if there are active calls. If turned off, the reset is not performed until the system is idle. By default, this is set to No. This option can also be accessed from the Major Reset Scheduling folder. (This field was previously called Forced Delayed Major Reset.)
- **Reset now:** Performs an immediate system reset. Do not select this option if the system is currently backing up the database; otherwise, the backup is aborted.

2. Click **OK** when finished.

Message Print

System messages can be printed to give service personnel and Mitel engineers information about system status during troubleshooting. You may enable any combination of the error message types. The available message types are:

- **Alarm Messages:** Indicate that a minor alarm has occurred, but that general system operation was not affected.
- **Information Messages:** Provide information concerning system operation.
- **Severe Messages:** Indicate that a severe error has occurred in the system.
- **Warning Messages:** Indicate that a condition exists which may affect system performance.
- **Network Dump:** Provides information concerning network operation.

The fields you must program to set up Message Print include the following:

- “Output Port And Local Backup Port” on [page 3-48](#)
- “Message Print Output Active” on [page 3-49](#)
- “Output Device Line Width” on [page 3-49](#)
- “Print Options” on [page 3-49](#)

For more information about Message Print, refer to the *Message Print Diagnostics Manual*, part no. 550.8018.

Output Port And Local Backup Port

Each node has its own Message Print programming, Message Print output port, and Message Print output port backup. There should be a Message Print terminal at each node to monitor node and network performance and aid in troubleshooting.

- If a node Message Print output port is a node, the network sends Message Print records to the specified node.
- You cannot select a node as the backup Message Print output port.
- If Message Print output programming forms a loop, the system sends the output to the node backup Message Print port. For example, if the Message Print port on Node 1 routes to Node 2 and the Message Print port on Node 2 routes to Node 1, the configuration causes an infinite loop. Message Print reports for Node 1 would be printed to the backup serial port on Node 2 and vice versa.

To select ports for the Message Print reports, use one of the following methods:

NOTE

Because a serial interface is not available on the Mitel 5000, the output to Message Print is sent over IP to a remote node.

Method A

1. Select System – Maintenance – Message Print – **Output Port** or **Local Backup Port**.
2. In the **Value** column, select the current value, and then type the new value in box. The port number must be a port on a remote node.
3. Click out of the field or press **ENTER**. A screen appears showing what is associated with the number entered.
4. Click **OK**. The new number appears in the field.

Method B

1. Select System – Maintenance – Message Print – **Output Port** or **Local Backup Port**.
2. Right-click the existing port. An option box appears.
3. Select **Change Port**. A window appears prompting for the device type to include.
4. Select **None** or **Remote Node**, and then click **Next**. The list of ports or nodes appears. To view items in a list only, click **List**.
5. Select the desired port, and then click **Finish**. The selection appears in the appropriate port field.

Message Print Output Active

When enabled, activates the error/message reporting feature. This option is enabled by default.

To disable the option:

1. Select System – Maintenance – Message Print – **Message Print Output Active**.
2. In the **Value** column, clear the check box. The field changes to **No**. To enable the option, select the check box.
3. Click out of the field or press **ENTER** to save the change.

Output Device Line Width

Indicates whether the output device has 64, 80, or 132 character columns.

To set the output device line width:

1. Select System – Maintenance – Message Print – **Output Device Line Width**.
2. Select the current value, and then scroll to the desired column width.
3. Click out of the field or press **ENTER** to save the change.

Print Options

Determine the types of error messages to be included in the error report. By default, the following options are included in the error report (set to Yes):

- **Print Alarm Messages:** Indicate that a minor alarm has occurred, but that general system operation was not affected.
- **Print Information Messages:** Provide information concerning system operation.
- **Print Severe Messages:** Indicate that a severe error has occurred in the system.
- **Print Warning Messages:** Indicate that a condition exists which may affect system performance.
- **Print Network Dump:** Provide information concerning network operation.

To disable a print option:

1. Select System – Maintenance – Message Print – *<print option>*.
2. In the **Value** column, clear the check box. The field changes to **No**. To enable the option, select the check box.
3. Click out of the field or press **ENTER** to save the change.

Station Message Detail Recording

Station Message Detail Recording (SMDR) produces a record of calls and their costs. For information about the record format, refer to the “System Features” chapter in the *Mitel 5000 Reference Manual*, part number 580.8007. SMDR buffering is *not* supported in BVM. An external voice processing system or other system designed to buffer SMDR is required.

Each node in a network has its own SMDR programming. You can enable or disable network call records on each node.

Devices

To assign the endpoints and trunks to be included in the SMDR output, double-click **Devices**. A list of current devices, if any, appears. You can add or delete devices as follows:

To add devices:

1. Select System – Maintenance – SMDR – **Devices**.
2. Right-click anywhere in the right pane, and then select **Add To Devices List**. A window appears prompting for the device type to include.
3. Select the device types (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. A list of devices appears. To view details, click **Details**.
4. Select the appropriate items, and then select **Add Items**. When you have added all the desired devices, click **Finish**. The selections appear in the list. To view programming options, double-click the extension number.

To delete devices:

Select the item(s) in the list, right-click, and then select **Remove Selected Items**.

Output Port and Local Backup Port

Each node has its own SMDR programming, SMDR output port, and a local (backup) SMDR output port. You can turn on/off network call records on each node. By default, the system suppresses network call records. However, when they are turned on, the following applies:

NOTE

Because a serial interface is not available on the Mitel 5000, the output to Message Print is sent over IP to a remote node.

- If the node SMDR output port is a node, the network sends SMDR records to the specified node.
- If SMDR output programming forms a loop, the system sends the SMDR output to the node local SMDR port. For example, if the SMDR port on Node 1 routes to Node 2 and the SMDR port on Node 2 routes to Node 1, the configuration causes an infinite loop of SMDR routing. SMDR reports for Node 1 would be printed to the local SMDR-associated IP address on Node 2 and vice versa.

To select the output port and local port for the Message Print reports:

1. Select System – Maintenance – SMDR – **Output Port or Local Backup Port**.
2. Right-click the existing port. An option box appears.
3. Select **Change Port**. A window appears prompting for the device type to include.
4. Select **None** or **Remote Node**, and then click **Next**. The list of ports or nodes with details appears. To view options in a list only, click **List**.
5. Select the port that you want to use, and then click **Finish**. The selection appears in the port field.

SMDR Output Active

The SMDR Output Active option activates the SMDR reporting feature. It is enabled by default.

To disable the SMDR Output Active option:

1. Select System – Maintenance – SMDR – **SMDR Output Active**.
2. In the **Value** column, clear the check box. The field changes to **No**. To enable the option, select the check box.
3. Click out of the field or press **ENTER** to save the change.

Output to System Manager

If the Output to System manager option is turned off, SMDR information is not available to System Manager users. If turned on, System Manager users can run call reports for this node.

To turn the option on:

1. Select System – Maintenance – SMDR – **Output to System Manager**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Click out of the field or press **ENTER** to save the change.

NOTE

Because a serial interface is not available on the Mitel 5000 system, the output to Message Print is sent over IP to a remote node.

Display Elapsed Time in Seconds

To allow SMDR to give a more accurate representation of elapsed time, the Display Elapsed Time in Seconds option can be turned on to record the elapsed time of calls in seconds instead of minutes. For calls up to 999,999 seconds in length, the ELAPSED TIME field shows "S=XXXXXX" (XXXXXX represents the number of seconds). For calls lasting longer than 999,999 seconds, ELAPSED TIME shows HH:MM. Hours and minutes rounded up to the nearest minute.

To have call durations of fewer than 999,999 seconds displayed in seconds:

1. Select System – Maintenance – SMDR – **Display Elapsed Time in Seconds**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Click out of the field or press **ENTER** to save the change.

Display "O/I" for Operator and International Calls

If turned on, operator and international calls are displayed in SMDR as one entry under the call-type abbreviation "O/I." If turned off, operator and international calls are displayed separately in SMDR: operator calls under "OP," and international calls under "INT." By default, this is turned on.

To turn off the Display "O/I" for Operator and International Calls option:

1. Select System – Maintenance – SMDR – **Display "O/I" for Operator and International Calls**.
2. In the **Value** column, select the check box. The field changes to **No**. To enable the option, clear the check box.
3. Click out of the field or press **ENTER** to save the change.

Display Redirected Station

An endpoint that transfers or manually forwards a call to the public network can be recorded in the SMDR report. To display redirected information for trunk-to-trunk calls, add the trunks and endpoints to the SMDR list. If the trunks and endpoints are not listed, the endpoints that transfer or manually forward CO calls are not recorded in the SMDR report for redirected calls. This option is disabled by default.

To enable the Display Redirected Station option:

1. Select System – Maintenance – SMDR – **Display Redirected Station**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Click out of the field or press **ENTER** to save the change.

Display “T” for Two B-Channel Transferred Calls

When enabled, SMDR displays a “T” in the output when a Two B-Channel Transfer (TBCT) occurs. This option is disabled by default. For more information about TBCT, see “ISDN PRI Two B-Channel Transfer” on [page 6-34](#).

To enable the TBCT option:

1. Select System – Maintenance – SMDR – **Display “T” for Two B-Channel Transferred Calls**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Click out of the field or press **ENTER** to save the change.

Record Calls

The Record Calls options determine the content of the SMDR output. Options include the following:

- **Record All Incoming Calls:** Includes all incoming calls in the SMDR report.
- **Record All Local Calls:** Records all local, non-toll, valid calls.
- **Record All Free Calls:** Records all calls that use the “free” call cost.
- **Record All Ring-in Diagnostics:** A ring-in message is recorded for every incoming call (whether answered or unanswered) to indicate how long it rang. All incoming calls are recorded, even those involving endpoints not listed in the endpoint list.
- **Record All Toll Local Calls:** (*U.S. only*). Records all valid local toll calls.
- **Record All Toll Long Distance Calls:** (*U.S. only*). Records all valid long distance toll calls.
- **Record All Toll (National) Calls:** (*Europe only*). Records all valid long distance toll calls.
- **Record All Operator Calls:** Records all operator-assisted calls.
- **Record All International Calls:** Records all international calls.
- **Record All DISA Calls:** Includes all DISA calls in the SMDR report.
- **Record All Conference Calls:** Includes all conference calls in the SMDR report.
- **Record All DID/DNIS Calls:** (*U.S. only*). Records all calls received through DID and DNIS.
- **Record All Trunk To Trunk Calls:** Records all calls made from one outside caller to another.

- **Record All Network Calls:** The system generates SMDR records (labeled "NET") for node-to-node Private Networking calls on the nodes where each trunk used resides. For example, if a caller on Node A places a call using a trunk group on Node B, the SMDR report for Node A shows a NET call to Node B and the SMDR reports on Node B shows a NET call from Node A. This option has no effect on the Record Off-Node Devices option described above.
- **Record All Off-Node Devices:** You can determine whether calls placed by off-node devices, through this node, are included in the reports. This option has no effect on the Record All Network Calls option described above.

To enable Record Calls options:

1. Select System – Maintenance – SMDR – **<record option>**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Click out of the field or press **ENTER** to save the change.

Suppress Digits Options

The Suppress Digits options determine which digits, if any, are suppressed when the dialed digits are reported. To choose an option, select its current Value and place a check mark in the box. To remove an option, select remove the check mark. Options include the following:

- **Suppress Absorbed Digits:** Absorbed digits on local or PBX lines do not appear in the report if this option is selected. If absorbed digits are repeatable on a local line, the absorbed digits do not appear in the SMDR report even when repeated.
- **Suppress Equal Access Digit:** (U.S. only). Equal access digits do not appear in the report if this option is selected.
- **Suppress Outside Party Number:** Caller information that is received through ANI or Caller ID [CLID] does not appear if this option is selected.
- **Suppress Toll Digits:** When this option is selected, toll digits do not appear in the report.
- **Suppress Trunk Number:** Information received through DID or DNIS [DDI] is not included in the report if this option is selected.

To enable Supress options:

1. Select System – Maintenance – SMDR – **<suppress option>**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Click out of the field or press **ENTER** to save the change.

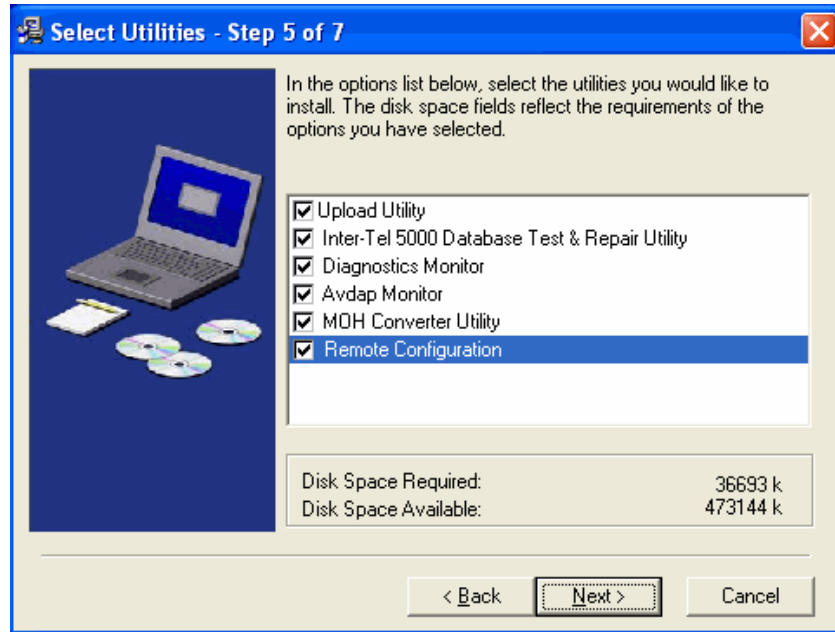
Remote Configuration

This feature is reserved for controlled introduction. After the remote user and Mitel 5000 system are configured in the Remote Proxy Server, remote users must use Session Manager to connect to the system.

Enabling Remote Configuration in DB Programming

You must enable the Remote Configuration check box (see [Figure 3-13](#)) in the DB Programming Configuration Wizard before you can use the feature.

Figure 3-13. Remote Configuration Wizard Check Box



DB Programming Remote Configuration Options

You can configure the following DB Programming options:

- **Remote Proxy Server Hostname/IP Address:** The IP address or hostname of the Configuration Management Server, not the fully qualified domain name (FQDN).
- **Remote Proxy Server IP Port:** The outbound port used to connect to the Configuration Management Server. The default port is 1194, but you can change it as necessary.
- **Idle Timeout:** The duration, in minutes, before the Mitel 5000 disconnects from the Remote Proxy Server. The default idle timeout period is 60 minutes, and the maximum timeout period is 10080 minutes. If the system reboots within the idle timeout period, the system automatically reconnects to the Remote Proxy Server.

To configure Remote Proxy Server DB Programming settings:

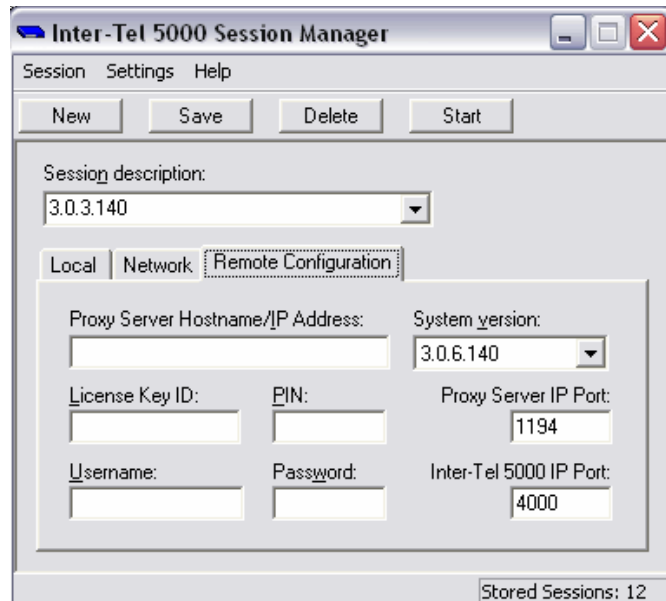
1. Select System – IP Settings – Remote Configuration Settings – <Remote Configuration option>.
2. In the **Value** column, type the new setting. If you are changing the Remote Proxy Server IP Hostname/IP Address field, click in the **Value** column, and then type the new IP address in the Edit Remote Proxy Hostname/IP Address dialog box.
3. Press **ENTER** or click out of the options to save the settings.

Enabling an On-Demand Remote Connection

To enable an on-demand remote connection, you must establish the connection in both Session Manager and a system endpoint (see [page 3-56](#)).

To enable an on-demand remote connection in Session Manager:

1. From the Mitel 5000 Session Manager dialog box, select the **Remote Configuration** tab. The following dialog box appears.

The screenshot shows the 'Inter-Tel 5000 Session Manager' window. It has a menu bar with 'Session', 'Settings', and 'Help'. Below the menu bar are four buttons: 'New', 'Save', 'Delete', and 'Start'. The main area is divided into three tabs: 'Local', 'Network', and 'Remote Configuration', with 'Remote Configuration' being the active tab. Under the 'Remote Configuration' tab, there are several input fields: 'Session description:' with a dropdown menu showing '3.0.3.140'; 'Proxy Server Hostname/IP Address:' with a text box; 'System version:' with a dropdown menu showing '3.0.6.140'; 'License Key ID:' with a text box; 'PIN:' with a text box; 'Proxy Server IP Port:' with a text box showing '1194'; 'Username:' with a text box; 'Password:' with a text box; and 'Inter-Tel 5000 IP Port:' with a text box showing '4000'. At the bottom right, it says 'Stored Sessions: 12'.

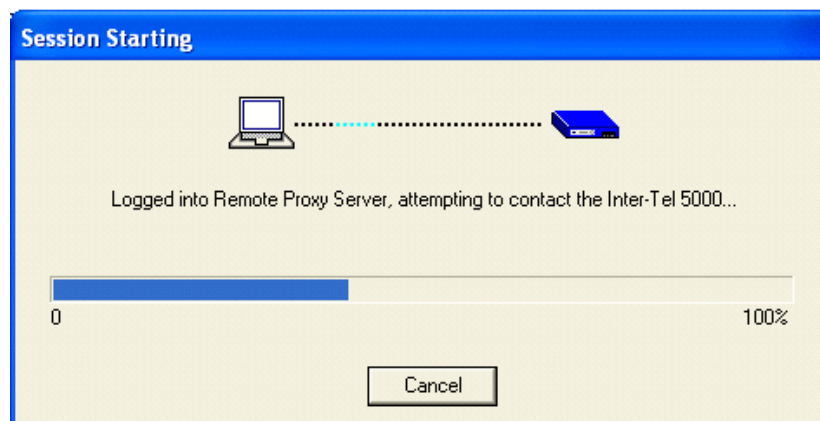
2. From the **Session description** list, select the session you are registering (if applicable).
3. In the **Proxy Server Hostname/IP Address** box, type the hostname or the IP address of the Remote Proxy Server. Because the IP address can change, Mitel recommends that you use the hostname. For example, if the server is moved to a new location, the IP address may change, but it will still be assigned to the original hostname.
4. From the **System version** list, select the system version (if applicable).
5. In the **License Key ID** box, type the Mitel 5000 version license key ID, which identifies the system. To find the license ID key, dial feature code **347** on any endpoint on the 5000 system in which you are connecting. See "Enabling an On-Demand Remote Connection from an Endpoint" on [page 3-56](#).
6. In the **PIN** box, type the PIN number, which identifies the session to be enabled. The PIN is determined by the person enabling the feature on a system endpoint (using feature code **342**). For more information, see "Enabling an On-Demand Remote Connection from an Endpoint" on [page 3-56](#).
7. In the **Proxy Server IP Port** box, type the port number used for outbound remote configuration connections. The default port number is **1194**.

To display the port settings:

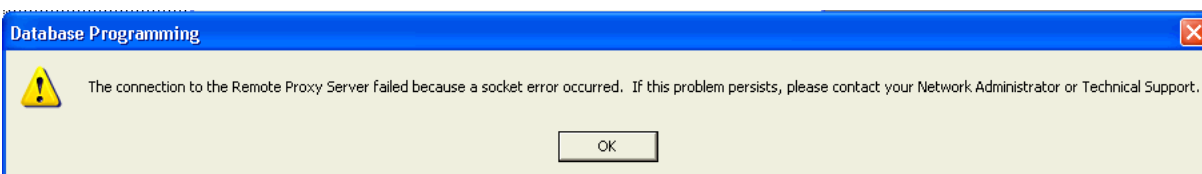
In the Session Manager Settings menu, select Network Connections – **View IP Port**. See "Settings Menu" on [page 2-6](#) for port descriptions.

8. In the **Username** box, type the user name supplied by Customer Care personnel.
9. In the **Password** box, type the password supplied by Customer Care personnel.
10. Click **Save**.

Session Manager then registers with the Remote Proxy Server. This may take a few minutes. The following progress message displays while the connection is established.



If you receive the following message, contact a Customer Care representative for assistance.



Enabling an On-Demand Remote Connection from an Endpoint

You must use any Mitel 5000 endpoint to enable or disable Remote Configuration sessions.

NOTE

Disabling Remote Configuration from a system endpoint prevents remote users from accessing the system in which the endpoint is registered.

To enable Remote Configuration from a system endpoint, the remote technician must provide you with the personal identification number (PIN) that is registered with the Remote Proxy Server. The remote technician must also enter the Mitel 5000 system license key ID, or Hardware Against Software Piracy (HASP) key. If necessary, you can use any system endpoint to view the HASP key and provide it to the remote technician, as described below.

To enable a Remote Configuration session:

1. On any system endpoint, dial **342**. ENTER PIN appears.
2. Enter the PIN number (supplied by the remote technician), and then press **#**. REMOTE CONFIG ENABLED appears.

To end a Remote Configuration session:

Dial **343**. REMOTE CONFIG DISABLED appears.

To display the license key ID (HASP key):

Dial **347**. HW SERIAL NUM <number> appears.

To reset the Remote Configuration session:

Dial **344**.

Private Networking and System Nodes

Introduction	4-2
Nodes	4-2
Local Nodes	4-2
Remote Nodes	4-3
Programming Remote Node Numbers	4-3
Changing Remote Node Information	4-3
Deleting a Remote Node	4-3
Remote Node Trunk/IP Connection Groups	4-4
Programming Remote Node Trunk/IP Connections Groups	4-4
Deleting Node Trunk Groups	4-4
Using a Remote Node Search Algorithm	4-5
Programming Remote Node Audio for Calls Camped onto this Device	4-5
Using The Networking Wizard	4-6
Starting the Private Networking Wizard	4-6
Configuring IP Networking	4-7
Configuring (Target Remote Node) IP Networking	4-7
Creating Off-Node IP Connections	4-8
Adding a Node Trunk/IP Connection Group	4-9
Configuring T1/E1 PRI Networking	4-10
Node Devices – Importing and Exporting	4-19
Modems	4-23
Off-Node Modems	4-24
Local Modems	4-25
Programming Local Modem Information	4-25
Configuring Local Modems	4-25
System Manager	4-26
Configuring the Node to Interface with System Manager	4-26
Uploading the System Manager CA Certificate	4-27

Introduction

This chapter provides information to help you configure network settings or add system nodes to a private IP or T1/E1 PRI network.

For more information about private networks and nodes, refer to the following chapters in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000:

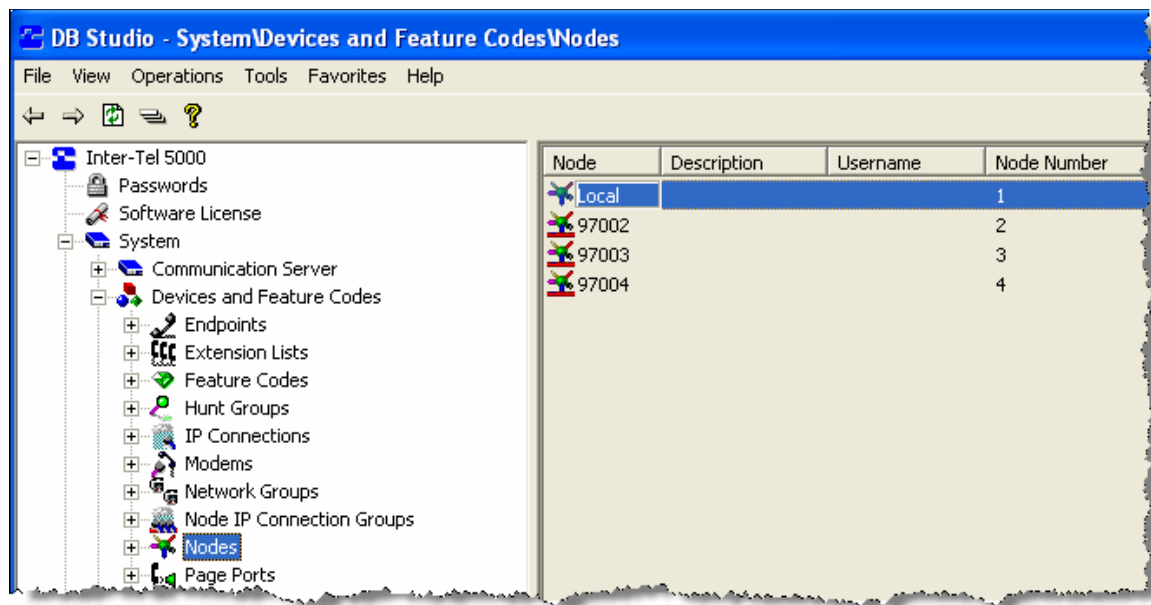
- Appendix A: Mitel Private Networking
- Appendix B: Network Topology

Nodes

The following sections describe local and remote nodes, as shown in [Figure 4-1](#), and how to create and program them. You must restart DB Programming when you create a node.

You can also use the Networking Wizard to quickly add and configure new nodes. See “Using The Networking Wizard” on [page 4-6](#).

Figure 4-1. DB Programming Local and Remote Nodes



Local Nodes

The local node is automatically created in DB Programming when the system is installed. For the local node, you can only assign the description, username, and node number.

Remote Nodes

Remote nodes are Mitel Advanced Communication Platform systems, such as the Mitel 5000 and Inter-Tel Axxess systems, which are connected to the local node. You must program each remote node with a node number, node trunk groups, and a search algorithm.

Your system supports up to 63 nodes (1–63). However, if your system meets compatibility requirements, you can also configure nodes 64–99. For more information about 99-Node configurations, refer to the “Private Networking” chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

Programming Remote Node Numbers

If you change the node number, the system resets when you exit.

To change the current node number:

1. Select System – Devices and Feature Codes – Nodes – **<node>**.
2. In the **Value** column, type the new number in the box. If the number you entered conflicts with an existing node number, an error message appears. You must change the number to a valid value.
3. Click out of the field or press **ENTER** to save the change.

Changing Remote Node Information

You can change the node description or user name.

To change the description and user name:

1. Select System – Devices and Feature Codes – Nodes – **<node>**.
2. Select the appropriate field, and then type the new information in the box. Descriptions can have up to 20 characters; Usernames can have up to 10 characters. Do not use slash (/), backslash (\), vertical slash (|), or tilde (~) characters in usernames. Do not use Control characters in descriptions or usernames.
3. Click out of the field or press **ENTER** to save the change.

Deleting a Remote Node

To delete a remote node:

1. Save the database.
2. Restart the session in local mode. You cannot remove a remote node while the session is in remote mode.
3. Select System – Devices and Feature Codes – **Nodes**.
4. Right-click the remote node that you want to remove.
5. Select **Delete**.
6. Click **Yes** to restart DB Programming.
7. Restore the database to the system in remote mode.

Remote Node Trunk/IP Connection Groups

Each remote node has a list of node trunk or node IP connection groups that access other remote nodes. The node IP connection groups correspond to an IP connection between a remote node and a local node. For each node in the network, you must define the routes to every other node. For example, in a network with four nodes, you would define three routes for each node (one to each of the other three nodes). For an example of node programming, refer to the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

Programming Remote Node Trunk/IP Connections Groups

To program the node trunk or node IP connection groups included in this node:

1. Select System – Devices and Feature Codes – Nodes – **<node>**.
2. Double-click **Node Trunk/IP Connection Groups**.
3. Do the following:

To add trunk or IP connection groups to the list:

Note that this is an *ordered list*. Place the trunk or IP connection groups in the order you want them to be accessed when the hunt group (if applicable) receives calls.

- *To add to the bottom of the list:* Do not select any existing trunk or IP connection groups.
- *To add to the list above an existing trunk group:* Select the trunk or IP connection group.
 - a.) Right-click in the right pane, and then click **Add To Node Trunk/IP Connection Groups List**. A window appears prompting for the device type to include.
 - b.) Select **Node Trunk Group** or **Node IP Connection Group**, and then click **Next**.
 - c.) The items with details appear. To view items in a list only, click **List**. Select the items (you can use the SHIFT or CTRL key to select more than one item), and then click **Add Items**.
 - d.) When you have added all the node trunk groups necessary, click **Finish**. The selections appear in the list. To view programming options, double-click the extension number.
- *To move a trunk or IP connection group to another location in the list:*

Drag and drop the trunk or IP connection group to the new position. Or, select the trunk or IP connection group to move and press **CTRL** + the up/down arrow to move the trunk or IP connection group up or down in the list.

Deleting Node Trunk Groups

To delete a node trunk group:

1. Select System – Devices and Feature Codes – Nodes – **<node>**.
2. Double-click **Node Trunk/IP Connection Groups**.
3. Select the node trunk or IP connection group.
4. Right-click, and then select **Remove Selected Items**. The item is removed from the list.

Using a Remote Node Search Algorithm

The search algorithm determines whether the node trunk groups are accessed in linear or distributed order:

- **Linear:** The system first attempts to route a call through the first node trunk group listed. If it is unable to route through that node trunk group, it attempts to route the call through the second node trunk group in the node. The system continues to attempt to route the call through the subsequent node trunk groups listed in the node until it successfully routes the call or exhausts all node trunk groups in the list.
- **Distributed:** The system equally distributes the first node trunk group used with each call. For example, if the system routed the first call through the first node trunk group in the node, it routes the second call through the second node trunk group in the node.

Determining the order to list the Node Trunk or IP Connection Groups in a node and when to use Linear or Distributed search type depends on your system configuration and traffic. For example, if the Node Trunk or IP Connection Group List has more than one trunk group that connects to the same node, you should use the Linear search type instead of Distributed. For more information, refer to “Appendix A: Mitel Private Networking,” in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

To set the search algorithm:

1. Select System – Devices and Feature Codes – Nodes – *<node>* – **Search Algorithm**.
2. In the **Value** column, select either **Linear** or **Distributed**.
3. Click out of the field or press **ENTER** to save the change.

Programming Remote Node Audio for Calls Camped onto this Device

The Audio for Calls Camped onto this Device field defines the audio that callers hear when camped-on to the node trunk or IP connection group. For more information about audio settings, see “Device Audio for Calls Settings” on [page 7-65](#).

To program the Audio for Calls Camped onto this Device field:

1. Select System – Devices and Feature Codes – Nodes – *<node>* – **Audio for Calls Camped onto this Device**.
2. In the **Value** column, select the option from the list.
3. Click out of the field or press **ENTER** to save the change.

Using The Networking Wizard

The Networking wizard allows you to quickly configure IP T1/E1 PRI networking for existing or new nodes, as shown in the following sections:

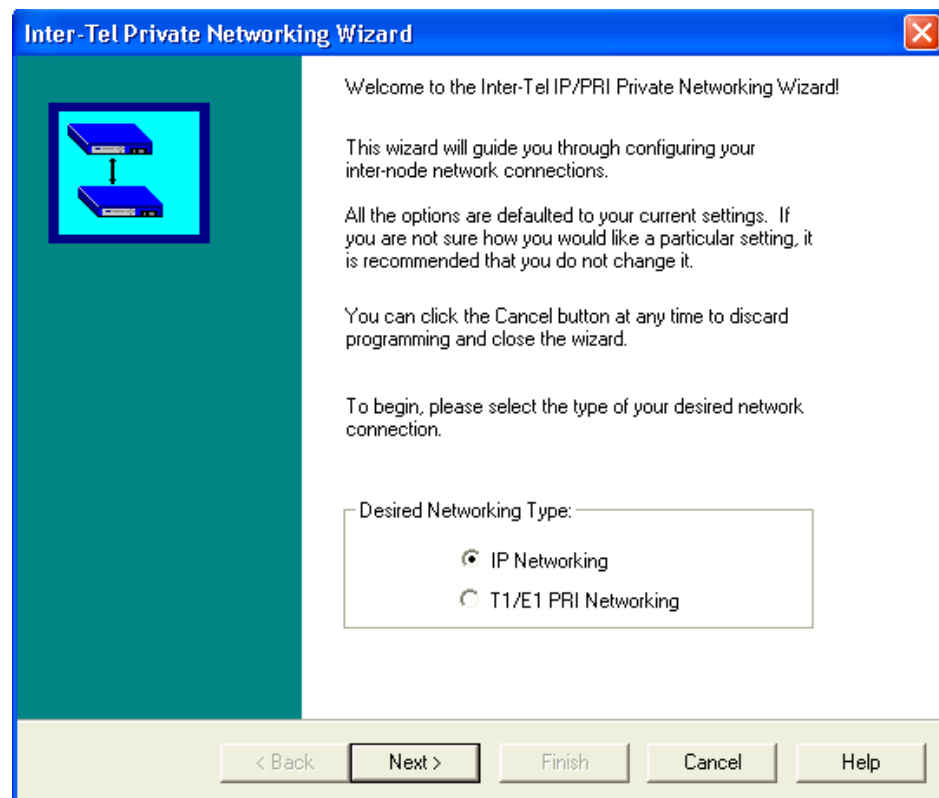
- “Starting the Private Networking Wizard” on [page 4-6](#) below
- “Configuring IP Networking” on [page 4-7](#)
- “Configuring T1/E1 PRI Networking” on [page 4-10](#)

Starting the Private Networking Wizard

To start the Private Networking Wizard:

1. From the DB Programming menu bar, select **Tools**, and then select **Networking Wizard**. The Networking Wizard Welcome screen appears, as shown in [Figure 4-2](#).

Figure 4-2. Networking Wizard



2. Depending on your system configuration, continue to either “Configuring IP Networking” on [page 4-7](#) or “Configuring T1/E1 PRI Networking” on [page 4-10](#).

Configuring IP Networking

The following sections describe IP networking configurations:

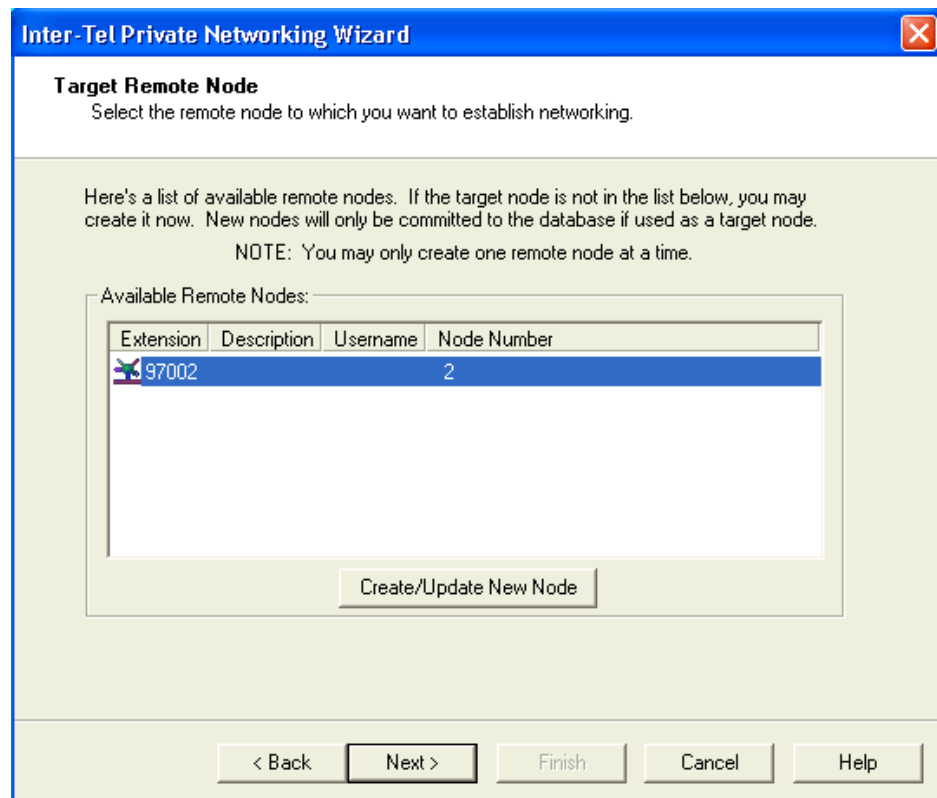
- “Configuring IP Networking” on [page 4-7](#)
- “Configuring (Target Remote Node) IP Networking” on [page 4-7](#)
- “Creating Off-Node IP Connections” on [page 4-8](#)

Configuring (Target Remote Node) IP Networking

The following sections describe IP networking settings for existing or new nodes.

To configure IP networking for an existing or new node:

1. After starting the Networking Wizard, select **IP Networking**, and then click **Next**. The Target Remote Node dialog box appears.



2. Do one of the following:
 - To configure an existing node:
 - Select the existing node from the list.
 - To configure a new node:
 - a. Click **Create/Update New Node**. The Create Remote Node dialog box appears.
 - b. Select an **Extension** for the node from the list.
 - c. Enter a node **Description** and **Username**.
 - d. Select the **Node Number** from the list. Make sure the node number you select for the new node complies with the site numbering plan.
 - e. Click **OK**. The new node is added to the Target Remote Node screen.
3. Click **Next**. Continue to “Creating Off-Node IP Connections” on [page 4-8](#).


Creating Off-Node IP Connections

The following section describes how to create a new IP connection.

To create a new IP connection:

1. In the Off Node IP Connection Configuration screen (shown above), click **Add Off-Node IP Connection**. The Create Off-Node IP Connection dialog box appears.

The screenshot shows a window titled "Inter-Tel Private Networking Wizard" with a close button in the top right corner. The main title is "Off-Node IP Connection Configuration" with the subtitle "Change and/or update Off-Node IP Connections". Below this, a text block reads: "For the detailed view of any of the Off-Node IP Connections in the list below, please right-click on the desired item. If the connection to the target node will be established through an intermediate node, you may skip ahead by clicking the 'Next' button." Below the text is a section titled "Off-Node IP Connections:" containing a table with three columns: "Extension", "Description", and "Username". The table has one row with a small icon, "P6002", and empty fields for Description and Username. Below the table is a button labeled "Add Off-Node IP Connection". At the bottom of the window are five buttons: "< Back", "Next >", "Finish", "Cancel", and "Help".

Extension	Description	Username
 P6002		

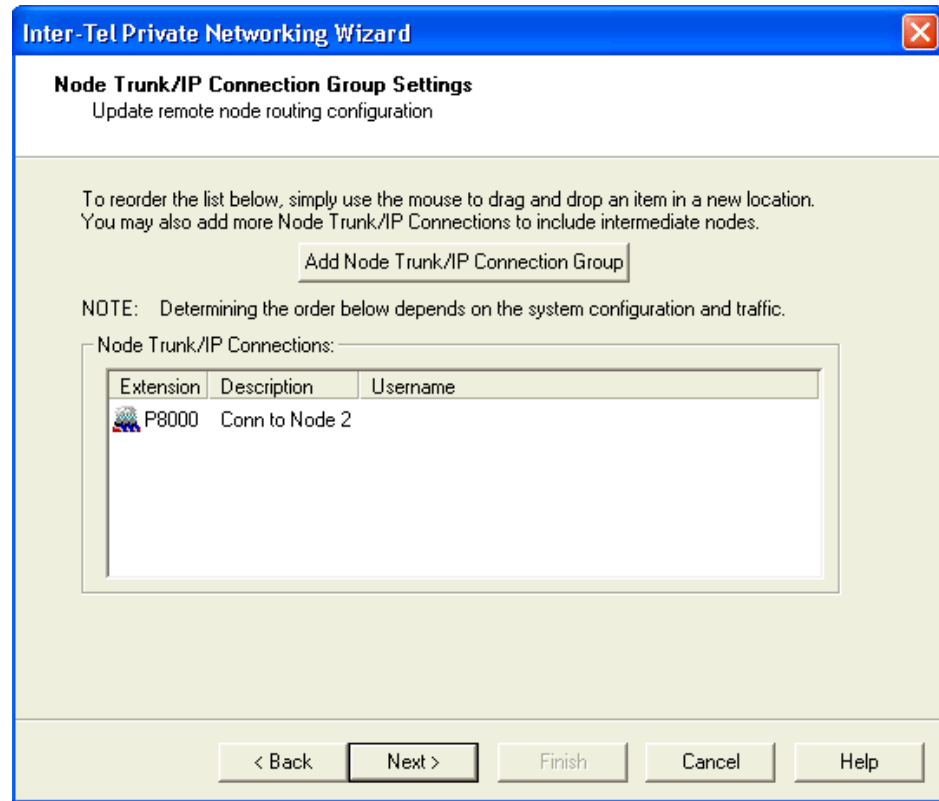
2. Select the **Extension** for the off-node IP connection from the list. Make sure the extension you select for the new IP connection complies with the site numbering plan.
3. In the **Description** and **Username** boxes, type the description and user name.
4. In the **IP Address** box, edit the IP address if necessary.
5. In the **Audio Receive Port**, edit the port number if necessary or use the default (6004).
6. In the **Listening Port box**, edit the listening port number if necessary or use the default (5570).
7. Click **OK**, and then click **Next**. The new off-node IP connection is added to the wizard. If you want to use the new IP connection, select it from the list. You can also right-click the entry to edit or delete it.
8. Click **Next**.
9. Click **Finish**. A message may appear stating that DB Studio is shutting down. This occurs if you created the first remote node using the Networking Wizard. Click **OK**.
10. Continue to "Adding a Node Trunk/IP Connection Group" on [page 4-9](#).

Adding a Node Trunk/IP Connection Group

Use the following procedure to add a Node Trunk/IP Connection Group.

To add a Node Trunk/IP Connection Group:

1. Click **Add Node Trunk/IP Connection Group**. The Add Node Trunk/IP connection Groups dialog box appears, pre populated with the system Node Trunk/IP Connections.



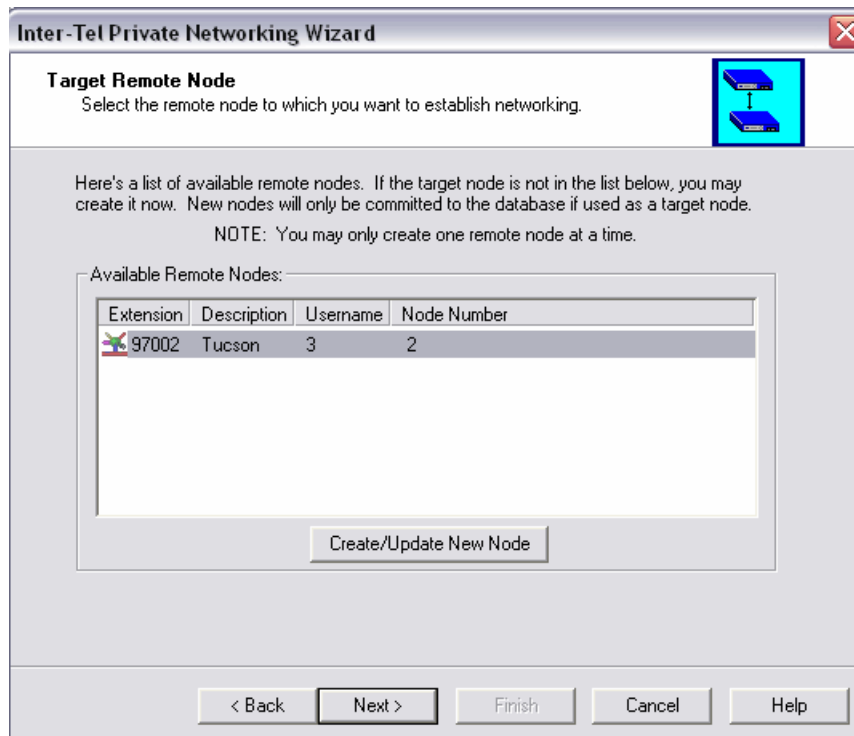
2. Select one or more Node Trunks or IP Connections and click **Add Item(s)**.
3. Click **Close**. The Node Trunks/IP Connections that you selected are added to the wizard.
4. Based on your system configuration and traffic, if necessary, reorder the list of Node Trunk/IP Connections by dropping and dragging them with the mouse.
5. Click **Next**. IP Networking configuration is complete.

Configuring T1/E1 PRI Networking

The following section describes instructions on how to configure the T1/E1 PRI Networking.

To configure PRI Private Networking:

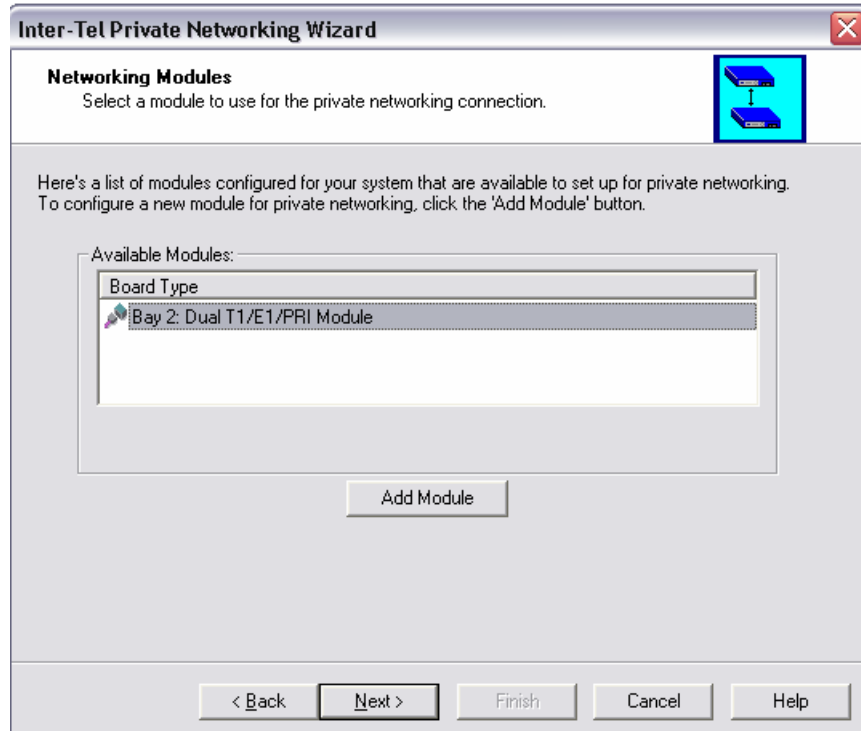
1. From the Networking Wizard Welcome screen, select **T1/E1 PRI Networking**, and then click **Next**. The Target Remote Node screen appears.



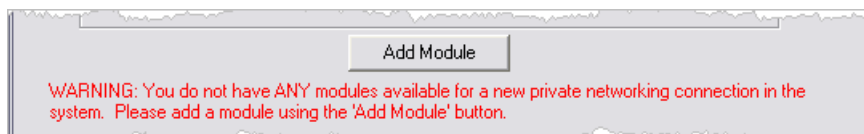
2. Select the existing node from the list, and then click **Next**.
3. *If the Networking module exists*, select the networking node from the list and then click **Next**.

If the Networking module does not exist, go to step 5 on [page 4-11](#).

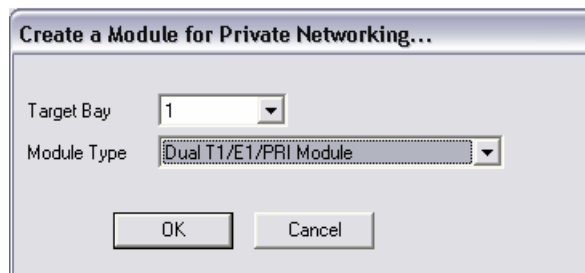
4. In the Networking Modules screen, select a **T1/E1/PRI Module** or **Dual T1/E1/PRI Module** for the private networking connection. If a module is available for private networking it is shown in the list. A module is considered “available” if it has at least one port that can support a new private networking connection. Modules that can support a new private networking connection include: “None” or T1/PRI or E1/PRI modules that are not already set up with a private networking connection.



If no modules are available, the following warning appears.



5. To create a new module, click **Add Module**. A dialog box pops up showing the available bays and module types.

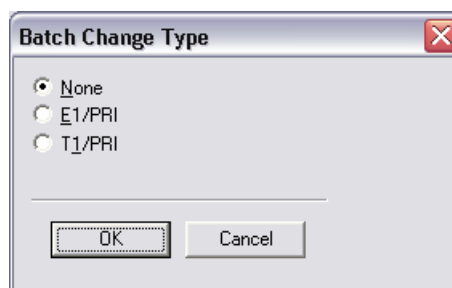


6. Select the desired information, and then click **OK**. The module appears in the Available Modules list.

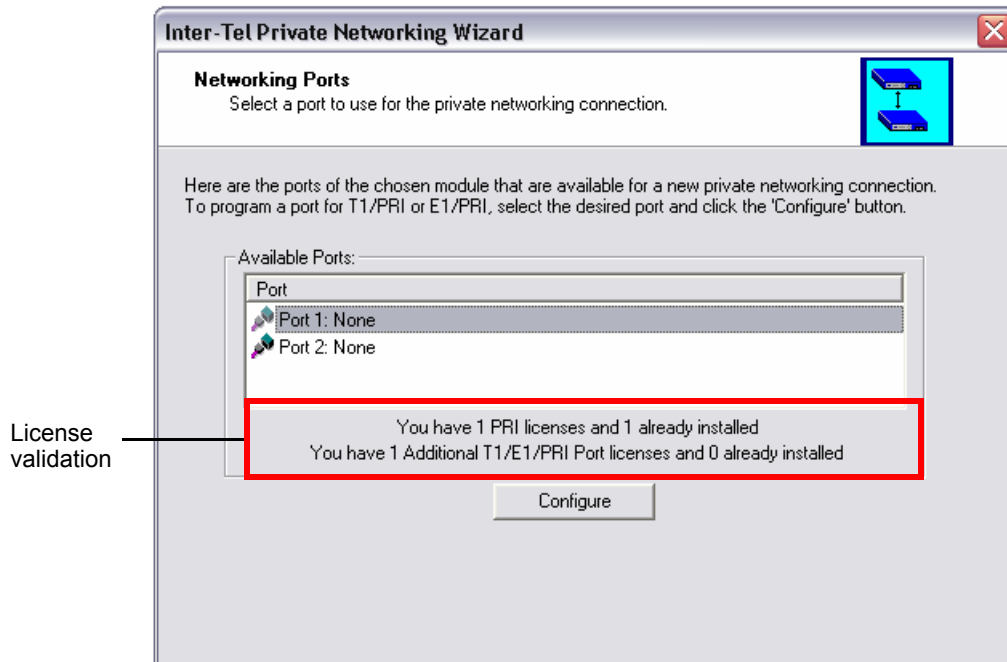
- After a module is selected, click **Next**. The Networking Ports screen appears. The Networking Ports screen shows the available ports from the selected module. Ports are considered available if they are configured as “None” ports, or T1/PRI or E1/PRI ports that are not already set up with a private networking connection.



- Click **Configure**. The following dialog box appears.



9. Select **T1/PRI** or **E1/PRI** for a private networking connection. The Networking Ports screen shows the results after the system validates the license, as shown below.



Trying to configure additional ports that exceed licensing causes the following warnings:

WARNING: Equipping this PRI port will exceed the number of PRI ports allowed in the software license. If you continue, not all ports will come online.

WARNING: Equipping the second port of this Dual T1/E1/PRI Module will exceed the number of Additional T1/E1/PRI ports allowed in the software license. If you continue, not all ports will come online.

10. Select a PRI port, and then click **Next** to configure the port. The T1/E1 Private Networking Configuration screen appears.

The screenshot shows a window titled "Inter-Tel Private Networking Wizard" with a close button in the top right. Below the title bar is a sub-header "T1/E1 Private Networking Configuration" with the instruction "Change and/or update PRI configuration" and a small icon of two network nodes. The main area contains several fields and sections:

- Port:** A dropdown menu showing "01:01.02 T1/PRI". To its right is a text instruction: "Select a port and verify the settings below to ensure that they comply with your network settings. Please contact a system administrator if you need assistance."
- Node Trunk Group:** A section with three fields: "Extension" (a dropdown showing "97501"), "Description" (a text box containing "Conn to Node 2"), and "Username" (an empty text box).
- Reference Clock List:** A section with a note: "Note that this setting has to be different on the other node for these two nodes to communicate." Below the note are two radio buttons: "Slaves to Private Network" (which is selected) and "Master for Private Network".
- Advanced:** A button located below the Reference Clock List section.

At the bottom of the window are five buttons: "< Back", "Next >", "Finish", "Cancel", and "Help".

11. For the **Node Trunk Group**, configure the following:
 - **Extension:** Select a node trunk group extension from the list.
 - **Description and Username:** Enter a description and username for the node trunk group.
12. For the **Reference Clock List**, configure the following:

NOTE

For more information about the Reference Clock list and PRI fields, refer to the "Installation" chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000 or *Mitel 5000 DB Programming Help*.

- Slaves to Private Network (Default setting)
 - Master for Private Network
13. For the **PRI Fields**, configure the following:
 - Line Build-Out
 - CO Provides Progress Tones
 - Connect On Call Proceeding

14. Click **Advanced** to display advanced programming options, as shown below.

Configure Advanced PRI Settings...

Configure the following settings for the selected PRI port.

Haul Mode: Long Haul

Line Build-Out: 0 dB (DSX-1)

Span Companding Type: Mu-Law

To submit your changes, click 'OK'. Otherwise, click 'Cancel' to keep the default settings for these fields.

For a Dual T1/E1/PRI module, the Span Companding Type field is displayed. This field is not displayed for T1/E1/PRI module ports.

For T1/PRI ports, haul mode and either line build-out or loop length (depending on haul mode selection) is displayed.

Configure Advanced PRI Settings...

Configure the following settings for the selected PRI port.

Haul Mode: Short Haul

Loop Length: 0 - 133 ft.

Span Companding Type: Mu-Law

To submit your changes, click 'OK'. Otherwise, click 'Cancel' to keep the default settings for these fields.

For E1/PRI ports, line impedance is displayed instead of haul mode fields.

Configure Advanced PRI Settings...

Configure the following settings for the selected PRI port.

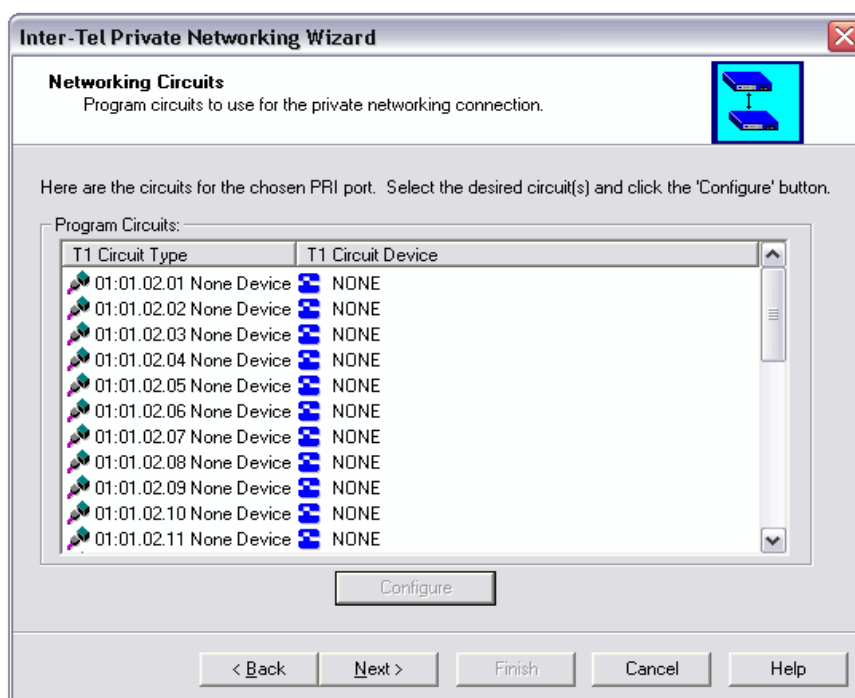
Line Impedance: 120 ohms

Span Companding Type: Mu-Law

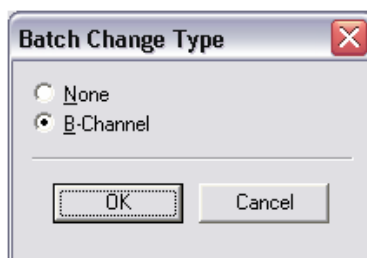
To submit your changes, click 'OK'. Otherwise, click 'Cancel' to keep the default settings for these fields.

For more information about these fields, refer to *Mitel 5000 DB Programming Help*.

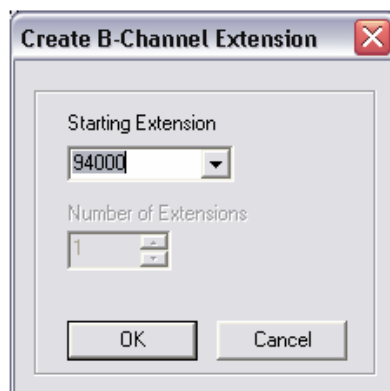
15. Click **Next** to configure the circuits. The Networking Circuits screen appears.



For T1/PRI ports, 23 circuits are displayed for programming. Thirty circuits are displayed for E1/PRI ports. To program circuits, select the desired locations, and then click **Configure**. Select **B-Channel** from the following dialog box.

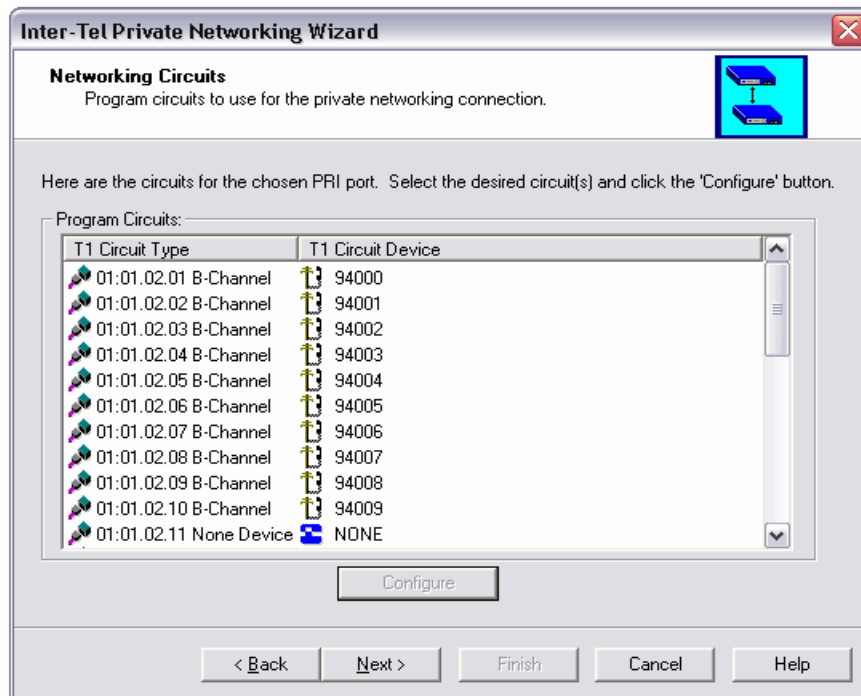


16. Click **OK**. The Create B-Channel Extension dialog box appears.

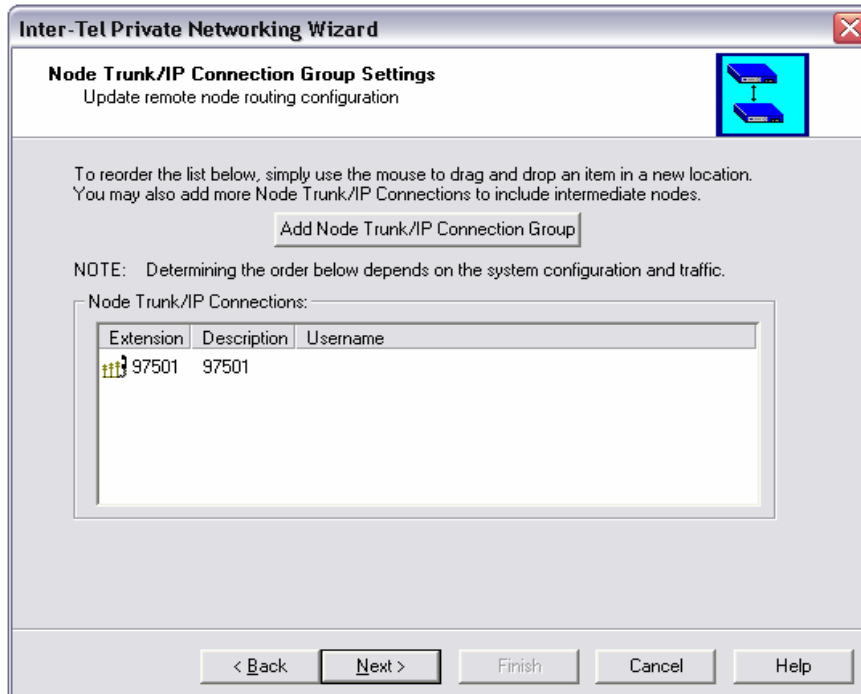


17. Select the starting extension.

18. Click **OK** to display the circuits that you have programmed in the Networking Circuits page.



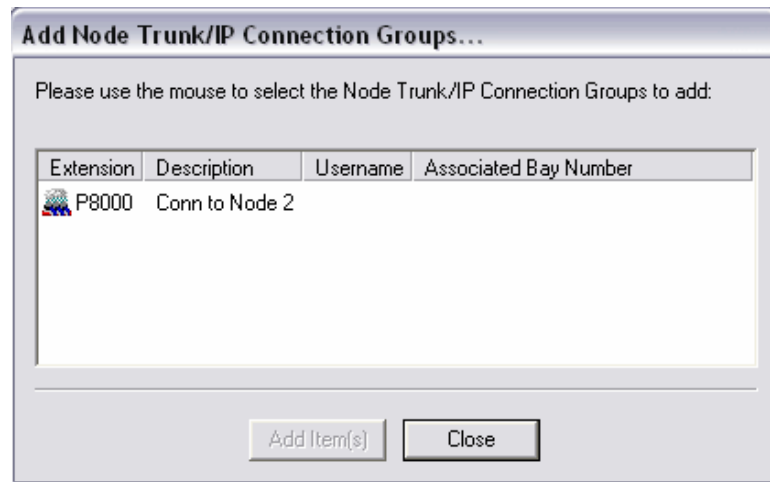
19. Click **Next**. The Node Route group screen appears.



20. *If Node Trunk/IP Connection Group Settings exist*, select the Node Trunk/IP Connection from the list, and then click **Next**.

If Node Trunk/IP Connection Group Settings do not exist, add a Node Trunk/IP Connection Group using the instructions below.

- a. Click **Add Node Trunk/IP Connection Group**. The Add Node Trunk/IP connection Groups dialog box appears. The dialog box is pre-populated with the Node Trunk/IP Connections Groups in the system.
- b. Select one or more Node Trunks or IP Connections and click **Add Item(s)**.



- c. Click **Close**. The Node Trunks/IP Connections you selected are added to the wizard.
21. Based on your system configuration and traffic, if necessary, reorder the list of Node Trunk/IP Connections by dropping and dragging them with the mouse.
 22. Click **Next**. The wizard complete screen appears.
 23. Click **Finish**. A message may appear stating that DB Studio is shutting down. This occurs if you created the first remote node using the networking wizard.
 24. Click **OK**.

Node Devices – Importing and Exporting

Perform this option after hours, when system usage is at a minimum. When another node adds a new extension or changes an existing extension, username, or description, the network broadcasts the new extension information to the other nodes in the network. Or, you can export local device information to other nodes, or import devices from the other nodes to the local node, using the Export/Import option in this menu. If there is a conflicting (duplicate) extension in a broadcast from another node, the receiving node ignores the new extension in favor of its existing extension number.

NOTE

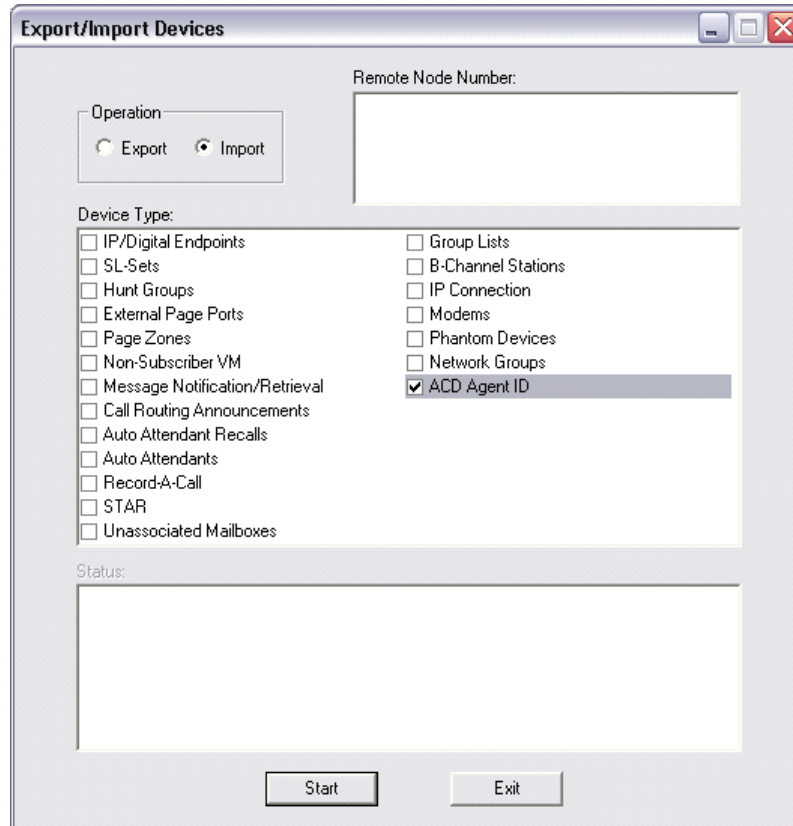
In the default state, the Voice Processor Enable flag is enabled. If you do not have an external voice processing system connected to the Mitel 5000, disable this flag before attempting to import or export information over the network.

If the network is unable to export or import an extension to a node (automatically or using the Export/Import feature) because there is an active programming session on that node, the node is unable to communicate with its Voice Processor port, the node is down, or the links to the node are down, the new extension will not be added to or changed on that node. (If Message Print is enabled, error messages will indicate any unsuccessful broadcasts.) You must manually add or change the new extension in the node database or try to export or import it later. You may want to check each node to verify that their off-node device lists are programmed properly to allow access between the nodes.

Extension numbers that exist before the network is established will not be automatically broadcast to other nodes, until they are modified. They must be exported or imported using the Export/Import option or programmed manually at each of the other nodes. Also, each node can have only 8000 off-node device entries in its database. When that limit has been reached, new devices received through network broadcasts cannot be added to that node database.

To export or import devices:

1. Start Session Manager.
2. From the DB Programming menu bar, select Operations – **Export/Import Devices**. The following dialog box appears. You must have a programmed Node to export or import information from the node.



The dialog box titled "Export/Import Devices" contains the following elements:

- Operation:** Two radio buttons, "Export" and "Import". The "Import" button is selected.
- Remote Node Number:** A large empty text box for entering a node number.
- Device Type:** A list of checkboxes for selecting device types to export or import. The "ACD Agent ID" checkbox is checked.

Device Type	Selected
IP/Digital Endpoints	<input type="checkbox"/>
SL-Sets	<input type="checkbox"/>
Hunt Groups	<input type="checkbox"/>
External Page Ports	<input type="checkbox"/>
Page Zones	<input type="checkbox"/>
Non-Subscriber VM	<input type="checkbox"/>
Message Notification/Retrieval	<input type="checkbox"/>
Call Routing Announcements	<input type="checkbox"/>
Auto Attendant Recalls	<input type="checkbox"/>
Auto Attendants	<input type="checkbox"/>
Record-A-Call	<input type="checkbox"/>
STAR	<input type="checkbox"/>
Unassociated Mailboxes	<input type="checkbox"/>
Group Lists	<input type="checkbox"/>
B-Channel Stations	<input type="checkbox"/>
IP Connection	<input type="checkbox"/>
Modems	<input type="checkbox"/>
Phantom Devices	<input type="checkbox"/>
Network Groups	<input type="checkbox"/>
ACD Agent ID	<input checked="" type="checkbox"/>
- Status:** A large empty text box for displaying the operation status.
- Buttons:** "Start" and "Exit" buttons at the bottom.

3. Select the following information, and then click **Start**. Or, click **Exit** to cancel the operation without exporting any information.
 - **Operation:** Select the desired option to determine whether you will be importing devices into the local node or exporting local devices to a remote node.
 - **Remote Node Number:** Select the node(s) you want to export the information to or import the information from, by placing checks in the appropriate boxes.
 - **Device Type:** Select any combination of device types you want to export or import by checking the appropriate boxes. IP device information is automatically included if you import or export all endpoints. In addition, IP SLAs are automatically included if you import or export all single line sets.

NOTE

ACD agents may be imported or exported the same as the other device types.

When you click **Start** to begin the export or import operation, the lower panel shows the export or import status.

If you are exporting information, the node you are exporting from is listed as "Node X: Export Source." The destination node or nodes will show the node number and the current status of the export. Once the import from a node is completed, either successfully or unsuccessfully, the import source node displays the final status of the import. The screen will show messages as explained in [Table 5-8](#).

Table 4-1. *Node Status Descriptions*

Status	Meaning
Starting Up	Indicates that the node is attempting to initiate the export.
Creation XX%	This node is XX percent done with the creation portion of the export.
Deletion XX%	This node is XX percent done with the deletion portion of the export.
COMPLETED	This node successfully completed the export.
Waiting...	When importing, this status indicates that this node is waiting for another node to finish before it can become an import source
Error – Not Reachable	The export to the node failed because the export source node could not communicate with this node.
Error – Endpoint Programming	The export to the node failed because someone on the node was performing Endpoint Programming.
Error – Voice Processor	The export to the node failed because the link to the Voice Processor is down.
Error – DB Programming	The export to the node failed because someone on the node was performing DB Programming.

4. After completing an import operation, close DB Programming to update the database.

If the local node cannot communicate with the remote node, the export or import will fail. Before you attempt to export or import information, verify that you can reach the remote node by dialing the extension assigned to the remote node. If you hear dial tone, you should be able to successfully export or import information. If you receive a NOT REACHABLE message, you must determine why calls are not properly being routed to the specified remote node before you can export or import information. If you camp on to a node while trying to reach the remote node, wait for the node trunk group to become available so that you can guarantee the remote node can be reached.

5. After attempting to export or import information, check Message Print output for error messages:
 - If a programming session is active on the remote node, you cannot export information to that node until the programming session has been terminated. Also, if the remote node has a Voice Processor and the link is down, the export will fail on the remote node.
 - If an existing extension on the remote node conflicts with an exported extension number, you will see one of the error messages listed in the following table. The error message indicates the resulting action on the remote node. In the example used in Table 4-2 on [page 4-22](#), the device information was exported from local node 1 to remote node 2.

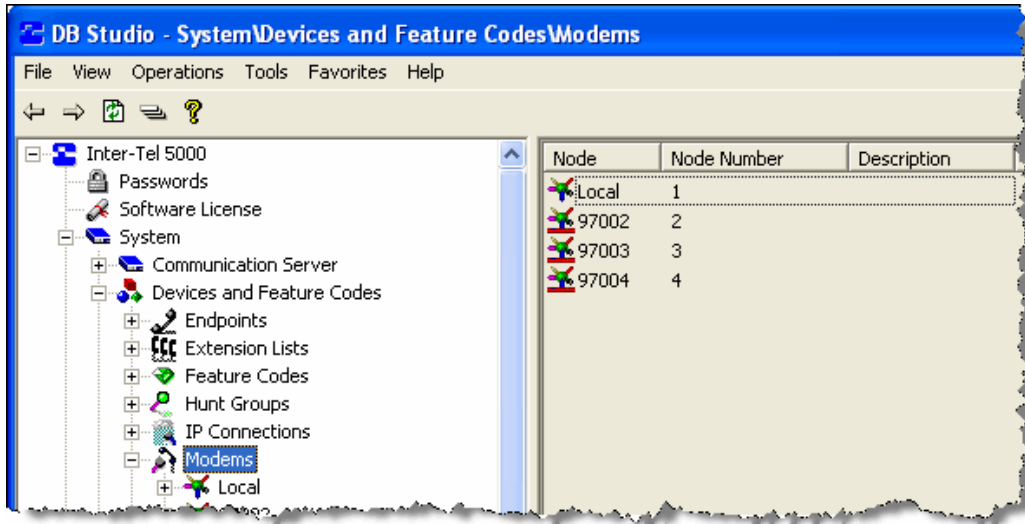
Table 4-2. *Example of Exporting an Extension from One Node to Another*

Extension # Exported From Local Node 1	Existing Extension # ON Remote Node 2	Results on Remote Node 2
Endpoint 1000	Endpoint 10	WRN DB CP Device Info Import For ID(1:'1000') Failed: Conflict with existing extension
Endpoint 1000	Endpoint 100	WRN DB CP Device Info Import For ID(1:'1000') Failed: Conflict with existing extension
Endpoint 1000	Endpoint 1000	WRN DB CP Device Info Import For ID(1:'1000') Failed: Conflict with existing extension
Endpoint 1000	Off-Node Device ID(3:1000)	WRN DB CP Device Info Import For ID(1:'1000') Failed: Conflict with existing extension
Endpoint 1000	Unassociated Mailbox 1000	Off-Node Device ID(1:1000) created and Mailbox 1000 is associated with the off-node device
Hunt Group 2000	Unassociated Mailbox 2000	Off-Node Device ID(1:2000) created and Mailbox 2000 is associated with the off-node device
Endpoint 1000	Unassociated Mailbox 100	Off-Node Device ID(1:1000) created and Unassociated Mailbox is deleted
Endpoint 1000	Off-Node SL-Set ID (1:1000)	Off-Node Device ID(1:1000) deleted and Off-Node Device ID(1:1000) created
Page Port 91000 (99000 in Europe)	Unassociated Mailbox 91000 (or 99000)	Off-Node Device ID(1:91000 or 1:99000) created and Mailbox 91000 (or 99000) remains unassociated
Endpoint 1000	Off-Node Device ID (1:10XX)	WRN DB CP Device Info Import For ID(1:'1000') Failed: New extension matches existing wildcard

Modems

You can create off-node devices for modems on the other nodes and program individual modems on the Local node, as shown in Figure 4-3.

Figure 4-3. DB Programming Local and Off-Node Modems



NOTICE

Possible Database Corruption. Poor line quality may cause data transmission problems when the modem connection exceeds 19200 baud. For this reason, Mitel recommends that you do *not* use the modem to restore the database. If you attempt a restore using the modem, the database may become corrupt.

Off-Node Modems

IMPORTANT

You cannot program off-node modems across an IP connection. Also, you must program a remote node on the system before you can create an off-node modem extension.

Off-node modems allow access to modems on other nodes. When you double-click a remote node, a list of its existing off-node page modems with extensions, descriptions, and usernames appears. You can create or delete off-node modems. After you create the modems, you can change modem extensions and enter descriptions and usernames. When programming modems, follow a universal numbering plan (for example, the extensions must be unique).

NOTICE

System Instability. Do not create or delete more than 2000 off-node devices at a time. Batch creating more than 2000 off-node devices may cause system problems.

To program off-node modem extensions:

1. Select System – Communication Server – Devices and Feature Codes – Modems – **<node>**.
2. Right-click in the right pane, and then select **Create Off-Node Modem**.
3. Select the starting extension and the number of modem extensions you want to create. The extension you assign to the off-node modem must match the extension programmed locally on that node. For example, if the modem extension for node **2** is **1502**, the off-node modem extension on other nodes must be **1502**.
4. For each extension, program the description (using up to 20 characters) and the user name (using up to 10 characters). After you program the off-node modem extension, you can use the off-node modem extension for the same functionality as the local modem extension.

Local Modems

You can program local modems.

Programming Local Modem Information

All modem extensions should have a description and a username.

To program the local modem description and user name:

1. Select System – Devices and Feature Codes – Modems – **Local**.
2. Enter the description and user name. The description can be up to 20 characters long. The user name, which appears on display endpoints, can have up to 10 characters. To program the names, select the desired text box and type the entry. Do not use slash (/), backslash (\), vertical slash (|), or tilde (~) characters in usernames. Do not use Control characters in descriptions or usernames.
3. Click out of the fields or press **ENTER** to save your changes.

Configuring Local Modems

To configure local modems:

1. Select System – Devices and Feature Codes – Modems – **Local**.
2. Double-click a modem extension, and then program either of the following fields:
 - **Modem Enabled:** Allows the modem to accept incoming calls, if enabled. If disabled, the modem does not accept incoming calls, and INVALID EXTENSION appears on display endpoints. By default, this is set to **Yes**. You can also use the administrator endpoint to reset the modem. For more information about using the administrator endpoint, refer to the *Mitel 5000 Endpoint and Voice Mail Administrator Guide*, part number 580.8001.
 - **Minimum Bit Rate:** Select the minimum bit rate the modem will use for its connection. The range is 9600–33600, and the default is 9600.
3. After programming the modem information, assign the modem extension as the following:
 - **Trunk Group Ring-In Destinations:** Allows remote access of the modem using a trunk call. See “Day or Night Multiple Ring-In Types” on [page 8-12](#).
 - **Call Routing Table Ring-In Destinations:** Allows modem access using one or more specific endpoint numbers. See “Call Routing Tables” on [page 6-22](#).
 - **Voice Mail Extension ID for Auto Attendant and Digit Translation:** Allows modem access through the Auto Attendant or Voice Mail extension. See “Extension IDs” on [page 11-47](#).

System Manager

System Manager is a server-based application that centralizes management functions for Mitel 5000 platforms. For more information about System Manager, refer to the *System Manager Installation Manual*, part no. 835.2743.

Configuring the Node to Interface with System Manager

To allow remote management, each system node must physically connect to the System Manager server. After a connection is established, the node is considered an “agent” to System Manager.

To configure the node to interface with System Manager:

1. Under System, double-click **System Manager**. If you have not selected a time zone, a warning message appears. You must first program a time zone before you can enable System Manager changes.
2. Configure the following options:
 - **Enable Connection:** Determines whether or not the node will attempt to connect to System Manager. Enable the option to allow the node to connect to System Manager. If disabled, the node will not connect to System Manager. By default, this option is disabled.
 - a. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
 - b. Click out of the field or press **ENTER** to save the change.
 - **History Capacity Limit:** Sets the size limit of the history message buffer for the Call Processing agent before messages are sent to Call Processing.
 - a. In the **Value** column, click the current value.
 - b. Type the new number or select the new number from the list.
 - c. Click out of the field or press **ENTER** to save the change.
 - **IP Address:** Identifies the IP address of the System Manager server.
 - a. In the **Value** column, click the current Value. The Edit IP Address dialog box appears.
 - b. Type the correct IP address, and then click **OK**. By default, this value is *192.168.200.1*.
 - c. Click out of the field or press **ENTER** to save the change.
 - **Password:** Identifies the password for the agent account that is programmed in System Manager.

NOTE

The **Username** and **Password** fields must match the information that is programmed in System Manager. If these fields do not match the agent account information, the node will **not** connect to System Manager.

- a. In the **Value** column, click the current value.
 - b. Enter the password, up to 64 characters. This field is case-sensitive.
 - c. Click out of the field or press **ENTER** to save the change.
- **Port:** Identifies the port used to connect to the System Manager server.
 - a. In the **Value** column, click the current value.
 - b. Type the new number. The valid range is 1025–65535; the default is 3707.
 - c. Click out of the field or press **ENTER** to save the change.

- **Require System Manager ACK:** When enabled, Call Processing sends an acknowledgement to the Call Processing agent whenever the Call Processing agent sends Call Processing a history message.
 - a. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
 - b. Click out of the field or press **ENTER** to save the change.
- **Send CPH to System Manager:** When enabled, the Call Processing agent sends history messages to Call Processing.
 - a. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
 - b. Click out of the field or press **ENTER** to save the change.
- **Username:** Indicates the user name of the agent account that is programmed in System Manager.
 - a. In the **Value** column, click the current value.
 - b. Enter the user name, up to 64 characters. This field is case-sensitive.
 - c. Click out of the field or press **ENTER** to save the change.
- **Valid CA Certificate:** Read only field that shows whether or not the CA certificate is valid. If not, you must upload the certificate. See the following section.

Uploading the System Manager CA Certificate

If a node will connect to System Manager, you must upload the Certification Authority (CA) certificate. The certificate allows the node to use Secure Socket Layer (SSL) for secure connections.

NOTE	You cannot upload the CA certificate while in local mode.
-------------	---

To upload the CA certificate:

1. From the DB Programming menu bar, select Operations – **System Manager CA Certificate Upload**.
2. When prompted, click **Browse**, and then locate the CA certificate. The certificate is usually in the following directory: C:\Inter-Tel\System Manager\CA. Certificates have a .cer extension.
3. Click **Start**. The CA certificate is uploaded.

Numbering Plans

Introduction	5-3
Area Flags	5-4
Classes of Service (COS)	5-5
COS for U.S. Systems	5-5
COS for European Systems	5-6
Programming COS Options	5-7
Changing or Adding COS Descriptions	5-7
Adding Devices to COS Day and Night Lists	5-7
Defining COS Dialing Patterns	5-8
Programming Dialing Pattern Digits	5-8
Allowing or Restricting Dialing Patterns	5-8
Device Baseline Extensions	5-9
Automatic Route Selection (ARS)	5-10
Planning ARS Requirements	5-11
Programming ARS Dial Rules	5-12
Programming ARS Facility Groups	5-13
Creating and Deleting Facility Groups	5-14
Programming ARS Facility Group Dialing Rules	5-14
Programming Trunk Groups and Nodes for Facility Groups	5-15
Programming ARS Route Groups	5-16
Default Route Groups	5-16
Creating or Deleting ARS Route Groups	5-17
Moving Route Groups in Lists	5-17
Programming ARS Route Group Dial Patterns	5-18
Adding Facility Groups to ARS Route Groups	5-19
Programming Audio for Calls Camped onto this Device for ARS Route Groups	5-20
Emergency Calls	5-21
Home Area Codes	5-22
Toll Strings	5-23
Programming Toll Strings	5-24
Adding or Deleting Toll String Dial Patterns	5-25

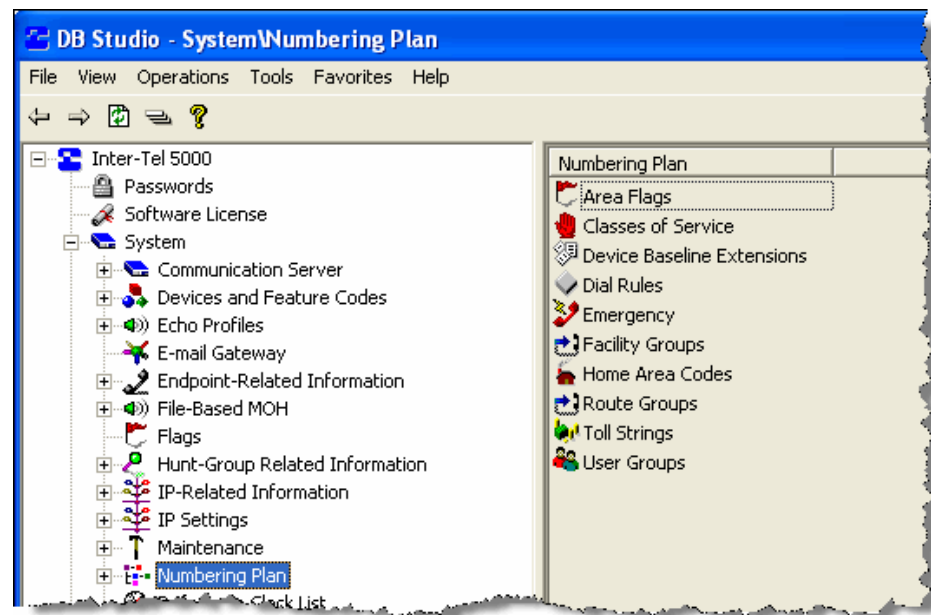
User Groups	5-25
Planning User Groups	5-25
Programming Area Codes	5-26
Programming Allowed Area Codes	5-26
Programming Extended Area Codes	5-26
Programming Restricted Area Codes	5-26
Programming the Area Code Day/Night List	5-27

Introduction

This chapter provides information to program Mitel 5000 Numbering Plan options, as shown in [Figure 5-1](#). The system Numbering Plan determines how the system manages outgoing calls. Numbering Plan programming options include the following:

- “Area Flags” on [page 5-4](#)
- “Classes of Service (COS)” on [page 5-5](#)
- “Device Baseline Extensions” on [page 5-9](#)
- “Automatic Route Selection (ARS)” on [page 5-10](#)
- “Emergency Calls” on [page 5-21](#)
- “Home Area Codes” on [page 5-22](#)
- “Toll Strings” on [page 5-23](#)
- “User Groups” on [page 5-25](#)

Figure 5-1. *Numbering Plan Options*



Area Flags

U.S. installations only. If your system office codes (digits 4, 5, and 5 in a 10-digit number) and area codes (digits 1, 2, and 3 in a 10-digit number) overlap, or if toll digits are allowed on toll calls or long distance calls, you can change the area and office code flags.

The first two flags from the bulleted list below determine how area and office codes overlap. [Table 5-1](#) shows the difference between the standard North American Numbering Plan (NANP) and each of the overlap flags, which are represented by the following variables:

- N = 2–9
- Z = 0 or 1
- X = 0–9

Table 5-1. *NANP and Overlap Flag Differences*

NANP/Overlap Flag	Area Codes Can Be:	Office Codes Can Be:
NANP	NZX	NXX
Office Codes as Area Codes	NZX or NXX	NXX
Area Codes as Office Codes	NZX	NXX or NZX

The following are system Area Flags used for Numbering Plans:

- **Office Codes Used as Area Codes:** An area code in another location uses an NXX pattern that matches an office code within the system site area code. Because the system cannot differentiate between an office code and an area code when the second digit dialed is 0–9, it will wait for the Interdigit timer to expire or another digit to be dialed before assuming that dialing is completed.
- **Area Codes Used as Office Codes:** One or more office codes within the system site area code use an NZX pattern that is the same as an area code in another area. Because area codes do not resemble office codes (NXX), end-of-dialing detection is not affected by this flag.
- **Local 7/10 Digit Dialing:** When this flag is enabled, outgoing calls are identified as having reached the end of dialing if the first digits are not a toll field, equal access field, operator access field, or a local area code. This function speeds up placement of local seven-digit calls in an area where some local calls require 10 digits.
- **Toll Digit Allowed On Toll Local Calls:** This option applies only if the area and office codes overlap. Callers in the site area code usually dial a 1 when placing a call within the local area code(s).
- **Toll Digit Required On Toll Long Distance Calls:** This option applies only if the area and office codes overlap. Callers in the site area code must dial a 1 when placing a call outside of the local area code(s).

To enable or disable a Numbering Plan flag:

1. Select System – Numbering Plan – Area Flags – *<flag>*.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Click out of the field or press **ENTER** to save the change.

Classes of Service (COS)

Class of Service (COS) is used for toll restriction, which prevents system users from placing outgoing calls. COS designations (01–09 or 01–07) have default values and COS designations. COS designations 10–16 or 08–16 are blank. Classes of service 02–16 have programmable dialing patterns, and all have programmable day and night lists of devices.

Exact (complete) pattern matches with classes of service marked as "allowed" always override exact (complete) pattern matches with classes of service marked as "denied." Also, partial (incomplete) pattern matches with classes of service marked as "allowed" always override partial (incomplete) pattern matches with classes of service marked as "denied." The only time a pattern in a denied class of service overrides a pattern in an allowed class of service is when the match with the denied pattern is exact (complete) and the match with the allowed pattern is

COS for U.S. Systems

The following are COS designations for U.S. systems (for European systems, see [page 5-6](#)):

- **COS 01 – ARS Only:** *(This is an endpoint COS only. It is not used for trunk groups.)* When enabled, users must use Automatic Route Selection (ARS) to place calls. Users hear reorder tones when attempting to place a call using any other method. A restricted user can still select individual trunks if the trunks are designated as "exempt from ARS Only" (see [page 8-17](#)), were transferred, were placed on hold, or are recalling or ringing. Trunk restriction determines which trunks in the ARS route group can be selected by the endpoint or voice processing application.
- **COS 02 – Deny Area/Office:** This restriction is divided into eight user groups (see [page 5-25](#)) to allow the use of varying area and office code restriction tables. This reduces restrictions for some of the endpoints, voice processing applications, or trunk groups while increasing restrictions for others. Each endpoint, application, and trunk group is assigned a day mode and a night mode user group. Within each user group, you can designate area codes as restricted, allowed, or extended. Restricting an area code prevents users from placing calls to that area code. Allowing an area code allows all office codes within that area code. You can designate an area code as extended to determine which office codes (up to 800) are allowed or restricted within that area code. For each user group, you can mark up to 800 area codes as allowed or restricted in the database list, and up to six area codes can be marked as extended.
- **COS 03 – Deny Operator:** Calls to numbers that match the dial patterns for this class of service (defaults to [Q]RN+, [Q]R0, and [Q]RE) are restricted, unless the number also matches a dial pattern in an "allowed" class of service that is assigned to the endpoint, voice processing application, or trunk group.
- **COS 04 – Deny Toll Access:** Calls to numbers that match the dial patterns for this class of service (defaults to [Q]TN+ and [Q]TE) are restricted, unless the number also matches a dial pattern in an "allowed" class of service that is assigned to the endpoint, voice processing application, or trunk group.
- **COS 05 – Deny International:** Calls to numbers that match the dial patterns for this class of service (defaults to [Q]I+) are restricted, unless the number also matches a dial pattern in an "allowed" class of service that is assigned to the endpoint, voice processing application, or trunk group.
- **COS 06 – Deny Equal Access:** Calls to numbers that match the dial patterns for this class of service (defaults to Q+) are restricted, unless the number also matches a dial pattern in an "allowed" class of service that is assigned to the endpoint, voice processing application, or trunk group.
- **COS 07 – Deny Local Calls:** Calls to numbers that match the dial patterns for this class of service (defaults to N+) are restricted, unless the number also matches a dial pattern in an "allowed" class of service that is assigned to the endpoint, voice processing application, or trunk group.

- **COS 08 – Denied Numbers:** Calls to numbers that match the dial patterns for this class of service (defaults to 1900NXXXXXX+ and 976XXXX+) are restricted, unless the number also matches a dial pattern in an “allowed” class of service that is assigned to the endpoint, voice processing application, or trunk group being used. Calls are only restricted if the dialed patterns match the denied pattern exactly and that is the only class of service you have. Allowed numbers (as follows) always override denied patterns, even if the numbers are similar.
- **COS 09 – Allowed Numbers:** Calls to numbers that match with the dial patterns for this class of service, defaults to 1(800, 888, 877, 866, 855, 844, 833, and 822)NXXXXXX+, are allowed, even if number also matches a dial pattern in a restricted class of service that is assigned to the endpoint, voice processing application, or trunk group being used.

COS for European Systems

The following are COS designations for European systems (for U.S. systems, see [page 5-5](#)):

- **COS 01 – ARS Only:** *(This is an endpoint COS only. It is not used for trunk groups.)* Calls can only be placed using the Automatic Route Selection (ARS) feature when this restriction is assigned. The user will hear reorder tones when attempting to place a call using any other method. A restricted user can still select individual trunks if the trunks are designated as “exempt from ARS Only” (see “[Toll Restrictions](#)” on [page 8-16](#)), were transferred, were placed on hold, or are recalling or ringing. Trunk restriction determines which trunks in the ARS route group can be selected by the endpoint or Voice Processing application.
- **COS 02 – Deny Operator:** Calls to numbers that match the dial patterns for this class of service (defaults to R+) are restricted, unless the number also matches a dial pattern in an “allowed” class of service that is assigned to the endpoint, voice processing application, or trunk group being used.
- **COS 03 – Deny Toll Access:** Calls to numbers that match the dial patterns for this class of service (defaults to TN+, TE, 010+, and T1+) are restricted, unless the number also matches a dial pattern in an “allowed” class of service that is assigned to the endpoint, voice processing application, or trunk group being used.
- **COS 04 – Deny International:** Calls to numbers that match the dial patterns for this class of service (defaults to I+) are restricted, unless the number also matches a dial pattern in an “allowed” class of service that is assigned to the endpoint, voice processing application, or trunk group being used.
- **COS 05 – Deny Local Calls:** Calls to numbers that match the dial patterns for this class of service (defaults to N+) are restricted, unless the number also matches a dial pattern in an “allowed” class of service that is assigned to the endpoint, voice processing application, or trunk group being used.
- **COS 06 – Denied Numbers:** Calls to numbers that match the dial patterns for this class of service (defaults to 0891+ and 0898+) are restricted, unless the number also matches a dial pattern in an “allowed” class of service that is assigned to the endpoint, voice processing application, or trunk group being used. Calls are only restricted if the dialed patterns match the denied pattern exactly and that is the only class of service you have. Allowed numbers (as follows) always override denied patterns, even if the numbers are similar.
- **COS 07 – Allowed Numbers:** Calls to numbers that match with the dial patterns for this class of service, defaults to 0345+, 0500+, 0645+, and 0800+, are allowed, even if number also matches a dial pattern in a restricted class of service that is assigned to the endpoint, voice processing application, or trunk group being used.

Programming COS Options

Program the COS options as described in the following sections.

Changing or Adding COS Descriptions

You can change or add COS descriptions.

To change or add a COS description:

1. Select System – Numbering Plan – Classes of Service– **<class of service>**.
2. Select the current description, and then type the new description in the box.
3. Click out of the field or press **ENTER** to save the change.

Adding Devices to COS Day and Night Lists

To add a device to the COS Day or Night list of devices:

1. Select System – Numbering Plan – **Classes of Service**.
2. Double-click the COS designation.
3. Double-click either **Day** or **Night**.
4. Right-click anywhere in the right pane, and then click **Add To Day** (or **Night**) **List**. A window appears prompting for the device type to include.
5. Select the device types (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
6. Select the appropriate items, and then select **Add Items**. When you have added all the devices, click **Finish**. The selections appear in the list. To view programming options, double-click the extension number.

To delete a device from the COS Day or Night list of devices:

Select the device, right-click, and then select **Remove Selected Items**.

Defining COS Dialing Patterns

(COS 03–16 only). You can define COS dialing patterns.

To add a dialing pattern to the class of service:

1. Select System – Numbering Plan – **Classes of Service**.
2. Double-click the COS designation.
3. Double-click **Dialing Patterns** to view the current list.
4. Do one of the following:

To add a dialing pattern to the bottom of the list:

- a. Do not select any existing patterns.
- b. Right-click anywhere in the right pane, and then select **Add To List**. A blank pattern appears at the bottom of the list.

To add to the list above an existing device:

- a. Select the device below the location where you want the new entry.
- b. Right-click and select **Add To List**. A blank pattern appears above the pattern you selected.

To delete a COS dial pattern:

Select the dialing pattern, right-click, and then select **Remove Selected Items**. (You can use the SHIFT or CTRL key to select more than one item.)

To move a pattern to another location in the list:

Do one of the following:

- Drag and drop the dial pattern to the new position
- Select the dial pattern to move and press **CTRL** + the up/down arrow to move the dial pattern up or down in the list.

Programming Dialing Pattern Digits

To program dialing pattern digits:

1. Select System – Numbering Plan – **Classes of Service**.
2. Double-click the COS designation.
3. Double-click **Dialing Patterns** to view the current list.
4. In the **Dialing Pattern** column, type the new digits in the box.
5. Click out of the field or press **ENTER** to save the change.

Allowing or Restricting Dialing Patterns

If you want the dialing patterns to be “allowed,” enable this option. If you want the dialing patterns to be “restricted,” disable the option.

To allow or restrict a dialing pattern:

1. Select System – Numbering Plan – **Classes of Service**.
2. Double-click the COS designation.
3. Select **Allow Dial Patterns**.
4. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
5. Click out of the field or press **ENTER** to save the change.

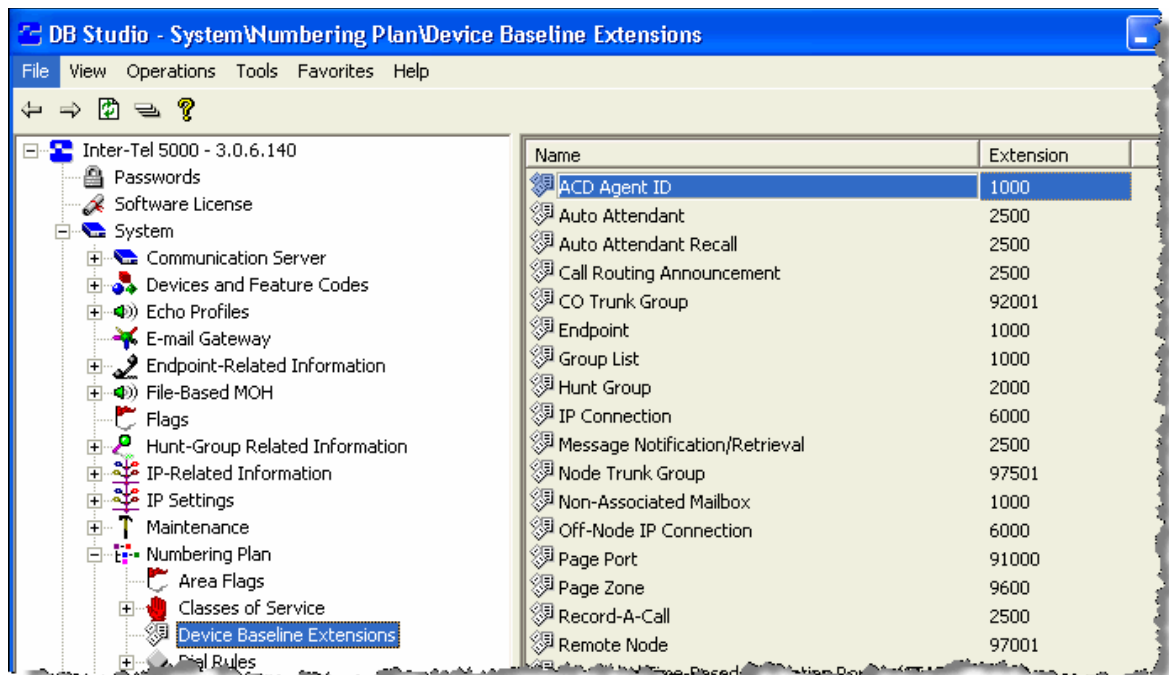
Device Baseline Extensions

Device Baseline Extensions define the recommended starting extension numbers for new system devices. See [Figure 5-2](#).

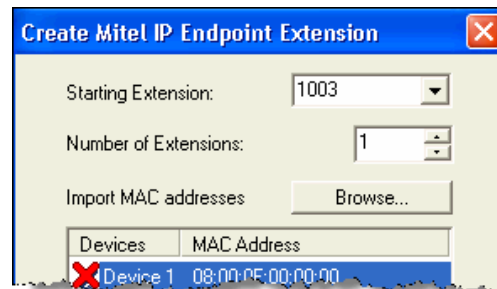
NOTE

To support the NuPoint Messenger voice processing system, Device Baseline Extensions include new Session Initiation Protocol (SIP) options. For more information about NuPoint Messenger, see [page 11-4](#).

Figure 5-2. Device Baseline Extensions



When you add a system device, the system checks the Device Baseline Extension list for the starting extension, as shown in the following example.



In this example, the Device Baseline Extension for an endpoint is 1000. However, extensions 1000 and 1001 were previously assigned, so the system shows the first available extension, extension 1003, in the Starting Extension box. The number of digits is maintained. That is, if the Device Baseline Extension were 10000 instead, the system would show the first available extension after 10000. Note that wildcard extensions (for example, 12XXX) are not valid.

To change a Device Baseline Extension:

1. Select **System – Numbering Plan – Device Baseline Extensions**. A list of the system Device Baseline Extensions appear in the right pane.
2. In the **Extension** column, select the current extension, and then type the new extension number in the box.
3. Click out of the field or press **ENTER** to save the change.

Automatic Route Selection (ARS)

Each node has its own Automatic Route Selection (ARS) programming, which the system uses to select the least expensive route for outgoing calls. Because users do not have direct access to trunks on other nodes, ARS is the only way users can place calls to trunks on other nodes.

ARS calls are limited to one “hop” to another node. For example, if the system routes an outgoing call to another node, the other node cannot route the outgoing call to any other node. This prevents the possibility of an infinite loop when the system searches for a node to route the outgoing call.

For a full description of ARS, refer to the “System Features” chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

Make sure the endpoints that use ARS have outgoing access for the trunk groups and nodes. For more information about trunk group programming, see “Programming CO Trunk Group Options” on [page 8-10](#). For more information about node trunk group programming, see “Viewing or Changing Node Trunk Group Information” on [page 8-28](#).

You program ARS using route groups and facility groups with dialing rules:

Route Groups: A route group contains dialing patterns and facility groups.

- The dialing patterns are used to determine the calls that will be routed through the route group. For example, the default dial pattern for Route Group 1 is N+, any number of digits beginning with digit 2–9 for the U.S. (digit 2–9, 345+, 0500+, 0645+, and 0800+ for Europe). If a number is dialed that begins with 1, it will not be routed through this route group.
- Each route group has an ordered list of facility groups that contain lists of local trunk groups and/or nodes. There can be 100 facility groups in the system. You should program facility groups so that the least-expensive route is checked and, if available, is selected first. If the least-expensive facility group is not available the system checks the other groups in the list until it finds an available trunk.

Facility Groups: A facility group contains trunk group or node lists and dial rules.

- The list can include local trunk groups or nodes. They cannot contain node trunk groups.
- The dial rules tell the system what to dial. The system can have up to 32 dial rules, 26 of which are programmable. Each facility group can use up to 32 dial rules. For example, if the selected route group requires that the number contain “1” but no area code (national dialing in Europe), the dial rules include the 1 and drop the area code (national dialing). The modified number can contain up to 32 digits. (If SMDR is enabled, the modified number, not the digits dialed, will appear in the SMDR call record.) When programming ARS, you can use preset dial rules or create new dial rules that add up to 16 digits each. For more information about Dial Rules, see “Programming ARS Dial Rules” on [page 5-12](#).

The following sections detail ARS programming.

- “Planning ARS Requirements” on [page 5-11](#)
- “Programming ARS Dial Rules” on [page 5-12](#)
- “Programming ARS Facility Groups” on [page 5-13](#)
- “Programming ARS Route Groups” on [page 5-16](#)

Planning ARS Requirements

The first step of implementing ARS for your system is to determine your requirements.

To determine your ARS requirements:

1. Determine the types of calls that system users will make (for example, local, long distance, international). Where will the call destinations be? You need a route group and a facility group for each type of call.
2. Determine the dialing patterns for each type of call. For example, local calls begin with any digit 2–9 (but **not** a toll digit) and operator assisted calls begin with 0 (1XX in Europe). These are the dialing patterns that tell the system which route group to select.
3. Determine the best routes for each type of call based on where the system is installed.

Examples:

- *U.S. systems:* What are the best routes for each type of call? If you have nodes in Phoenix and Los Angeles, would it be better to route calls from Phoenix to Southern California through a node or over your long distance service? This will determine the trunk groups and nodes included in each facility group.
 - *European systems:* What are the best routes for each type of call? If you have nodes in London and Kettering, would it be better to route calls from London to Glasgow through a node or over your long distance service? This will determine the trunk groups and nodes included in each facility group.
4. Determine the facility group order. That is, determine the trunks on this node or other nodes that would be the best route for each type of call.
 5. Determine facility groups dial rules. That is, determine what special characters, if any, need to be added or removed from the dialed number when calls are placed? Determine this for each trunk you are using.

Examples:

- *U.S. systems:* If a caller in Phoenix dials 1-714-XXX-XXXX, the system must remove the toll digit and possibly the area code if the call is sent out over local trunks on the Los Angeles node. However, if the call is routed through the long distance provider in Phoenix, you probably need to include (echo) the toll and area code digits or even add other digits as required by the long distance service.
- *European systems:* If a caller in London dials 020-8335XXX, the system must remove the toll digit and possibly the national dialing code if the call is sent out over local trunks on the Kettering node. However, if the call is routed through the long distance provider in London, you will probably need to include (echo) the toll and national dialing code digits or even add other digits as required by the long distance service.

Programming ARS Dial Rules

After you determine the ARS requirements for your organization (see [page 5-11](#)), program the dial rules. Each facility group (see [page 5-13](#)) includes dial rules that determines system dialing. For example, if the selected facility group requires that the number contain the digit “1” but no area code (national dialing in Europe), the dial rules include (echo) the toll field, but would not echo the area code. When programming ARS, you can use preset dial rules or create new dial rules. The system can have up to 32 dial rules, 26 of which are programmable. The following are the default dial rules:

U.S. Systems:

- **Dial Rule 1 – ECHO Equal Access:** Includes the equal access digits (wildcard Q, which defaults to 10XXX and 101XXX) in the number, if dialed.
- **Dial Rule 2 – ECHO Toll Field:** Includes the toll field in the number, if dialed.
- **Dial Rule 3 – ECHO 3 Digits After Toll Field:** Includes the three digits after the toll field in the number. These digits are usually the area code.
- **Dial Rule 4 – ECHO Local Address:** Allows ARS to dial the rest of the digits that were dialed by the endpoint user.
- **Dial Rule 5 – ECHO Account Code:** Causes the system to dial the account code that is associated with the call, if available before end of dialing. The account code can be entered using any of the account code types, including All Calls Following, as long as the system receives the account code before end of dialing.
- **Dial Rule 6 – ECHO Extension Number:** Requires the system to include the extension number of the endpoint being used to place the call.
- **Dial Rule 7 – ADD #:** Adds a pound/hash (#) to the dialed number. This dial rule is programmable.

European Systems:

- **Dial Rule 1 – ECHO Toll Field:** Includes the toll field in the number, if dialed.
- **Dial Rule 2 – ECHO Local Address:** Allows ARS to dial the rest of the digits that were dialed by the endpoint user.
- **Dial Rule 3 – ECHO Extension Number:** Tells the system to include the last three digits of the extension number of the endpoint being used to place the call.
- **Dial Rule 4 – ECHO Account Code:** Causes the system to dial the last three digits of account code that is associated with the call, if available, before end of dialing. The account code can be entered using any of the account code types, including All Calls Following, as long as the system receives the account code before end of dialing.
- **Dial Rule 5 – ECHO Serial Number:** Tells the system to dial the system-assigned serial number of an ARS call. The serial number range is 000–998, excluding 112. The serial number can be reset in dial rule programming.
- **Dial Rule 6 – ADD #:** Adds a hash (#) to the dialed number. This dial rule is programmable. Dial Rules 3 (echo extension), 4 (echo account code), and 5 (echo serial number) will *always* come after Dial Rules 1 and 2. If 3, 4, or 5 precedes Dial Rules 1 or 2, the SMDR Call Type and Call Cost will be affected.

To program ARS dial rules:

NOTE You cannot edit the dial rule description (Dial Rule field).

1. Select System – Numbering Plan – **Dial Rules**. The list of rules 1–32 is shown in the right pane. You can program rules 7–32, allowing you to add digits to a dialed number.
2. In the **Digits** column, type the digits for the dial rule. Dial rules can contain any digit (0–9, *, #) hookflashes, and pauses. The number can have up to 32 digits.
3. *If you are programming dial rules for a U.S. system, go to [step 5](#).*
4. *If you are programming dial rules for a European system, complete the following:*
 - a. *(For European systems only).* In the **Hidden** column, enable or disable the Hidden flag to determine if the dial rules will be hidden. It is set to **No** by default.
 - b. *(For European systems only).* In the **Absorbed** column, enable or disable the Absorbed flag to determine if the dial rules will be hidden. It is set to **Yes** by default.
 - c. *(For European systems only).* In the **ARS Serial Number** column, enter the serial number (000-998, excluding 112) that you are using. This is only programmable for Dial Rule 5 – ECHO Serial Number.
5. Click out of the field or press **ENTER** or to save the change.

Programming ARS Facility Groups

Facility groups determine the trunk groups that will route calls and the required dial rules. All facility groups are programmable. The default facility group values are as follows.

U.S. systems:

- **Local (P1500):** Uses Trunk Group 1 and Dial Rules 3 and 4.
- **Toll Local (P1501):** Uses Trunk Group 1 and Dial Rules 2 and 4.
- **Toll Long Distance (P1502):** Uses Trunk Group 1 and Dial Rules 1, 2, 3, and 4.
- **Operator (P1503):** Uses Trunk Group 1 and Dial Rules 1, 2, 3, and 4.
- **International Station-to-Station (P1504):** Uses Trunk Group 1 and Dial Rules 1, 2, 3, 4, and 7.
- **International Operator (P1505):** Uses Trunk Group 1 and Dial Rules 1, 2, 3, 4, and 7.

European systems:

- **Local (P1500):** Uses Trunk Group 1 and Dial Rules 1 and 2.
- **National (P1510):** Uses Trunk Group 1 and Dial Rules 1 and 2.
- **Operator (P1512):** Uses Trunk Group 1 and Dial Rules 1 and 2.
- **International (P1513):** uses Trunk Group 1 and Dial Rules 1 and 2.

Each facility group has a list of trunk groups and/or node trunk groups for routing calls. For example, the “Local” facility group would contain trunk groups that include local trunks, but a “Los Angeles” facility group might have node trunk groups that include local trunks on a node in Los Angeles.

You must place facility groups in the in the order that you want them to be selected. Make sure that the facility groups contain the proper type of trunks (local, FX, WATS, long distance, and so on) for the calls that are routed.

Make sure you do the following for each facility group:

- Determine the following facility group options based on your ARS requirements (see [page 5-11](#)).
- Determine what types of calls will be processed and program names for those groups.
- Determine which trunk groups and nodes will be used and program the list. Make sure that the trunk groups and nodes contain the proper type of trunks (local, FX, WATS, long distance, and so on) for the calls that will be routed (use the information from steps 3 and 4 on [page 5-11](#). Also, make sure the endpoints that will be using ARS have outgoing access for the trunk groups and nodes. For more information, see “CO Trunk Groups” on [page 8-7](#) and “Node Trunk Groups” on [page 8-28](#).
- Program the list of dialing rules so that the outgoing numbers include all of the necessary digits. See [page 5-14](#).

Creating and Deleting Facility Groups

To create a facility group:

1. Select System – Numbering Plan – **Facility Groups**.
2. Right-click in any blank area in the right pane.
3. Select **Create Facility Group**.
4. Enter the starting extension number and number of extensions, and then click **OK**. The new facility group appears in the list.
5. If applicable, select the description, and then type the new description in the box.
6. Click out of the field or press **ENTER** to save the change.

To delete a facility group:

Select the facility group, right-click, and then select **Delete**.

Programming ARS Facility Group Dialing Rules

You must assign dial rules to each facility group.

To program ARS facility group options:

1. Select System – **Numbering Plan**.
2. Double-click **Facility Groups**. The current list of facility groups appears in the right pane.
3. Double-click **Dial Rules**. The current list of dial rules, if any, appears. This is an *ordered list*. Place the dial rules in the list in the order you want them to be used.
4. Do one of the following

To add to the bottom of the list:

- a. Do not select any existing dial rules.
- b. Right-click anywhere in the right side pane. An option box appears.

To add to the list above an existing dial rule:

Select the dial rule below the location where you want the new entry, and then right-click. An option box appears.

5. Select **Add To Dial Rules List**. A window appears prompting for the types to include.
6. Select the type (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
7. Select the appropriate items, and then select **Add Items**. When you have added all dial rules, click **Finish**. The selections appear in the list. To view programming options, double-click the dial rule.

To move a dial rule to another location in the list:

Do one of the following:

- Drag and drop the dial rule to the new position
- Select the dial rule to move and press **CTRL** + the up/down arrow to move the dial rule up or down in the list.

To delete one or more dial rule from the list:

Select the dial rule, right-click, and then select **Remove Selected Items**.

Programming Trunk Groups and Nodes for Facility Groups

Trunk groups and nodes must be placed in the list in the order that they should be selected. Make sure that the trunk groups or nodes being used in the facility group contain the proper type of trunks (local, FX, WATS, long distance, and so on) for the calls that will be routed. Trunk group toll restrictions will not apply when ARS is used; only endpoint toll restrictions are checked.

To add the trunk groups and/or nodes to be used by this facility group:

1. Select System – **Numbering Plan – Facility Groups**. The current list of facility groups appears in the right pane.
2. Double-click the facility group.
3. Double-click **Trunk Groups/Nodes**. The current list of trunks/nodes, if any, appears. This is an ordered list. Place the trunks and nodes in the list in the order you want them to be used.
4. Do one of the following

To add to the bottom of the list:

- a. Do not select any existing dial rules.
- b. Right-click anywhere in the right side pane. An option box appears.

To add to the list above an existing dial rule:

Select the trunk group or node below the location where you want the new entry, and then right-click. An option box appears.

5. Select **Add To Trunk Groups/Nodes List**. A window appears prompting for the device types to include.
6. Select **CO Trunk Group** and/or **Remote Node**, and then click **Next**. The list of available devices with details appears. To view devices in a list only, click **List**.
7. Select the appropriate items, and then select **Add Items**. When you have added all dial rules, click **Finish**. The selections appear in the list. To view programming options, double-click the dial rule.

To delete dial rules from the list:

Select the dial rule, right-click, and then select **Remove Selected Items**.

To move a trunk group or node to another location in the list:

Do one of the following:

- Drag and drop the trunk group or node to the new position
- Select the trunk group or node to move and press **CTRL** + the up/down arrow to move the trunk group or node up or down in the list.

To delete a trunk group or node:

Select the trunk group or node, right-click, and then select **Remove Selected Items**.

Programming ARS Route Groups

Make sure you do the following for each ARS route group:

- Determine what types of calls will be processed by each route group and program names for those groups. See step 1 on [page 5-11](#).
- Program dial patterns (see [page 5-12](#)). Dial patterns determine which route group to select, as described in step 2 on [page 5-11](#). When checking the route group, the system looks at the first dial pattern. If it does not match, the system continues to check the other patterns in the route group list. If a match is found, the route group is selected. If not, the next route group is checked.
- Select the facility groups to route the calls. See [page 5-19](#).

Default Route Groups

All route groups are programmable. The Default values are as follows:

U.S. systems:

- **Local (P1000):** Used for all calls that do **not** begin with a toll digit (1) or operator digit (0) and for calls to Emergency Numbers (its default dial pattern is N+). It uses the Local facility group.

NOTICE

When ARS is used to place an emergency call (see [page 5-21](#)), the system uses Route Group 1, even if it contains nodes. This means that the network *can* access a trunk on a node other than the user's node if the user accesses ARS and dials the emergency number. Mitel highly recommends that local trunks be installed and used for emergency number trunk access and that nodes are **not** used in Route Group 1.

- **Toll Local (P1003):** Used for calls with a toll digit (1) and a seven-digit number, and for calls to 1N11 (N=Any digit 2–9). Its default dial patterns are TN11 and TXXXXXXX. It uses the Local Facility Group.
- **Toll Long Distance (P1011):** Processes calls with a toll digit (1) and a 10-digit number. The numbers may also include equal access digits. The default dial pattern is [Q]TNXXXXXX+. This Route Group uses the Toll Long Distance Facility Group.
- **Operator (P1013):** Processes calls that begin with an operator digit (0) but do **not** begin with an international access code (01 or 011). The numbers may also include equal access digits. Its default dial patterns are [Q]RN+, [Q]RR, and [Q]R. This Route Group uses the Operator Facility Group.
- **International Station-to-Station (P1014):** Used for calls that begin with an international endpoint-to-endpoint access code (011) but do **not** begin with the international operator access code (01). The numbers may also include equal access digits. The default dial pattern is [Q]011+. This Route Group uses the International Station Facility Group.
- **International Operator (P1015):** Used for calls that begin with an international operator access code (01). The numbers may also include equal access digits. The default dial pattern is [Q]01+. This Route Group uses the International Operator Facility Group.

European systems:

- **Local (P1000):** Used for all calls that do **not** begin with a toll digit (01 or 0) or operator digit (1XX) and for calls to emergency services.

NOTICE

When ARS is used to place an emergency call (see [page 5-21](#)), the system uses Route Group 1, even if it contains nodes. This means that the network *can* access a trunk on a node other than the user's node if the user accesses ARS and dials the emergency number. Mitel highly recommends that local trunks be installed and used for emergency number trunk access and that nodes are **not** used in Route Group 1.

- **Toll [National] (P1011):** Processes calls with a toll digit (0 or 01). This Route Group uses the National Facility Group.
- **Operator (P1013):** Processes calls that begin with an operator digit (1XX) but do **not** begin with an international access code (00).
- **International (P1014):** Used for calls that begin with an international access code (00). Dial patterns are assigned to the route group in the order they will be used. When checking the route group, the system will look at the first dial pattern. If it does not match, the system will continue checking the other patterns in the route group list. If a match is found, the route group is selected. If not, the next route group is checked.

Creating or Deleting ARS Route Groups

This procedure can be done only if there are fewer than 32 route groups.

To create a route group:

1. Select System – **Numbering Plan**.
2. Double-click **Route Groups**. The current list of facility groups appears in the right pane.
3. Right-click in any open area in the right pane.
4. Select **Create Route Group**. The new route group appears at the bottom of the list.
5. If applicable, change the description of the route group by selecting its current description, and then typing the new information in the box.
6. Press **ENTER** or select another field to save the change.

To delete a route group:

Select the group to be removed, right-click, and then click **Delete**.

Moving Route Groups in Lists

To move a route group to another location in the list:

Do one of the following:

- Drag and drop the route group to the new position.
- Select the route group to move and press **CTRL** + the up/down arrow to move the route group up or down in the list.

Programming ARS Route Group Dial Patterns

The dial pattern tells the system which route group to select. When checking the route group, the system looks at the first dial pattern. If it does not match, the system continues to check the other patterns in the route group list. If a match is found, the route group is selected. If not, the next route group is checked. Only the default route groups have default dial patterns, as summarized in [Table 5-2](#) and [Table 5-3](#). A complete list of special characters and toll strings is shown on [page 5-23](#).

Table 5-2. Route Group Dial Patterns for U.S. Systems

Route Group #	Dial Pattern(s)
Local (1001)	N+
Toll Local (1004)	TN11, TXXXXXXX
Toll Long Distance (1011)	[Q]TNXXXXXX+
Operator (1013)	[Q]RN+, [Q]RR, [Q]R
International Station-to-Station (1014)	[Q]011+
International Operator (1015)	[Q]01+

Table 5-3. Route Group Dial Patterns for European Systems

Route Group #	Dial Pattern(s)
Local (1001)	N+
Toll Local (1004)	TN11, TXXXXXXX
Toll Long Distance (1011)	[Q]TNXXXXXX+
Operator (1013)	[Q]RN+, [Q]RR, [Q]R
International Station-to-Station (1014)	[Q]011+
International Operator (1015)	[Q]01+

To program ARS route group dial pattern:

1. Select System – **Numbering Plan – Route Groups**. The current list of route groups is displayed.
2. Double-click **Dial Patterns**. The current list of dial patterns, if any, appears.
3. Right-click anywhere in the right pane, and then click **Add To Dial Patterns List**. The Batch Create Patterns dialog box appears.
4. Type the digits or special characters that apply to all patterns created in this screen.
5. Select the number of patterns to create.
6. Click **OK**. The new dial patterns are added to the list, each reflecting the specified base pattern. For example, if you entered 1480 as the base pattern and you selected 5 as the number of patterns, five patterns, each with 1480, is added to the list.
7. Press **ENTER** or select another field to save the change.

To move a dial pattern to another location in the list:

Do one of the following:

- Drag and drop the dial pattern to the new position.
- Select the dial pattern to move and press **CTRL** + the up/down arrow to move the dial pattern up or down in the list.

To delete one or more dial pattern from the list:

Select the dial pattern, right-click, and then select **Remove Selected Items**.

Adding Facility Groups to ARS Route Groups

For each route group, select the facility group(s) to be used to route the calls. Facility groups must be placed in the list in the order that you want them to be selected.

To add facility groups that will be used by this route group:

1. Select **System – Numbering Plan – Route Groups**. The current list of route groups is displayed.
2. Double-click **Facility Groups**. The current list of facility groups, if any, appears. This is an *ordered list*. Place the facility groups in the list in the order you want them to be used.
3. Do one of the following

To add to the bottom of the list:

- a. Do not select any existing dial rules.
- b. Right-click anywhere in the right side pane. An option box appears.

To add to the list above an existing dial rule:

Select the facility group below the location where you want the new entry, and then right-click. An option box appears.

4. Select **Add To Facility Groups List**. A window appears prompting for the device type to include.
5. Select **Facility Group**, and then click **Next**. A list of available facility groups with details appears. To view facility groups in a list only, click **List**.
6. Select the facility groups, and then click **Add Items**. If you select more than one, they are placed in the list in numerical order, *not* in the order you select them. To keep the list in the proper order, you may have to add one at a time.
7. When you have added all dial rules, click **Finish**. The selections appear in the list. To view programming options, double-click the dial rule.

To move a facility group to another location in the list:

Do one of the following:

- Drag and drop the facility group to the new position.
- Select the facility group to move and press **CTRL** + the up/down arrow to move the facility group up or down in the list.

To delete a facility group from the list:

Select the facility group, right-click, and then click **Remove Selected Items**.

Programming Audio for Calls Camped onto this Device for ARS Route Groups

Audio for Calls Camped onto this Device defines the audio that a caller hears when camped-on to the route group. For more information about audio settings, see [page 7-65](#).

To program the Audio for Calls Camped onto this Device option:

1. Select System – Numbering Plan – Route Groups.
2. Double-click the route group.
3. Select **Audio for Calls Camped onto this Device**.
4. In the Value column, select the option from the list.
5. Click out of the field or press **ENTER** to save the change.

Emergency Calls

The Numbering Plan Emergency option is where you program the emergency numbers that the system uses when users enter the Emergency Call feature code (for example, 911 in the U.S.).

WARNING

Possible Delay in Local Emergency Response to Remote Sites.

IP and SIP endpoint users should be alerted to the following hazardous situations:

- If an Emergency Call phone number is dialed from an IP or Session Initiation Protocol (SIP) endpoint located at a remote site that is not equipped with a correctly configured gateway, the call will be placed from the location where system chassis is installed rather than from the location where the emergency call is made.

In this situation, emergency responders may be dispatched to the wrong location. To minimize the risk of remote site users misdirecting emergency responders, Mitel recommends regular testing of MGCP/SIP gateway trunks for dial tone.

- If uninterruptible power supply (UPS) protection has not been installed as part of the Mitel 5000 system, IP and SIP endpoints will **not** operate when electrical power fails either at remote sites or at the main system location.

To place calls during a power failure in this situation, IP and SIP endpoint users can only use a single line endpoint connected to one of the power failure bypass circuits built into the system chassis. If an endpoint connected to a power failure bypass circuit is not available, users should make emergency calls **from a local phone not connected to the system**. For details about the Power Failure Bypass feature, refer to the “Installation” chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

NOTICE

It is the responsibility of the organization and persons performing the installation and maintenance of Mitel Advanced Communications Platforms to know and comply with all regulations required for ensuring Emergency Outgoing Access at the location of both the main system and any remote communication endpoints. Remote IP and SIP endpoints may require gateway access to nearby emergency responders. Emergency Call phone numbers include:

- 911, the default for Mitel systems located in the U.S.
- 999, the default for Mitel systems located in the European market and used primarily in the U.K.
- If applicable, 112, an emergency number used widely in Europe outside of the U.K.

Any emergency number, such as for a police or fire station, that is appropriate for the location of the main system and/or remote endpoints.

Emergency calls, by default, use the first local trunk group and are not sent through other nodes using node trunk groups. However, when ARS is used to place an emergency call, Route Group 1 is used even if it contains nodes. This means that the network *can* access a trunk on a node other than the user’s node if the user accesses ARS and dials the emergency number. **Mitel highly recommends that local trunks be installed and used for emergency number trunk access and that nodes are not used in Route Group 1.** When a user places an emergency call, every administrator in the network receives an emergency alarm.

You can store up to 10 emergency numbers. For more information about the emergency call feature, refer to the “System Features” chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

To program or change emergency numbers:

1. Select System – Numbering Plan – **Emergency**.
2. Double-click **Emergency Numbers**.
3. Select the current value or blank field of the number you want to program.
4. Type the number, up to 48 digits, in the box. Only the first emergency number has a default value (911 in the U.S. or 999 in the European market).
5. Click out of the field or press **ENTER** to save the change.

Home Area Codes

U.S. installations only. The database requires a “home” area code for identifying local calls. It also allows up to 15 additional (codes 2–15) home area codes. The system refers to these area codes for toll restriction and call cost.

NOTE

The first area code is an area code that is always stripped from the dialing number. Other home area codes serve to identify local calls, but are still dialed. If local 10-digit dialing is always required despite the area codes, do not list an area code in the first home area code. If a return call (callback feature) from voice mail is not working correctly, refer to the Knowledge Base article 1224 for possible solutions. See “Technical Support” on [page 2-2](#).

To program the home area code(s) for the system site:

1. Select System – Numbering Plan – **Home Area Codes**.
2. Select the home area code option (1–16).
3. In the **Digits** column, type the new area code in the box.
4. Click out of the field or press **ENTER** to save the change.

Toll Strings

Toll strings are dialing patterns that are abbreviated to single character “wildcards.” Wildcards are used in COS and ARS programming. Toll strings can contain any digit from 0 through 9 and the keypad special characters # and *. You can also use a variety of characters to represent particular digit strings, hookflashes (recalls in Europe), or special digit strings. Each of the following toll string wildcards can be reprogrammed or renamed for your system.

NOTE

Changing toll string dialing patterns affects all of the other parts of the system where they are used.

Table 5-4 shows the programmable toll string wildcards for U.S. systems.

Table 5-4. *Toll String Wildcards for U.S. systems*

Character	Meaning
S	Any Toll String: Any of the designated patterns can be dialed at that point in the number. In the default state, the dialing patterns for this toll string are “I,” “R,” and “T.”
R	Operator Access: Represents the digit string that is required to call the service provider's operator. In the default state, this dialing pattern is 0.
T	Toll Access: Represents the digit(s) required for using long distance service. In the default state, this dialing string is 1.
I	International: Represents the digits required for international dialing. In the default state, the dialing patterns for this toll string are 011 and 01.
Q	Equal Access: Represents the digits required to select secondary carriers for equal access dialing. In the default state, the dialing patterns for this toll string are 101XXXX, 10NXX, and 100XX.

Table 5-5 shows the programmable toll string wildcards for European systems.

Table 5-5. *Toll String Wildcards for European Systems*

Character	Meaning
S	Any Toll String: Any of the designated patterns can be dialed at that point in the number. (In the default state, the dialing patterns for this toll string are “I,” “R,” and “T.”)
R	Operator Access: Represents the digit string that is required to call the network provider's operator. (In the default state, this dialing pattern is 1XX.)
T	Toll Access: Represents the digit(s) required for using long distance service. (In the default state, this dialing strings are 0 and 01.)
I	International: Represents the digits required for international dialing. (In the default state, the dialing pattern for this toll string is 00.)

Table 5-6 shows the special characters that may be used when specifying dialing patterns. These characters are **not** programmable.

Table 5-6. *Special Characters for Dialing Patterns*

Character	Meaning
X	Any digit 0–9
A	Any keypad entry (0–9, #, *)
N	Any digit 2–9
Z	Any digit 0 or 1
B	# or *
H	A hookflash (recall)
E	End of dialing; the pattern will not match if any other digits are dialed beyond this point
+	Any additional dialing will be accepted, from that point in the string, with no further checking for a match. This also means that no further dialing is required beyond this point.
[x]	Indicates an optional pattern within another pattern. For example, with a U.S. system, the International Access character (I) could be defined as 01[1]. (The 01 is followed by an optional 1.)
(x-x)	Indicates a range of digit strings within a pattern. The strings on either side of the hyphen and all strings that fall within the numerical range are included in the match. The strings on either side of the hyphen must be the same length, and the only digits that may appear in the range are 0–9 (#, *, pauses, and flashes are not allowed).
<x>	Indicates repeatable patterns within patterns. In other words, no matter how many times the digit string within the brackets is dialed, the system considers the dialed digits to match the pattern. Note that a repeatable pattern is an entire pattern; no other characters are allowed before or after a repeatable pattern. In other words, a repeatable pattern cannot be included within any other pattern.

Programming Toll Strings

To program toll strings:

1. Select System – Numbering Plan – **Toll Strings**. Toll strings are shown in the right pane.
2. If desired, select the current description, and then enter the new description in the box.
3. Click out of the field or press **ENTER** to save the change.

To move a dial pattern to another location in the list:

Do one of the following:

- Drag and drop the dial pattern to the new position.
- Select the dial pattern to move and press **CTRL** + the up/down arrow to move the dial pattern up or down in the list.

To program the digits for a pattern:

1. Select the current value for the pattern, and then enter the new digits in the box.
2. Click out of the field or press **ENTER** to save the change.

Adding or Deleting Toll String Dial Patterns

To add or delete a toll string dial pattern:

1. Select System – Numbering Plan – **Toll Strings**. Toll strings are shown in the right pane. This is an *ordered list*. Place the devices in the list in the order you want them to be accessed.
2. Do one of the following
To add to the bottom of the list:
 - a. Do not select any existing dial patterns.
 - b. Right-click anywhere in the right pane, and then click **Add to List**.*To add to the list above an dialing pattern:*

Select the device below the location where you want the new entry, right-click, and then click **Add To List**. A blank pattern appears above the pattern you selected.
- 3.

To delete one or more patterns from the list:

1. Double-click the toll string to view the current pattern(s).
2. Select the item(s), right-click, and then select **Remove Selected Items**. (You can press the SHIFT or CTRL keys to select more than one item.)

User Groups

U.S. installations only. This section describes how to program area and office code restriction used for the Deny Area/Office class of service.

You can set up area and office code tables of up to eight user groups to allow different area/office code restriction to be used. This is useful for reducing restrictions for some users while increasing restrictions for others. Each endpoint, application, and trunk group is assigned to a user group.

Planning User Groups

Within each user group, area codes can be restricted, allowed, or extended:

- Restricting an area code prevents users from placing calls to that area code and all of its office codes.
- Allowing an area code allows all office codes within that area code.
- Designating an area code as “extended” allows you to determine which office codes within that area code are allowed or restricted. Up to six extended area codes can be identified within each user group.

To prepare for programming:

1. List the area codes that are allowed, restricted, and extended. Also, list the office codes within the extended area codes that are allowed and restricted.
2. Select System – Numbering Plan – **User Groups** to view a list of the eight user groups. The list shows the user group numbers and their descriptions, if programmed. At this level, you can program the description. To program the area codes, office codes, day list, and night list for a user group, double-click the user group that you want to program.
3. Select the current description, and then enter a name for the user group, up to 20 characters, in the text box.
4. Click out of the field or press **ENTER** to save the change.

Programming Area Codes

You can drag and drop area codes from one location to another. This ensures that each area code is include in a list and none are skipped. To select a series of items, hold down **SHIFT** while selecting the first and last items in the range. To select two or more items that are not consecutive, hold down **CTRL** while selecting the desired items.

Programming Allowed Area Codes

To allow users in the user group access to area codes, the codes must be placed in the Allowed list.

To place an area code in the Allowed list:

1. Select System – Numbering Plan – **User Groups**.
2. Double-click the user group.
3. Double-click **Extended** or **Restricted Area Codes**, and then locate the area code that you want to restrict.
4. Drag and drop that area code to the Allowed area codes directory in the left pane. The next time you open Allowed area codes, the codes will be in the directory.

To remove an area code from the Allowed list:

Move the area code to the Restricted or Extended list in the user group.

Programming Extended Area Codes

You can use up to six extended area codes for each user group, and each of the six can support an individual list of allowed and restricted office codes.

To create an Extended Area Code:

1. Select System – Numbering Plan – **User Groups**.
2. Double-click the user group.
3. Double-click **Allowed** or **Restricted Area Codes**, then locate the area code you want to extend.
4. Drag and drop the area code to the Extended Area Codes directory in the left pane. The next time you open Extended Area Codes, the codes will be in the directory. Office codes can then be programmed as allowed or restricted for that area code by dragging and dropping them into the appropriate categories.

To remove an area code from the Extended list:

Move the area code to the Restricted or Allowed list in this user group.

Programming Restricted Area Codes

You can prevent users from placing calls to certain area codes.

To place area codes in the Restricted list:

1. Select System – Numbering Plan – **User Groups**.
2. Double-click the user group.
3. Double-click **Allowed** or **Extended Area Codes**, and then locate the user group that you want to restrict.
4. Drag and drop the area code to the Restricted Area Codes directory in the left portion of the window. The next time you open Restricted Area codes, the codes will be in the directory. To remove an area code from the Restricted list, move it to the Allowed or Extended list in this user group.

Programming the Area Code Day/Night List

Only extensions with COS 02 can be placed in a user group day or night list.

To program the area code Day or Night list:

Method A

Drag and drop the endpoint to the appropriate list. You can only move from Day list to Day list or Night list to Night list. You cannot move endpoints between Day and Night lists.

Method B

1. Select System – Numbering Plan – **User Groups**.
2. Double-click the user group.
3. Right-click anywhere in the right pane, and then click **Move To List**. A window appears prompting for the device type to include.
4. Select the device types (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
5. Select the appropriate items, and then select **Move Items**. When you have added all the devices, click **Finish**. The selections appear in the list. To view programming options, double-click the extension number.

To delete an item from the list:

You must move the item to another User Group or select Endpoint programming (see “Day and Night Classes of Service” on [page 7-55](#)) and remove COS 2 as a toll restriction.

Trunks and Gateways

Introduction	6-3
Trunk Programming	6-3
Viewing or Programming Trunks	6-4
Changing Trunk Extension Numbers	6-4
Copying Trunks	6-5
Assigning Trunks to CO Trunk Groups	6-5
SIP Gateways	6-6
Understanding NAT Challenges for SIP Devices	6-6
Placing a SIP Gateway Behind a NAT Device	6-7
SIP Trunks	6-8
Creating SIP Trunks	6-8
Programming SIP Trunk Options	6-8
MGCP Gateways, Devices, and Trunks	6-9
Creating an MGCP Gateway and Endpoint	6-9
Adding an MGCP Endpoint	6-10
Changing the MGCP Gateway IP Address	6-10
Trunk Programming Options	6-11
CO Trunk Group	6-13
Service Type	6-13
DTMF Signaling	6-13
Start Type	6-14
DID Disconnect Timer	6-14
Answer Supervision Types	6-15
Connect Trunk-to-Trunk Calls on Polarity Reversal	6-16
Send Digits En Bloc	6-16
Echo Profile	6-16
Connected to CO	6-17
Hybrid Balance	6-17
Measured Echo Return Loss	6-17
Service Prefix Base Number	6-17
Number Of Digits To Receive	6-18
Language	6-18
Network Group	6-18
Reserve IP Resources for Device	6-19
NAT Address Type	6-19
Call Configuration	6-20
CP History	6-20
MGCP Gateway Port	6-20

Communication Timeout	6-21
Manufacturer	6-21
Gateway Name and Endpoint Name	6-21
Associated Gateway	6-21
Call Routing Tables	6-22
Changing Call Routing Table Descriptions	6-23
Programming Call Routing Keys	6-23
Call Routing Patterns	6-24
Editing Call Routing Table Patterns	6-25
Viewing Call Routing Patterns	6-26
Deleting a Pattern	6-26
Adding a Single Pattern	6-26
Copying and Pasting Patterns	6-27
Selecting Batch Create Patterns	6-27
Persistent Music-On-Hold Selection	6-29
Creating Music-On-Hold Profiles	6-30
Assigning Music-On-Hold Profiles to CRTs	6-30
Loop Loss Measurement Test	6-31
Configuring Loop Loss Measurement Test Fields	6-32
Starting a Loop Loss Measurement Test	6-32
Loop Start AC Impedance	6-33
ISDN PRI Two B-Channel Transfer	6-34

Introduction

This chapter describes how to program trunks and gateways for your system. A trunk is a communication line between two switching systems. In this guide, the communication line is either the connection between the Mitel 5000 Public Branch Exchange (PBX) and the Central Office (CO), or it is the communication line between Mitel PBXs.

Your system may use a SIP or Media Gateway Control Protocol (MGCP) gateway, a device that serves as an entrance and exit into a communications network, to connect trunks to the CO or other networked systems. For instructions to program gateways, see “SIP Gateways” on [page 6-6](#) or “MGCP Gateways, Devices, and Trunks” on [page 6-9](#).

Trunks can be any of the following types:

- **Loop start:** Trunks that seize lines by bridging through a resistance of the Tip and Ring wires of the telephone line when the phone goes off-hook. Loop start trunks on a Mitel 5000 loop start module are analog. Loop start trunks on a Mitel 5000 T1 module are digital.
- **Ground start:** Digital trunks on a T1 module in which signaling occurs when one side of the two-wire trunk, typically the “Ring” conductor of the Tip and Ring, is momentarily grounded to get dialtone.
- **T1:** Digital lines with a signaling speed of 1.544 megabits per second (Mbps) pulse code modulation (PCM) that connect the CO to the phone system.
- **T1/Primary Rate Interface (PRI):** A digital transmission system that clusters 24 T1 channels, 23 information-bearing (B) channels and one data (D) channel, for signaling and control.
- **E1/PRI:** European transmission system, similar to T1/PRI, except that E1/PRI trunks have 30 B channels and one D channel (2.048 Mbps per channel).
- **Ear and Mouth (E&M):** A (digital) trunk that uses separate leads, called the “E” and “M” leads, for signaling and supervisory purposes.
- **Direct Inward Dialing (DID) [Direct Dial Inward (DDI)]:** Digital trunks on a T1 module that can dial an extension directly without going through the attendant.
- **Session Initiation Protocol (SIP):** Trunks that allow the system to use Voice-over-IP (VoIP) outside the network by using the same connection as the Internet connection.

Trunk Programming

Trunk programming includes the following:

- “Viewing or Programming Trunks” on [page 6-4](#)
- “Changing Trunk Extension Numbers” on [page 6-4](#)
- “Copying Trunks” on [page 6-5](#)
- “Assigning Trunks to CO Trunk Groups” on [page 6-5](#)

Viewing or Programming Trunks

You can view system trunks and program trunk options.

To view or program a specific trunk:

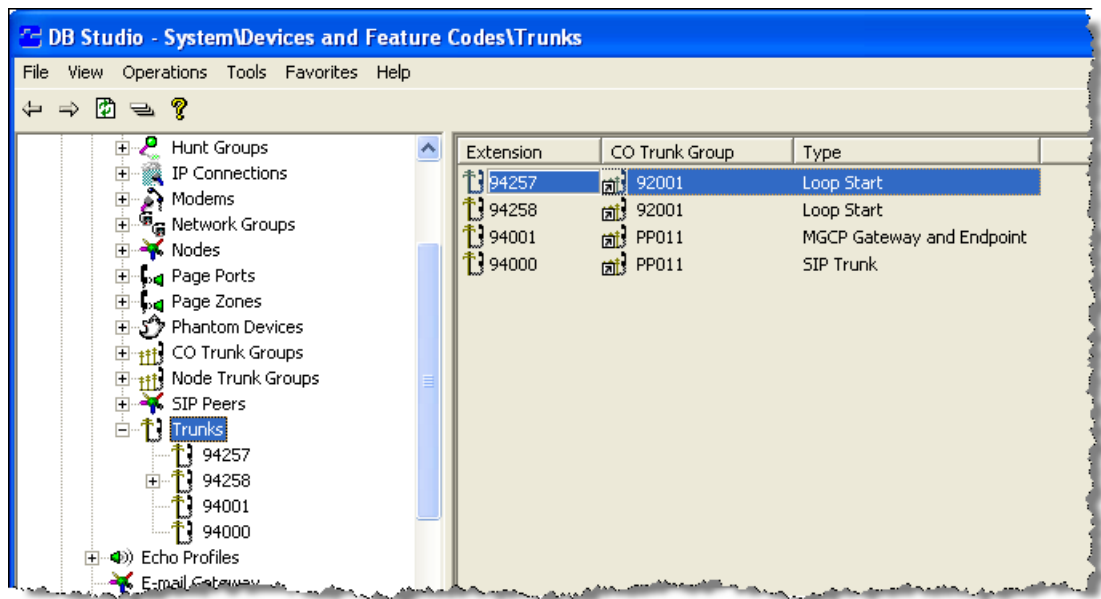
1. Select System – Devices and Feature Codes – **Trunks**.

NOTE

T1 or E1 trunks with a switch type of “Private Networking” or “IP Private Networking” appear in the trunk list, but you cannot change the options.

2. Double-click the trunk number. Trunk options appear in the right pane, as shown in [Figure 6-1](#). To program trunk options, see [page 6-11](#).

Figure 6-1. *Trunks Location*



Changing Trunk Extension Numbers

You can change a single trunk number or use Batch Extension Exchange to change several trunk extension numbers at once.

To change a single trunk extension number:

1. Select System – Devices and Feature Codes – **Trunks**.
2. In the **Extension** column, select the trunk number, and then select the new number from the list.
3. Click out of the field or press **ENTER** to save the change.

To change several trunk extension numbers:

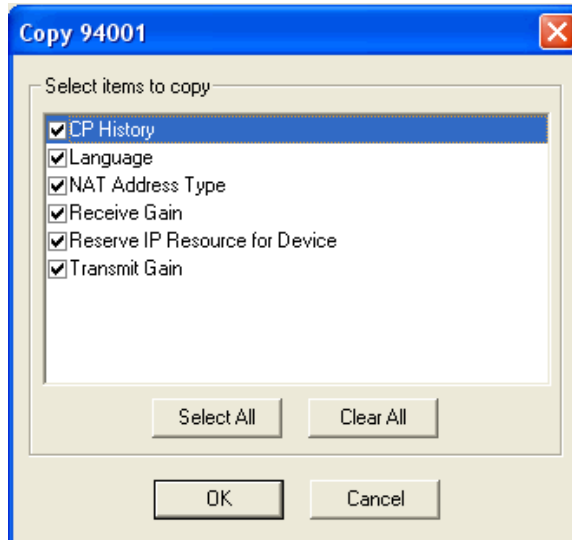
1. Select the trunks you want to change (you can use the SHIFT or CTRL key to select more than one trunk), right-click, and then select **Batch Extension Change**. The Create Extension dialog box appears.
2. Select the number that you want to assign to the first selected trunk (the other trunks will be numbered consecutively after this number).
3. Click **OK**. The trunks are automatically renumbered and resorted.

Copying Trunks

To save time, you can copy a trunk and its settings instead of creating a new one.

To copy a trunk:

1. Right-click the trunk extension, and then select **Copy**.
2. To paste the programming information into another trunk, right-click the trunk where you want the information pasted, then select **Paste**. The Copy <trunk> dialog box appears.



3. Select the attributes, and then click **OK**.

Assigning Trunks to CO Trunk Groups

You can assign individual trunks to CO trunk groups. See “CO Trunk Groups” on [page 8-7](#) for more information about CO trunk groups.

To assign trunks to a CO trunk group:

1. Select System – Devices and Feature Codes – **Trunks**.
2. Double-click the trunk number.
3. Select **CO Trunk Group**.
4. Do one of the following:

Method A

- a. In the **Value** column, select the current value, and then enter the new value in the box.
- b. Click out of the field or press **ENTER**. The Select a Device dialog box appears.
- c. Click **OK**. The new number appears in the field.

Method B

- a. Right-click the current CO Trunk Group value, and then select **Change CO Trunk Group**. A window appears prompting for the device type to include.
- b. Select **CO Trunk Group**, and then click **Next**. CO Trunk Groups with details appear in the right pane. To view them in a list only, click **List**.
- c. Select the trunk group, and then click **Finish**. Trunk groups with details appear in the right pane. You can also move trunks between trunk groups. See “Moving Trunks Between CO Trunk Groups” on [page 8-9](#).

SIP Gateways

NOTICE

SIP trunks and gateways require special configuration settings for emergency calls. For more information, see “Emergency Extensions for IP Devices” on [page 9-37](#).

The system supports SIP trunks to connect to CO. SIP trunks allow the system to communicate with the CO through SIP-enabled gateways. If you are using SIP trunks, at least one SIP gateway must exist at all times, even in a default system, because it follows the model of a CO trunk group.

The Mitel 5000 system currently supports the following SIP gateways:

- AudioCodes™ MP-114 SIP gateway
- Quintum® AFT 400 SIP gateway

To view SIP Gateways and options:

Select System – Trunk-Related Information – **SIP Gateways**.

To view SIP Trunks:

Select System – Trunk-Related Information – **SIP Gateways** – *<gateway>* – **SIP Trunks**.

Understanding NAT Challenges for SIP Devices

A Network Address Translation (NAT) device translates private network IP addresses to one or more public network IP addresses based on NAT translation rules.

NAT devices are installed at the edge of the private network and have internal and external interfaces (and IP addresses). For outgoing IP traffic from the private network to the Internet, NAT translates the source IP address. For incoming IP traffic from the Internet to the private network, NAT translates the destination IP address.

NAT devices provide the following advantages:

- Internal IP addresses are hidden from the open Internet and therefore more secure.
- IP addresses are conserved because they are allocated dynamically when needed.

Despite the advantages of NAT devices, they can cause problems for protocols using Peer-to-Peer technologies like multimedia traffic on VoIP networks using SIP.

Placing a SIP Gateway Behind a NAT Device

Applies only to IP gateway trunks for SIP gateways. If you are using SIP trunks, at least one SIP gateway must exist at all times, even in a default system, because it follows the model of a CO trunk group.

You can place a SIP gateway behind a NAT device. For more information about NAT devices, see “Understanding NAT Challenges for SIP Devices” on [page 6-6](#) and refer to “Appendix B: Network Topology,” in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

To place a SIP gateway behind a NAT device, you must program the following two fields:

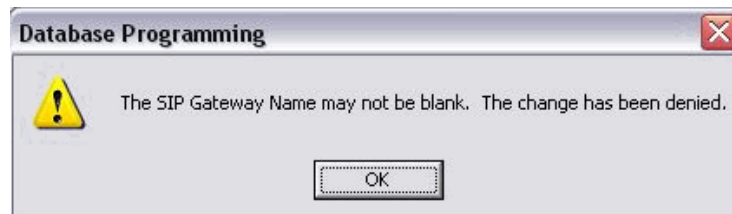
- **System NAT IP Address:** To establish the NAT, or public, IP address.
- **SIP Gateway Name:** To inform the gateway where the SIP messages are originating.

To program the System NAT IP Address:

1. Select System – IP Settings – **System NAT IP Address**.
2. In the **Value** column, type the NAT, or public, IP address that the system has on the NAT side of the firewall. For a description of the field, see [page 9-10](#).

To program SIP Gateway options:

1. Select System – Trunk-Related Information – SIP Gateways – **<gateway>**.
2. Enter the gateway that is programmed on the SIP gateway itself. The default value is DEFAULT. If you attempt to set the SIP Gateway Name to an empty string, the system displays the following error message, and denies the change, as shown in the following illustration.



3. Program the following options:
 - **SIP Trunks:** The SIP gateway where SIP trunks are placed.
 - **IP Address:** The IP address of the SIP gateway.
 - **Listening Port:** The port that the system “listens” to for SIP messages. By default, this port is set to 5060 (standard SIP port).
4. Click out the fields or press **ENTER** to save the changes.

SIP Trunks

SIP trunks allow the system to communicate with the CO through SIP gateways. For more information about SIP gateways, see “SIP Gateways” on [page 6-6](#). SIP trunks:

- Are transparent to the system user because SIP trunks function like any other CO trunk in the system.
- Support transferring trunks, putting trunks on hold, and connecting trunks to conferences similar to other CO trunks in the system.
- Support making and receiving calls by any endpoint.
- Support peer-to-peer audio by IP endpoints.
- Reside in CO trunk groups just like other trunks so that SIP trunk calls can be routed using Automatic Route Selection (ARS).

Creating SIP Trunks

You can also use the Configuration Wizard to create SIP trunks. For more information, refer to the “Installation” chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

To create a SIP trunk:

1. Select System – Devices and Feature Codes – **Trunks**.
2. Right-click in a blank area in the right pane, and then select **Create SIP Trunk**. The Create SIP Extension dialog box appears.
3. Enter the starting extension number and the number of extensions, and then click **OK**. The SIP trunk appears in the list.

Programming SIP Trunk Options

To program SIP trunk options:

1. Select System – Devices and Feature Codes – **Trunks**.
2. Double-click the SIP trunk. SIP trunk options are shown in the right pane.
3. Program the following options:
 - **Call Configuration:** See “Call Configuration” on [page 6-20](#).
 - **CO Trunk Group:** See “CO Trunk Groups” on [page 8-7](#).
 - **Network Group:** See “Network Group” on [page 6-18](#).
 - **SIP Gateway:** See “SIP Gateways” on [page 6-6](#).
 - **CP History:** See “CP History” on [page 6-20](#).
 - **Language:** See “Language” on [page 6-18](#).

MGCP Gateways, Devices, and Trunks

NOTICE

Media Gateway Control Protocol (MGCP) trunks and gateways require special configuration settings for emergency calls. For more information, see “Emergency Extensions for IP Devices” on [page 9-37](#).

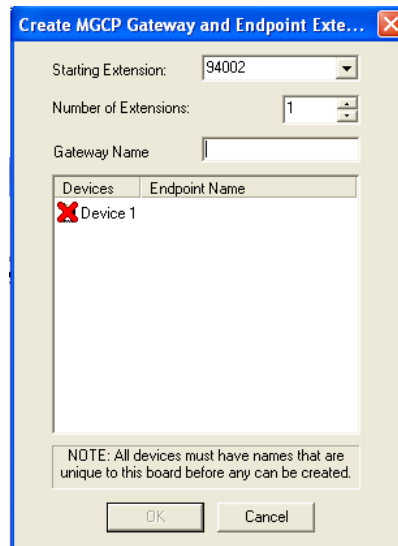
The following sections provide instructions to add and configure MGCP devices. You can also use the Configuration Wizard to add and configure MGCP devices. For more information about the Configuration Wizard, refer to the “Installation” chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

Creating an MGCP Gateway and Endpoint

Because you must assign MGCP endpoints to MGCP gateways when you create new MGCP endpoints, you must create an “MGCP Gateway and Endpoint” before you can add an MGCP endpoint. See “Adding an MGCP Endpoint” on [page 6-10](#).

To create an MGCP gateway and endpoint:

1. Under System – Devices and Feature Codes – **Trunks**, right-click in the right pane.
2. Select **Create MGCP Gateway and Endpoint**. The following dialog box appears.

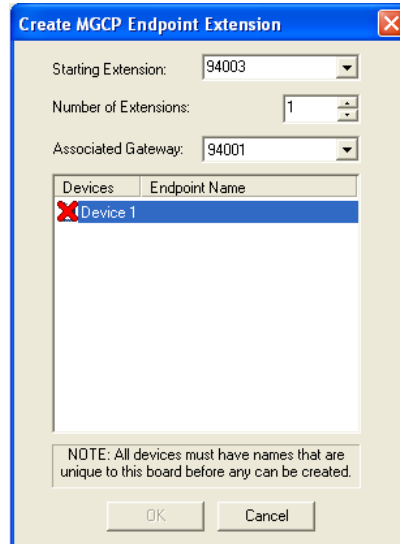


3. In the **Starting Extension** list, either use the default starting extension shown or select a different extension from the list.
4. In the **Number of Extensions** box, enter the number of extensions either by clicking the up and down arrows or by typing the number in the box.
5. In the **Gateway Name** box, type the gateway name.
6. Click any device with a red “X,” and then type a name.
7. Click **OK**.
8. Configure trunk options as necessary. See “Trunk Programming Options” on [page 6-11](#).

Adding an MGCP Endpoint

To create MGCP endpoints:

1. Under System – Devices and Feature Codes – **Trunks**, right-click in the right pane.
2. Select **Create MGCP Endpoint**. The following dialog box appears.



3. In the **Starting Extension** list, either use the default starting extension shown or select a different extension from the list.
4. In the **Number of Extensions** box, enter the number of extensions either by clicking the up and down arrows or by typing the number in the box.
5. In the **Associated Gateway** list, select the MGCP gateway to be assigned to the endpoints.
6. Click any device with a red "X," and then type a name.
7. Click **OK**.
8. Configure trunk options as necessary.

Changing the MGCP Gateway IP Address

Applies only to IP gateway trunks for MGCP gateways. The MGCP Gateway IP Address option identifies the IP address used to access the MGCP gateway.

To enter an IP address:

1. Click the current Value. The Edit MGCP Gateway IP Address dialog box appears.
2. Without including the periods, enter the IP address, and then click **OK**. The default IP address is 192.168.200.201 (entered as 192168200201).

Trunk Programming Options

The options described in this section vary depending on trunk type (see [Table 6-1](#) for available options for each trunk type). Example trunk options are shown in [Figure 6-2](#).

Figure 6-2. Trunk Options (Loop Start Trunk)

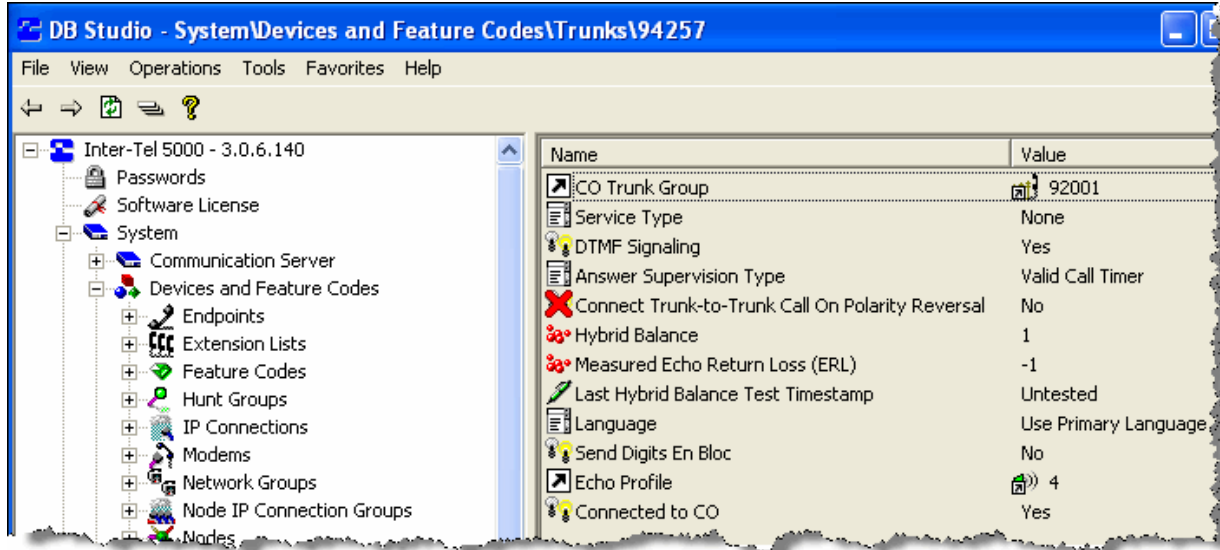


Table 6-1. Trunk Types and Feature Options

Trunk Option	Analog LS (LSM)	Digital LS (T1)	GS (T1)	DID (T1)	B-Channel (T1/PRI or E1/PRI)	E&M (T1)	MGCP Gtwy. and Endpnt.	MGCP Endpnt.	SIP	Page
Answer Supervision Type	✓	✓	✓			✓	✓	✓		6-15
Associated Gateway								✓		6-21
Call Configuration							✓	✓	✓	6-20
CO Trunk Group	✓	✓	✓	✓	✓	✓	✓	✓	✓	6-13
Communication Timeout							✓			6-21
Connect Trunk-to-Trunk Call On Polarity Reversal	✓				✓		✓	✓		6-16
Connected to CO	✓	✓								6-17
CP History									✓	6-20
Disconnect Timer				✓		✓				6-14
DTMF Signaling	✓	✓	✓	✓		✓	✓	✓		6-13
Echo Profile	✓	✓	✓	✓	✓	✓	✓	✓		6-16
Endpoint Name							✓	✓		6-21
Gateway Name							✓			6-21

Chapter 6: Trunks and Gateways

Trunk Programming Options

Table 6-1. *Trunk Types and Feature Options (Continued)*

Trunk Option	Analog LS (LSM)	Digital LS (T1)	GS (T1)	DID (T1)	B-Channel (T1/PRI or E1/PRI)	E&M (T1)	MGCP Gtwy. and Endpnt.	MGCP Endpnt.	SIP	Page
Hybrid Balance	✓	✓					✓	✓		6-17
Language	✓	✓	✓	✓	✓	✓	✓	✓	✓	6-18
Last Hybrid Balance Test Timestamp	✓	✓								6-17
Manufacturer							✓			6-21
Measured Echo Return Loss (ERL)	✓									6-17
MGCP Gateway IP Address							✓			6-10
MGCP Gateway Port							✓			6-20
NAT Address Type							✓	✓	✓	6-19
Network Group							✓	✓	✓	6-18
Number of Digits to Receive				✓		✓				6-18
Reserve IP Resource for Device							✓	✓	✓	6-19
Send Digits En Bloc	✓	✓					✓	✓		6-16
Service (Prefix) Base Number				✓	✓	✓				6-17
Service Type	✓	✓				✓	✓	✓		6-13
SIP Gateway									✓	6-7
Span Echo Profile		✓ ¹	✓ ¹	✓ ¹	✓	✓*				10-5
Start Type				✓		✓				6-14

1. Available for Dual T1/E1/PRI modules only

CO Trunk Group

Program CO trunk group options. For more information, see “Programming CO Trunk Group Options” on [page 8-10](#).

Service Type

You must program each trunk, not the trunk group, to collect digits using Caller ID [CLID], DID [DDI], ANI, DNIS, or DNIS-ANI. If the trunk is programmed to collect digits, but the trunk group does not use call routing tables, the system routes the call based on the trunk group programming and ignores the collected digits. However, the collected digits do appear in SMDR and can be used by the Desktop Interface. If the trunk is not set up to collect digits and the trunk group uses call routing tables, the system uses the call routing destination for “no-digit” calls.

Desktop Interface functionality requires the Desktop Interface software license, part no. 840.0319.

Available service types are determined by the trunk type. Service types are as follows:

- **Loop Start and MGCP Gateway and Endpoint:** *Do not change the Service Type to Caller ID unless you are using IP SLAs.* Loop start trunks can use Caller ID [CLID]. When selected, the Caller ID [CLID] service type option indicates that the associated trunk provides caller identification signals. Because the CO [local exchange] sends the information after the first cycle of ring voltage is applied, selecting this box also prevents the system from signaling an incoming call to the endpoint users until the system has had an opportunity to collect the caller information. If no caller information is collected, the system provides ring signaling on the second ring signal. Caller ID [CLID] uses Caller ID [CLID] receivers.

In Europe, the loop start trunk provides caller identification signals when used with an MGCP gateway.

- **E&M and DID [DDI]:** E&M and DID trunks can use DID, E&M, ANI, or DNIS.
- **Ground Start and B-Channel:** Ground start and B-channel trunks do **not** support any of the caller information service types.

To set the Service Type:

1. Select System – Devices and Feature Codes – Trunks – **<trunk number>**.
2. Select **Service Type**.
3. In the value column, select the service type from the list.
4. Click outside the field or press **ENTER** to save the change.

DTMF Signaling

Does not apply to SIP and B-channel trunks. Other trunks use DTMF signals. Do not disable this flag. It is enabled by default.

NOTE

Enable this option for MGCP trunks; otherwise, the system may receive double digits.

Start Type

Applies only to E&M and DID [DDI] trunks only. E&M and DID trunks perform a “handshake” between the system and the CO [local exchange] to transfer call information. The following are E&M and DID Start Types:

- **Immediate:** The calling system immediately begins sending the dialed digits to the receiving system.
- **Wink:** The systems perform a “handshake” to allow the receiving system to signal that it is ready to receive the digits dialed by the other system. This is the default start type.
- **Delay Dial:** The calling system waits until its E&M Dial Delay timer expires before sending any digits to the receiving system.
- **Dial Tone (E&M trunks only):** The calling system waits until it detects dial tone from the other system before sending digits.

To set the Start Type:

1. Select System – Devices and Feature Codes – Trunks – **<E&M or DID trunk>**.
2. Select **Start Type**.
3. In the **Value** column, select the option from the list.
4. Click out of the field or press **ENTER** to save the change.

DID Disconnect Timer

Applies only to E&M and DID [DDI] trunks only. You can program trunks to use the Disconnect timer to disconnect calls immediately whenever the inside party hangs up on a call. If the Disconnect timer is not enabled, it waits up to two seconds for an on-hook signal from the CO [local exchange].

To set the Disconnect Timer option:

1. Select System – Devices and Feature Codes – Trunks – **<trunk number>**.
2. Select **E&M and DID Disconnect Timer**.
3. In the **Value** column, select either **Disconnect Timer** or **Wait for Remote On-Hook**.
4. Click out of the field or press **ENTER** to save the change.

Answer Supervision Types

Applies to loop start, ground start, and MGCP gateway and endpoint trunks only. The Answer Supervision Type determines whether the system should consider a call valid or disconnected. Available Answer Supervision Types depend on whether you are programming a loop-start or E&M trunk:

For Loop Start, Ground Start, or MGCP Gateway and Endpoint trunks:

- **Polarity Reversal:** A loop reversal must be received to consider the call valid. When the first loop reversal is received, the call is made valid immediately, and the endpoint display begins call cost. When a second loop reversal is received, the system terminates the call. If a second loop reversal is not received, the system does not terminate the call unless the inside party hangs up or loss-of-loop is received from the CO [local exchange].
- **Valid Call Timer:** After the Valid Call Timer expires, the call is validated. All polarity reversals received before and after the Valid Call Timer are ignored.
- **Valid Call Timer with Polarity Reversal:** If a loop reversal is received before the Valid Call Timer expires, the call is made valid immediately, and the endpoint display begins call cost. When a second loop reversal is received, the system terminates the call. If a loop reversal is not received before the Valid Call Timer expires, the call is validated by the timer. If a loop reversal is received after the timer expires, the loop reversal is ignored, but the call cost is reset. If a second loop reversal is then received, the system terminates the call. If a second loop reversal is not received, the system does not terminate the call unless the inside party hangs up or loss-of-loop is received from the CO [local exchange].

For E&M trunks:

- **Use Off-Hook Debounce Timer:** After the Use Off-Hook Debounce Timer expires, the call is validated. All polarity reversals received before and after the Off-Hook Debounce Timer duration are ignored.
- **Use Answer Recognition Timer:** After the Use Answer Recognition Timer expires, the call is validated. All polarity reversals received before and after the Answer Recognition Timer duration are ignored.

To set the Answer Supervision Type:

1. Select System – Devices and Feature Codes – Trunks – **<Loop Start, Ground Start, or MGCP Gateway and Endpoint trunk>**.
2. Select **Answer Supervision Type**.
3. In the **Value** column, select the option from the list.
4. Click out of the field or press **ENTER** to save the change.

Connect Trunk-to-Trunk Calls on Polarity Reversal

Applies to loop start, B-channel, MGCP Gateway and Endpoint, and MGCP Endpoint trunks only.

NOTE

For this feature to work properly, both the incoming (B-channel trunk) and outgoing (non-T1 Loop Start trunk) sides of the trunk-to-trunk call must have this flag enabled (Yes). For non T-1 Loop Start trunks, this flag is available only when the answer supervision is set to "Polarity Reversal" or "Valid Call Timer with Polarity Reversal."

Trunk-to-Trunk Calls on Polarity Reversal settings are as follows:

- **Enabled (Yes):** When an ISDN incoming call is made to a loop start trunk (trunk-to-trunk call), the call is validated when a polarity reversal is received. The Mitel 5000 system connects the voice path to hear progress tones and then sends the ISDN connect message when the loop start polarity reversal is detected.
- **Disabled (No):** When an ISDN incoming call is made to a loop start trunk (trunk-to-trunk call), the call is validated after receiving an end of dialing handshake. After the handshake, the CO [local exchange] may provide progress tones, such as ringback.

To enable or disable Trunk-to-Trunk Calls on Polarity Reversal:

1. Select System – Devices and Feature Codes – Trunks – **<trunk number>**.
2. Select **Connect Trunk-to-Trunk Calls on Polarity Reversal**.
3. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
4. Click out of the field or press **ENTER** to save the change.

Send Digits En Bloc

Applies to loop start trunks and MGCP Gateway and endpoint trunks only. The Send Digits En Bloc option determines how the system sends digits to the trunk. If enabled (set to Yes), the system sends all of the available digits when the system seizes the trunk (for example, when the user accesses ARS). If disabled (set to No), the system sends the digits to the trunk one at a time. By default, this is *disabled*, which is recommended for loop start trunks and MGCP gateways/endpoints.

To enable or disable Sending Digits En Bloc:

1. Select System – Devices and Feature Codes – Trunks – **<Loop Start, MGCP Gateway and Endpoint, or MGCP Endpoint trunk>**.
2. Select **Send Digits En Bloc**.
3. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
4. Click out of the field or press **ENTER** to save the change.

Echo Profile

All system devices are associated with an echo profile. For more information and programming instructions, see "Echo Profiles" on [page 10-5](#).

Connected to CO

Indicates whether or not the trunk is connected to another PBX or the CO. The default setting is “Yes,” because most systems connect trunks to the CO.

To enable the Connected to CO option:

1. Select System – Devices and Feature Codes – Trunks – *<trunk number>*.
2. Select **Connected to CO**.
3. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
4. Click out of the field or press **ENTER** to save the change.

Hybrid Balance

Applies to analog loop start trunks only. The (improved) Hybrid Balance Test automatically measures and determines the best hybrid balance setting for each type of trunk.

You can start an Automatic Hybrid Balance Test on a single trunk or all trunks. For more information, see “Hybrid Balance Test” on [page 16-26](#).

Measured Echo Return Loss

This read-only value is the Finalized Hybrid Balance Test – ERL measured in the most recent Hybrid Balance Test on an analog loop start trunk. This value displays in Message Print output. A red “X” appears on digital loop start trunks. For more information, see “Hybrid Balance Test” on [page 16-26](#).

Service Prefix Base Number

*Applies to DID [DDI] and E&M trunks that are programmed for the DID (DDI for Europe), ANI, DNIS, *DNIS*, and *ANI*DNIS* service types only.* This is the base number for the trunk. If you are using B-channel trunks, the CO [local exchange] sends fewer than 10 digits for the DNIS number on some ISDN calls. When this happens, the system must construct a 10-digit number for the System Open Architecture Interface (OAI) and Desktop Interface features (both of these features require a software license). To construct the number, the system requires a base number for the trunk.

To set the Service Prefix Base Number:

1. Select System – Devices and Feature Codes – Trunks – *<DID or E&M trunk>*.
2. Select **Service Prefix Base Number**.
3. In the **Value** column, select the current value, and then enter the digits in the box (up to 48 digits).
4. Click out of the field or press **ENTER** to save the change.

Number Of Digits To Receive

Applies to DID and E&M trunks that are programmed for the DID [DDI], ANI, and DNIS service types only. This is the number of digits the system uses for directing calls.

To set the Number of Digits to Receive:

1. Select System – Devices and Feature Codes – Trunks – **<trunk number>**.
2. Select **Number of Digits to Receive**.
3. In the **Value** column, type or select the correct amount (1–32) in the box.
4. Click out of the field or press **ENTER** to save the change.

Language

You can select the language used for voice prompts and displays when this trunk is used. Options include Use Primary Language, Use Secondary Language, American English, British English, Japanese, or Spanish.

NOTE	The Japanese language is not supported on Mitel IP endpoints.
-------------	---

To set the language:

1. Select System – Devices and Feature Codes – Trunks – **<trunk number>**.
2. Select **Language**.
3. In the **Value** column, select the language from the list.
4. Click out of the field or press **ENTER** to save the change.

Network Group

Applies to IP gateway trunks for MGCP and SIP gateways and MGCP endpoints only. The Network Group option is required only if you are using peer-to-peer (P2P) audio for the selected MGCP gateway, MGCP endpoint, or SIP gateway. This option is also located under System – Devices and Feature Codes – **Network Groups**. See “Network Groups” on [page 8-52](#).

To assign the gateway or endpoint to a network group:

1. Select System – Devices and Feature Codes – Trunks – **<trunk number>**.
2. Double-click **Network Group**.
3. Double-click the desired Network Group extension, and then add the gateway or endpoint to the IP Trunks list.
4. Click out of the field or press **ENTER** to save the change.

Reserve IP Resources for Device

You can program IP trunks (and IP endpoints) with a dedicated IP resource. When the Reserve IP Resource for Device field is enabled (set to Yes), an IP Resource is reserved for the device. You can also use the Resource Reservation Tool to program this option. See “Resource Reservation Tool” on [page 9-42](#).

NOTE

Mitel recommends that you reserve IP resources for attendants and other high traffic users (for example, call center agents). However, excessive use of reservations degrades the effectiveness of oversubscription by reducing the amount of resources available to be shared.

If a device that has a reserved IP resource goes off-line in Call Processing, the IP resource returns to the shared pool of available IP resources. Although Call Processing makes this adjustment, the database does not change until you delete the device or change this flag.

To reserve or unreserve an IP resource for a particular IP trunk:

1. Select System – Devices and Feature Codes – Trunks – **<trunk number>**.
2. Select the type of IP trunk device, MGCP gateway or SIP trunk.
3. Select **Yes** to reserve a resource for the device, or select **No** to unreserve the resource. The default setting is **No**.
4. Click out of the field or press **ENTER** to save the change.

NAT Address Type

Applies to MGCP Gateway and Endpoint or SIP Gateway trunks only. This option specifies whether to use the Native or NAT IP Address for audio commands. For more information, see “Understanding NAT Challenges for SIP Devices” on [page 6-6](#), and refer to Appendix B: Network Topology, in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000

To set the NAT Address Type:

1. Select System – Devices and Feature Codes – Trunks – **<trunk number>**.
2. Double-click the trunk extension or CO [Local Exchange] trunk group number.
3. Click **NAT Address Type**, and then select either **Native** or **NAT**. The default setting is Native.
4. Click out of the field or press **ENTER** to save the change.

Call Configuration

Applies only to IP gateway trunks for MGCP gateways and endpoints and for SIP gateways. The Call Configuration information is only required if using P2P audio for the selected MGCP gateway, endpoint, or SIP gateway. The Call Configuration defines the settings that the gateways and endpoints use when connected to a call. For more information about Call Configurations, see “IP Call Configurations” on [page 9-24](#).

To assign the IP device to a call configuration:

1. Select System – Devices and Feature Codes – Trunks – **<trunk number>**. (You can also configure this option from System – IP-Related Information – **Call Configurations**.)
2. Double-click **Call Configuration**.
3. Double-click the Call Configuration ID.
4. Double-click **Trunks**.
5. Right-click in the right pane, and then click **Move to Trunks list**. The Move to Trunks List dialog box appears.
6. Select the gateway or endpoint to the IP Trunks list, and then click **Next**.
7. Click **Move Items**, and then click **Finish** to save the change.

To change the call configuration:

1. Right-click the trunk number, and then select **Change Call Configuration**. The Change Call Configuration dialog box appears.
2. Select **Call Configuration**, and then click **Next**. The devices with details appear. To view items in a list only, click **List**.
3. Click **Finish**.

CP History

Applies to SIP trunks only. The CP History is used for diagnostic purposes only. It enables SIP message output in the Call Processing history file. You can use the CP History to trace SIP trunk calls. The system-wide SIP format is set to No Output by default.

To change the CP History setting:

1. Select System – Devices and Feature Codes – Trunks – **<SIP trunk>**.
2. Select **CP History**.
3. In the **Value** column, select the option from the list. The available output options are Headers Only, No History, or Full History. The default setting is Headers Only.
4. Click out of the field or press **ENTER** to save the change.

MGCP Gateway Port

Applies to MGCP gateway trunks only. The MGCP Gateway Port option defines the port number the system uses to access the MGCP gateway.

To change the port number:

1. Select System – Devices and Feature Codes – Trunks – **<MGCP Gateway and Endpoint trunk>**.
2. In the **Value** column, type or select the new port number. The valid port range is 1024–65535; the default is 2427.
3. Click out of the field or press **ENTER** to save the change.

Communication Timeout

Applies to MGCP gateway trunks only. The Communication Timeout option specifies the number of seconds that the gateway waits for an acknowledgement from an associated endpoint before it considers the endpoint offline.

To change the Communication Timeout option:

1. Select System – Devices and Feature Codes – Trunks – **<MGCP Gateway and Endpoint trunk>**.
2. In the **Value** column, select the new value from the list. The valid range is 3–300; the default value is 15.
3. Click out of the field or press **ENTER** to save the change.

Manufacturer

Applies to MGCP gateway trunks only. The Manufacturer option identifies the brand of the MGCP gateway that is connected to the system. The values are None and Audiocodes MP10X, where “X” is a number.

To change the manufacturer/model:

1. Select System – Devices and Feature Codes – Trunks – **<MGCP Gateway and Endpoint trunk>**.
2. In the **Value** column, select either None or Audiocodes MP10X.
3. Click out of the field or press **ENTER** to save the change.

Gateway Name and Endpoint Name

Applies to MGCP gateways and endpoints only. The gateway name and endpoint name are the names that were assigned to the gateway and associated endpoint when the circuits were programmed. If desired, you can change the names here.

To change a name:

1. Select System – Devices and Feature Codes – Trunks – **<trunk number>**.
2. In the **Value** column, click the current value. The Edit Gateway (or Endpoint) Name dialog box appears. Enter a new name, up to 18 characters, that identifies the gateway or endpoint on the network.
3. Click **OK** to save the change.

Associated Gateway

Applies to MGCP endpoints only. The Associated Gateway option displays the MGCP gateway to which the MGCP endpoint is connected. If a gateway was not assigned when the circuit was programmed, this defaults to the first gateway.

To change the associated gateway:

1. Select System – Devices and Feature Codes – Trunks – **<trunk number>**.
2. Right-click the current extension, and then select **Change Associated Gateway**.
3. Select **MGCP Gateway and Endpoint**, and then click **Next**.
4. Select the desired gateway, and then click **Finish**. If you know the trunk extension for the associated gateway, you can click the current value, and then enter the extension.
5. Click out of the field or press **ENTER** to save the change.

Call Routing Tables

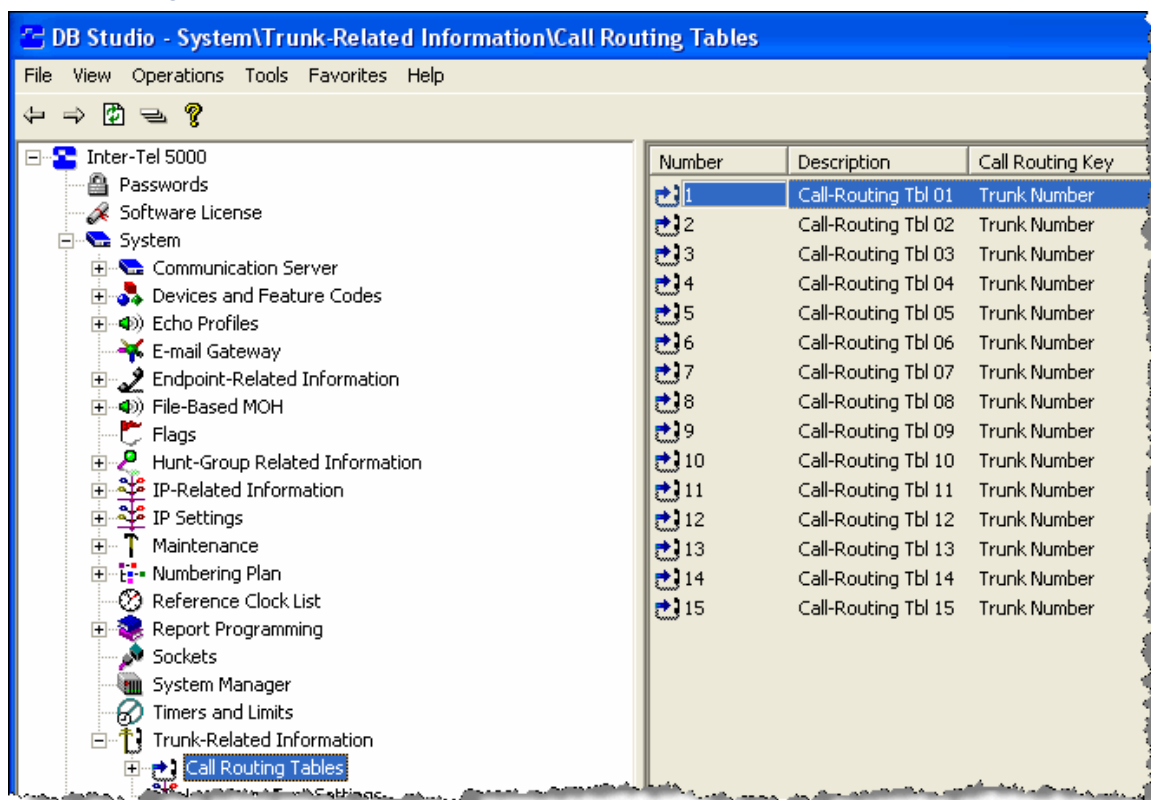
The system uses call routing tables (CRTs) to analyze the digits received from the following:

- **Direct Inward Dialing (DID) [DDI]:** Allows system users to call an system extension without dialing directly into the telephone system.
- **Automatic Number Identification (ANI):** Transmits the billing number, rather than the telephone number, of the calling party.
- **Dialed Number Identification Service (DNIS):** Provides the “800” or “900” number that callers dial to reach system.
- **Caller ID [CLID]:** Transmits callers’ numbers to system equipment during the ringing signal, or when the call is being set up but before the call is answered.

For more information about CRTs, refer to the System Features chapter in the *Mitel 5000 Reference Manual*, part number 580.8007. The system uses these digits to determine which route to use for the call, as determined by the call routing table. The caller information is passed on to the system users’ display along with other call routing table information about the callers (such as location, name, or advertisement information).

Figure 6-3 shows the DB Programming Call Routing location. For a full description of how call routing tables work and sample applications, refer to the System Features chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

Figure 6-3. System Call Routing Tables



Changing Call Routing Table Descriptions

You can change CRT descriptions.

To program Call Routing Descriptions:

1. Select System – Trunk-Related Information – **Call Routing Tables**. The Call Routing Table list (1–15) appears.
2. In the **Description** column, select the current value, and then type the new description in the box.
3. Click out of the field or press **ENTER** to save the change.

Programming Call Routing Keys

Call Routing Keys determine which information the CRT uses to direct the call.

To program Call Routing Keys:

1. Select System – Trunk-Related Information – **Call Routing Tables**. The Call Routing Table list (1–15) appears.
2. Select the current value, and then select one of the following options:
 - **Trunk number**: The system looks for the dialed number provided by DID [DID] or DNIS.
 - **Outside Party Number**: The system checks for the ANI or Caller ID [CLID] information that identifies the source of the call.
3. Click out of the field or press **ENTER** to save the change.

Call Routing Patterns

CRT patterns are listed in the CRT in the order they are checked against the incoming digits received from the trunk interface for the incoming call. When the system finds a match with a pattern, it stops searching through the list and routes the call according to the programming for that pattern. If the call reaches the end of the list without matching any patterns, the call is automatically sent to the primary attendant. Pattern entries can include up to 32 digits. [Table 6-2](#) shows valid characters for CRT entries.

NOTE

To ensure all patterns are included in the CRT, make sure that the last two patterns always include + followed by E. The + pattern allows the system to detect any digits that did not match the other patterns in the list. The E pattern allows the system to detect when no digits are received. This ensures that the call is labeled as either ANY or EMPTY when the call is sent to the primary attendant. These labels notify the attendant that the Telco did not properly route the DNIS digits.

[Table 6-2](#) shows Call Routing Table Pattern characters.

Table 6-2. *Call Routing Table Pattern Characters*

Character	Matches
0–9, *, #	Specific digits
X	Any digit 0–9
A	Any digit 0–9, #, or *
N	Any digit 2–9
Z	Digits 0 or 1
[x]	Optional digits; for example, 2[13]2 matches 22 or 2132.
(x-x)	Range of digits; for example, with a U.S. system, (320–360)XXXX matches any 7-digit number with an office code between 320 and 360, inclusive; with a European system, (200–209)XXXX would catch all 7-digit DDI numbers in the range 200–209.
+	Matches 0 or more digits of any value. A “+” by itself will match any incoming information, including anonymous calls that send no digits.
E	End of dialing; the pattern will not match if any digits are dialed beyond this point. An “E” by itself in a pattern will match when no digits are received, such as anonymous Caller ID [CLID] calls.

Editing Call Routing Table Patterns

You can edit CRT patterns.

To edit call routing patterns:

1. Select System – Trunk-Related Information – **Call Routing Tables**. The Call Routing Table list (1–15) appears.
2. Double-click the CRT. A list of existing patterns, if any, appears in the right pane.
3. Program the following options as necessary.
 - **Description:** Determines how the call is identified at display endpoints when received. The name can be any word or number (up to 12 characters) that identifies the call source. You can use any combination of letters and numbers.

To change the description of the pattern:

- a. Select the current value, then enter the new description in the text box.
 - b. Press **ENTER** or select another field to save the change.
- **Ring-In Type:** The following ring-in types are available:
 - **Single:** The destination can be an endpoint, hunt group, application, trunk group, individual trunk, or ARS. These can be local or off-node devices.
 - **Extension List:** You can select from any extension list in the local node.
 - **Call Routing Table:** When programming a CRT that rings in to another table, make sure the two tables do not send calls to each other, creating a “loop.” You can only select call routing tables located on the local node.
 - **DISA:** This allows the caller to select a destination.
 - **Collected Digits:** This ring-in type indicates that the collected DID [DDI] or DNIS digits (plus the base digits) should be used as the destination extension. This variable helps to keep the number of call routing table entries to a minimum.

Both trunk groups and call routing table entries can use this ring-in type. When Ring-In Type of Collected Digits is selected, the Ring-In Destination field is empty. If the collected digits plus the base digits do not make up a valid ring-in destination, the call is routed to the primary attendant. Valid ring-in destinations include on- or off-node endpoints, on- or off-node hunt groups, trunk groups, individual trunks, voice mail applications, automated attendants, and ARS.

NOTE

If Single, Extension List, or Call Routing Table is selected, you must also program the destination as described below. DISA ring-in requires no additional programming. Any DISA security codes programmed for the trunk group (see [page 8-25](#)) will apply to callers.

To change the Ring-In Type:

- a. Select the current Value, then scroll to the desired setting.
- b. Press **ENTER** or select another field to save the change.

- **Ring-In Destination:** To select the specific destination for the pattern, use one of the following methods:

Method A

- a. Select the current value, and then type the new value in the text box.
- b. Press **ENTER**. A screen appears displaying what is associated with the number entered.
- c. Click **OK**. The new number appears in the field.

Method B

- a. Right-click the existing Ring In Destination. An option box appears.
- b. Select the Change Ring-In Destination option. A window appears prompting for the device type to include.
- c. Select the appropriate destination type, and then click **Next**. The list of devices appears. You can view them in a list by selecting the List button or view details by selecting the Details button. If the Ring-In Destination is set to "None" the call will be sent to the primary attendant. Do not set this to None if there is not a primary attendant, because the call will not ring at any endpoint. Even though Primary Rate trunks appear in the selection list, they can only be used by selecting ARS; individual B-channel trunks or trunk groups containing B-channel trunks will not function properly with this feature.
- d. Select the desired device, then click **Finish**. The selection appears in the Ring-In Destination field.

Viewing Call Routing Patterns

To program the patterns for the Call Routing Table:

1. Select System – Trunk-Related Information – **Call Routing Tables**. The Call Routing Table list (1–15) appears.
2. Double-click the Call Routing Table. A list of existing patterns, if any, appears in the right pane.

Deleting a Pattern

To delete a pattern:

1. Select System – Trunk-Related Information – **Call Routing Tables**. The Call Routing Table list (1–15) appears.
2. Double-click the Call Routing Table. A list of existing patterns, if any, appears in the right pane.
3. Select the pattern you want to delete, right-click, and then select **Remove Selected Items**.

Adding a Single Pattern

To add a single pattern:

1. Select System – Trunk-Related Information – **Call Routing Tables**. The Call Routing Table list (1–15) appears.
2. Double-click the Call Routing Table.
3. Right-click anywhere in the right pane, and then select **Add To List**. The new pattern appears in the list.

Copying and Pasting Patterns

To copy and paste one or more patterns:

1. Select System – Trunk-Related Information – **Call Routing Tables**. The Call Routing Table list (1–15) appears.
2. Double-click the Call Routing Table.
3. Select the pattern that you want to copy.
4. Right-click, and then select **Copy Selected Pattern to**. The Copy Pattern(s) dialog box appears displaying the Current CRT.
5. Select the Destination CRT using the drop-down list box.
6. Click **Copy** to copy the pattern(s) from the Current CRT to the Destination CRT.

Selecting Batch Create Patterns

You can use the Batch Create Patterns feature for either U.S. or European installations.

To Batch Create Patterns:

1. Select System – Trunk-Related Information – **Call Routing Tables**. The Call Routing Table list (1–15) appears.
2. Double-click the Call Routing Table.
3. Right-click anywhere in the right pane, and then select **Batch Create Patterns**.
4. Select **Area Code** or **DID [DDI]**, and then click **Next**. A dialog box appears to program the pattern options.
5. To program an area code, follow the steps below. To program a DID number, go to [step 6](#).
 - a. In the **Pattern Name** box, type the name. The name is used for all area code patterns created using this batch command and determines how calls are identified at display endpoints. The name can be a word or number that identifies the call source. You can use any combination of letters and numbers.
 - b. In the **Ring-in Type** area, select the Ring-in Type option for the Call Routing Pattern. The ring-in type is used for all area code patterns created using this batch command. Ring-in destination types are as follows (see [page 6-25](#) for descriptions):
 - Single extension number (off-node device, endpoint, hunt group, application, trunk group, individual trunk, or ARS). Also requires the Ring-in Destination (see [step c](#)).
 - Extension list. Also requires the Ring-in Destination (see [step c](#)).
 - DISA (allows the caller to select a destination)
 - Collected digits
 - Call routing table. Also requires the Ring-in Destination (see [step c](#)).
 - c. *For Single, Extension List, and Call Routing Table Ring-in types only (see [step b](#)).* Click **Ring-In Destination**, and then select the destination type. After you return to the Call Routing Name and Ring-In Information screen, click **Next** to continue.

NOTE

Even though PRI trunks appear in the selection lists, they can only be used by selecting ARS; individual B-channel trunks or trunk groups containing B-channel trunks will not function properly with this feature.

- d. Select the area codes that will be included in the batch of patterns. (You can use the SHIFT or CTRL key to select more than one area code.)
- e. Click **Finish**.

6. Program the following DID [DDI] options:

U.S. DID installations only.

- a. In the **Enter the Description** box, type the base number of the DID number block in the box. Each pattern is identified in the list by the digits that are sent after the handshake. The base number of the DID numbers is the name prefix. The prefix and the collected digits are combined to form a complete number for display (for example, a base number 9619 would combine with digits 000 to display 9619000).
- b. In the **Enter the Initial DID** box, type the first number in the series of DID numbers being programmed. For example, if you were programming for DID numbers 9619000 through 9619019 (9619 is the base number), you would type 000.
- c. In the **Enter the Number of Patterns** list, select the number of DID numbers (up to 999) to include in the pattern list. In the example above (9619000 through 9619019) you would enter 20 because the range includes 20 DID numbers. Scroll to or enter the appropriate number (up to 999) for your DID list in the box.
- d. Click **Finish**.

European DDI installations only.

- a. In the **Enter the Description** box, type the base number of the DDI number block in the box. Each pattern is identified in the list by the digits that are sent after the handshake. The base number of the DDI numbers is the name prefix. The prefix and the collected digits are combined to form a complete number for display (for example, a base number 01162903 would combine with digits 000 to display 01162903000).
- b. In the **Enter the Initial DDI** box, type the first number in the series of DDI numbers being programmed (without the base number). For example, if you were programming for DDI numbers 01162903000 to 01162903019 (01162903 is the base number), you would enter 000.
- c. In the **Enter the Number of Patterns** list, select the number of DDI numbers (up to 999) to include in the pattern list. In the previous example (01162903000 to 01162903019), you would enter 20 because the range includes 20 DDI numbers.
- d. Click **Finish**.

Persistent Music-On-Hold Selection

Mitel 5000 Call Processing manages the audio connections for incoming Public Switched Telephone Network (PSTN) calls. When a device places a call on hold, CO trunk group settings determine the hold audio (see “Programming CO Trunk Group Options” on [page 8-10](#).)

You can route CO trunk calls through CRTs and use the matching CRT entry’s “Music-On-Hold Profile” to overwrite the settings at the CO trunk group. The Music-On-Hold profile provides the same Music-On-Hold fields that currently exist in a CO trunk group. [Table 6-3](#) shows an example of how the Music-On-Hold Profiles are handled when three CRT entries are chained.

Table 6-3. *An Example of the Music-On-Hold (MoH) Profiles for Chained CRTs*

	CRT #1	CRT #2	CRT #3	RESULT
MoH Profile IDs	None	None	None	Use the CO Trunk Group's MoH settings
	1	None	None	Use MoH Profile ID 1
	1	2	3	Use MoH Profile ID 3

If the matching CRT entry does not have a “Music-On-Hold Profile” set or the call is not routed through a CRT, the trunk determines the audio setting based on the CO trunk group settings. Therefore, the “Music-On-Hold Profile” in the matching CRT entry has priority over the audio settings in the CO trunk group.

If CRT entries are “chained” (a CRT entry may point to another CRT), the last matching CRT entry in the chain with a Music-On-Hold Profile set to anything other than “None” takes precedence. If the last matching CRT entry has a Music-On-Hold Profile set to “None,” the associated CO trunk group settings apply.

When the Music-On-Hold selection is set for a specific call, the Music-On-Hold setting persists through the duration of the call even if that call is forwarded, moved, or transferred.

The following are usage examples:

- Several businesses share a single phone system. Due to the layout and size of the companies involved, each business does not require its own CO trunk group. However, each business in the group owns a specific subset of the DID [DDI] numbers available. These businesses require their own Music-On-Hold played for callers. Using Persistent Music-On-Hold, each business would have a Music-On-Hold source assigned and would specify that source within the CRT entry for the matching called number.
- A business sells several different products. Customers call different numbers based on the product of interest. Management would like customers to hear Music-On-Hold based on the product in question. This feature would allow the specific CRT entry to dictate which source provides the Music-On-Hold for the incoming calls.

Creating Music-On-Hold Profiles

You must program Music-On-Hold Profiles before you can assign them to CRTs (see the following section).

To create Music-On-Hold Profiles:

1. Select System – Trunk-Related Information – **Music-On-Hold Profiles**.
2. Right-click **Add to Music-On-Hold Profiles List** in the right pane. The Get ID dialog box appears.
3. Select the starting ID and the number of IDs (up to 25) to create. For example, to create IDs 1–9, select **1** as the “Starting ID” and **9** as the “Number of IDs.”
4. Click **OK**. The items are added to the list with default values.
5. In the **Description** column, type the profile description.
6. Double-click the Music-On-Hold Profile that you want to program.
7. For each profile, select one of the following options from the list:
 - Music-On-Hold. For a feature description, see “Music-On-Hold” on [page 8-19](#).
 - Audio on Transfer to Ring. For a feature description, see “Audio on Transfer To Ring” on [page 8-19](#).
 - Audio on Hold for Transfer Announcement. For a feature description, see “Audio On Hold For Transfer Announcement” on [page 8-21](#).
 - Audio on Transfer to Hold. For a feature description, see “Audio On Transfer To Hold” on [page 8-20](#).
8. Click out of the field or press **ENTER** to save your change.

Assigning Music-On-Hold Profiles to CRTs

To assign Music-On-Hold Profiles to CRTs:

1. Select System – Trunk-Related Information – **Call Routing Tables**. A list of CRTs appears.
2. Click the desired CRT.
3. Right-click anywhere in the right pane, and then click **Add To List**. The Patterns list appears.
4. Do one of the following:
 - Type the desired profile ID in the **Music-On-Hold Profile** field.
 - Select the profile ID from the Change Music-On-Hold Profile dialog box:
 - a.) Right-click the existing Music-On-Hold Profile, and then select **Change Music-On-Hold Profile**. The Change Music-On-Hold Profile dialog box appears.
 - b.) Select **Music-On-Hold Profiles**, and then click **Next**.
 - c.) Select the desired Music-On-Hold profile, and then click **Finish**.

Loop Loss Measurement Test

Available in Remote Mode only. The Loop Loss Measurement Test measures and reports loop loss on loop start trunks. The test helps to determine the cause of low volume on loop start trunk calls. The test results appear in Message Print, as shown in [Figure 6-4](#). For more information, refer to the following resources:

- *Message Print Diagnostics Manual*, part number 550.8018
- *DB Programming Help*

Figure 6-4. Loop Loss Measurement Test Results

```

-01:512- 15:43 06-05 *** Scheduling Loop Loss trunk test on ext. 94257
-01:513- 15:43 06-05 *** Trunk: ID(1:'94257') Starting Automated Loop Loss Test.
-01:514- 15:43 06-05 *** Trunk: ID(1:'94257') Loop Loss Test # 1 Raw DSP Value: 548334 Loop Loss: 32.60 dB
-01:515- 15:43 06-05 *** Warning: Loop Loss value of 32.60 dB is greater than recommended threshold.
-01:516- 15:43 06-05 *** Trunk: ID(1:'94257') Loop Loss Test # 2 Raw DSP Value: 523554 Loop Loss: 32.80 dB
-01:517- 15:43 06-05 *** Warning: Loop Loss value of 32.80 dB is greater than recommended threshold.
-01:518- 15:43 06-05 *** Trunk: ID(1:'94257') Loop Loss Test # 3 Raw DSP Value: 423328 Loop Loss: 33.72 dB
-01:519- 15:43 06-05 *** Warning: Loop Loss value of 33.72 dB is greater than recommended threshold.
-01:520- 15:43 06-05 *** Trunk: ID(1:'94257') Loop Loss Test # 4 Raw DSP Value: 548423 Loop Loss: 32.60 dB
-01:521- 15:43 06-05 *** Warning: Loop Loss value of 32.60 dB is greater than recommended threshold.
-01:522- 15:43 06-05 *** Trunk: ID(1:'94257') Loop Loss Test # 5 Raw DSP Value: 549074 Loop Loss: 32.59 dB
-01:523- 15:43 06-05 *** Warning: Loop Loss value of 32.59 dB is greater than recommended threshold.
-01:524- 15:43 06-05 *** Trunk: ID(1:'94257') Loop Loss Test # 6 Raw DSP Value: 422915 Loop Loss: 33.73 dB
-01:525- 15:43 06-05 *** Warning: Loop Loss value of 33.73 dB is greater than recommended threshold.
-01:526- 15:43 06-05 *** Trunk: ID(1:'94257') Loop Loss Test # 7 Raw DSP Value: 424281 Loop Loss: 33.71 dB
-01:527- 15:43 06-05 *** Warning: Loop Loss value of 33.71 dB is greater than recommended threshold.
-01:528- 15:43 06-05 *** Trunk: ID(1:'94257') Loop Loss Test # 8 Raw DSP Value: 548818 Loop Loss: 32.60 dB
-01:529- 15:43 06-05 *** Warning: Loop Loss value of 32.60 dB is greater than recommended threshold.
-01:530- 15:43 06-05 *** Trunk: ID(1:'94257') Loop Loss Test # 9 Raw DSP Value: 549497 Loop Loss: 32.59 dB
-01:531- 15:43 06-05 *** Warning: Loop Loss value of 32.59 dB is greater than recommended threshold.
-01:532- 15:43 06-05 *** Trunk: ID(1:'94257') Loop Loss Test # 10 Raw DSP Value: 423451 Loop Loss: 33.72 dB
-01:533- 15:43 06-05 *** Warning: Loop Loss value of 33.72 dB is greater than recommended threshold.
-01:534- 15:43 06-05 *** Trunk: ID(1:'94257') Finished Loop Loss Test
-01:535- 15:43 06-05 M2038 INF HW CP Failed Session Startup With Node 2
-01:536- 15:44 06-05 M2038 INF HW CP Failed Session Startup With Node 2
  
```

You should run the Loop Loss Measurement test after you run the Hybrid Balance Test. For more information about the Hybrid Balance Test, see [page 6-17](#). For troubleshooting information, see [page 17-16](#).

Configuring Loop Loss Measurement Test Fields

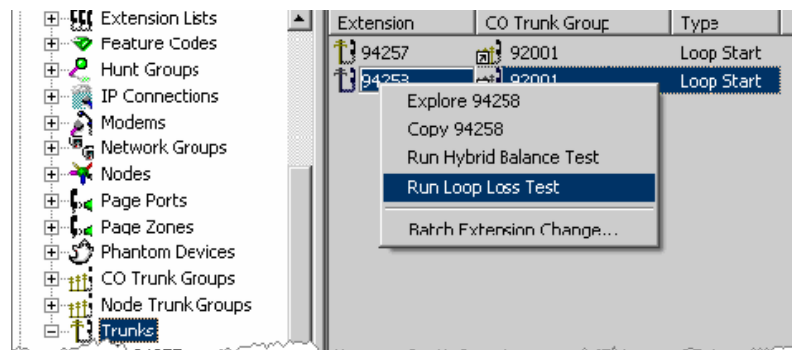
To configure global settings for the loop loss measurement test:

1. Select System – Trunk-Related Information – **Loop Loss Test Settings**.
2. Program the following fields:
 - **Test Number:** Type the phone number to call that plays the test tone. Do not prepend an outgoing digit. The range is 15 numeric characters.
 - **Test Transmit Level in dBm:** The Test Transmit Level is the volume of the tone that the test number sends when you call it. This tells the system what the original tone was, and it compares the tone that it measures against that to calculate the loop loss. The value needs to come from whoever you get the test number itself from (that is, whoever provided your analog trunks). Usually this field is either 0 or -10 dBm (most likely 0 dBm). The range is 1–120 dBm; the default is 0 dBm.
 - **Warning Threshold for Loss in dB:** Specifies how much loss must be present for Call Processing to issue a Message Print indicating that there has been too much loss on the line. The range is 0–75 dB; the default is 8 dB.
 - **Number of Test Passes:** The length of time after you dial the number before the DSP Resource starts measuring the signal. You must time how long it takes the tone to start playing from the time you dial the last digit of the test number. The range is 0–255 ms; the default is 10 ms.
 - **Duration of Measurement in milliseconds:** Specifies how long the DSP Resource spends measuring the signal. The range is 1-65535 ms; the default is 500 ms.

Starting a Loop Loss Measurement Test

To start a Loop Loss Measurement Test on a single trunk:

1. Select System – Devices and Feature Codes – **Trunks**.
2. In the **Extension** column, right-click on the trunk, and then select **Run Loop Loss Test**, as shown below. The test results appear in Message Print.



Loop Start AC Impedance

The Loop Start AC Impedance setting consists of default line types specific to each country. Each country should have a default value that corresponds to the country type of the software build.

Table 6-4. *AC Impedance Settings by Country*

AC Impedance	Country
600 Ohms	Argentina, Brazil, Chile, China (data), Columbia, Ecuador, El Salvador, Guam, Hong Kong, India, Indonesia, Japan, Jordan, Kazakhstan, Kuwait, Macao, Malaysia, Mexico, Oman, Pakistan, Peru, Philippines, Russia, Saudi Arabia, Singapore, South Korea, Taiwan, Thailand, United Arab Emerites, United States, Yemen
900 Ohms	United States alternate
TBR21 270R + (750R// 150 NF)	Austria, Bahrain, Belgium, Croatia, Cyprus, Czeck Republic, Denmark, Egypt, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Latvia, Lebanon, Luxembourg, Malta, Morocco, Netherlands, Nigeria, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom
220R + (820R// 120NF	Australia, Bulgaria, South Africa
370R + (620R// 310NF	New Zealand
320R + (1050R/ /230NF)	United Kingdom (old)

To change the Loop Start Impedance setting:

1. Select System – Trunk-Related Information – **Loop Start Impedance**.
2. In the Value column, select the option from the list.
3. Click out of the field or press **ENTER** to save the change.

ISDN PRI Two B-Channel Transfer

The ISDN PRI Two B-Channel Transfer (TBCT) feature is an ISDN optimization service offered by the PSTN. You must purchase support for the TBCT from the CO. The TBCT feature optimizes trunk-to-trunk calls by releasing them from the PBX and connecting them through the Central Office (CO). This optimization removes the trunk-to-trunk call legs from the system and allows the system to reuse the 2 B-channels for new calls.

This feature supports the basic TBCT functionality from the *Telcordia specification GR-2865-CORE, Generic Requirements for ISDN PRI Two B-Channel Transfer, Issue 3, March 2000*. A future release may implement other 2B-Transfer methods based on other specifications.

TBCT includes the following options:

- **Enable ISDN Two B-Channel Transfer:** When selected, the TBCT feature is initiated for the ISDN port (the default is *No*), see [page 6-35](#).
- **Display “T” for Two B-Channel Transferred Calls:** When selected, SMDR displays a “T” in the output when a TBCT occurs (the default is *No*). See “Display “T” for Two B-Channel Transferred Calls” on [page 3-52](#).

For sample call flow diagrams, refer to the “System Features” chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

TBCT includes basic functionality with support for the following conditions:

- Both the PBX and PSTN must support the feature.
- TBCT requires two PRI calls, which the PSTN connects before releasing them from the PBX. From an ISDN signaling perspective, one call must be an incoming or outgoing call to the PBX in the connected state (answered) and the other call must be an outgoing call from the PBX in the alerting or connected state.
- The two PRI calls involved in the TBCT may be on a single PRI port or in separate PRI ports.
- In a multi-PRI scenario, both PRI ports need to connect to the same CO and they must be in the same trunk group at the CO. The TBCT is still attempted, but it fails if this condition is not met.
- Although the PSTN may send the values of counters (Active Transfers and Available Transfers) in the TBCT messaging, the Mitel 5000 system ignores these counters.
- The Mitel 5000 system automatically attempts the TBCT as long as both calls are in the correct state, the PRI port (or both ports) has its corresponding TBCT flag enabled, and all the TBCT information is available to generate the TBCT request. You do not need to use a feature code to initiate a TBCT.
- If the PSTN rejects a TBCT request, the Mitel 5000 system does not retry the TBCT request for the same calls. The Mitel 5000 system logs the TBCT request failure and attempts a new TBCT request for only new calls. The calls involved in the failed TBCT attempt remain connected as if the TBCT was never requested.
- Upon completion of a TBCT, the system no longer has the ability to monitor the transferred call. Even if the PSTN notifies the system when the transferred call terminates, the system ignores such notification. Because of this implementation, third-party System OAI applications (such as Contact Center Suite and Unified Communicator[®]) are not able to detect that a TBCT occurred. These applications view the TBCT event as if both calls involved in the TBCT disconnected. Similarly, call cost records (such as those recorded in SMDR) terminate once the optimization occurs.

For multiple node configurations, both nodes with the PRIs involved in a TBCT must be running Mitel 5000 v3.0 or later software. Intermediate nodes do not have to be running the latest software. If one of the two nodes involved in the TBCT is not running the latest software, the systems do not attempt a TBCT and the calls work normally as unsupervised CO trunk-to-trunk calls.

You can enable TBCT for PRI reports. To enable TBCT for Station Message Detail Recording (SMDR), see “Display “T” for Two B-Channel Transferred Calls” on [page 3-52](#).

To enable TBCT:

1. Select System – Communication Server – **Dual T1/E1/PRI Module or T1/E1/PRI Module**, and then click **T1/PRI or E1/PRI**.
2. Select **Enable ISDN Two B-Channel Transfer**.
3. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
4. Press **ENTER** or select another field to save the change.

Endpoints and Devices

Introduction	7-4
Viewing System Endpoints	7-4
Creating (Adding) Devices	7-4
Adding Digital Endpoints	7-4
Creating Local IP Endpoints and Devices	7-5
Creating Endpoints from CSV Files	7-8
Creating a CSV File	7-9
Creating IP Endpoints from CSV Files	7-10
Creating Digital Endpoints from CSV Files	7-11
Creating Off-Node Devices	7-13
Using the Wildcard Character in Off-Node Extensions	7-14
Programming Device Descriptions and User Names	7-15
IDS Support	7-15
Hiding User Names in Voice Mail Directories	7-15
Copying Endpoint Programming	7-16
Viewing Associated Devices and References	7-17
Converting Usernames to Mixed Case	7-18
Converting Inter-Tel IP Endpoints to Mitel IP Endpoints	7-19
Editing IP Device MAC Addresses	7-20
Editing a Single MAC Address	7-20
Editing Multiple MAC Addresses	7-20
Changing Endpoint Extension Numbers	7-21
Changing a Single Extension Number	7-21
Changing Multiple Extension Numbers at One Time	7-21
Endpoint Flags	7-22
Programming Flags for Individual Endpoints	7-22
Programming Flags for Multiple Endpoints	7-22
Keymaps	7-27
Viewing Default Keymaps	7-28
Adding New Keymaps	7-29
Programming Endpoint Keymaps	7-30
Keymap Number Column	7-30
Keymap Value Column	7-30
Keymap Selection Column	7-31
Selecting Standard or Alternate Keymaps	7-39
Changing Keymap Types	7-40
Copying and Pasting Keymaps	7-41

Programming Endpoint Keymap Buttons	7-42
Programming DSS Keymaps	7-44
Automatically Populating DSS Keymaps	7-44
Manually Populating DSS Keymaps	7-45
Programming DSS Endpoint Lists	7-48
Programming DSS/BLF Devices for Digital Endpoints	7-49
Programming Endpoint Options	7-50
Associated Extensions	7-51
Call Logging	7-54
Day and Night Classes of Service	7-55
Programming Endpoint Toll Restrictions	7-55
Deleting Classes of Service	7-55
Forwarding Paths	7-56
Adding Forwarding Paths	7-57
Deleting Forwarding Paths	7-57
Programming Specific Forwarding Paths	7-57
Enabling Forwarding Path Options	7-57
Mailboxes	7-58
Record-A-Call	7-58
Programming the Record-A-Call Mailbox	7-59
Programming the Mailbox User-Keyed Extension	7-59
Programming the Record-A-Call Application	7-60
Languages	7-60
Secondary Language	7-61
House Phones	7-62
Assigning an Endpoint as a House Phone	7-62
Assigning House Phone Day and Night Extension Numbers	7-62
Remote Programming Password	7-63
Calling Party Name	7-63
Calling Party Number	7-64
Emergency Party Calling Number	7-64
Attached Device	7-64
Device Audio for Calls Settings	7-65
Audio for Calls Camped onto this Device	7-65
Audio for Calls Holding for this Device	7-65
Audio for Calls Ringing this Device	7-66
Phantom Devices	7-67

Account Codes	7-69
Viewing Account Codes	7-70
Programming Forced Account Code Options	7-70
Adding Devices to an Account Code List	7-70
Deleting Devices from Account Code Lists	7-71
Assigning an Account Code Type to an Individual Endpoint	7-71
Setting the Forced Account Code Validated Flag	7-71
Endpoint Messages	7-72
Changing Do-Not-Disturb Messages	7-72
Changing Reminder Messages	7-73
System Forwarding Paths	7-74
System Speed Dial	7-75
Administrator Endpoint DB Programming Password	7-76
Message Centers	7-77
Attendants	7-78
Primary Attendants	7-79
Single Line Endpoint CLID Timers	7-80

Introduction

This section provides information about how to program endpoints and devices. Endpoints and devices can either use analog, digital, or Internet Protocol (IP) transmission lines.

Because IP devices require configured network settings, you must program IP endpoint settings in DB Programming. See “Creating Local IP Endpoints and Devices” on [page 7-5](#). IP devices also require specific IP configurations and system settings. For more information about IP system settings, see “System and Device IP Settings” on [page 9-1](#).

Viewing System Endpoints

In the Endpoints programming section, you can create off-node devices for endpoints on the other nodes and program individual endpoints on the Local node.

To view the list of endpoints on the Local node:

1. Select System – Devices and Feature Codes – **Endpoints**.
2. Double-click **Local**. A list of current endpoints appears. At this level, you can change the description or username and view the endpoint type and circuit number (address).

Creating (Adding) Devices

You can create new endpoints for the local node or remote nodes. You can also use the Configuration Wizard to create endpoints. For more information about the Configuration Wizard, refer to the Installation chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

Each node in the network has its own extension and feature code programming. However, the network should have a universal numbering plan so that extension numbers on the various nodes do not overlap and do not conflict with feature codes. That is, when planning the extension numbers for each of the nodes in the network, set aside a block of extension numbers (for endpoints, hunt groups, voice processor applications, and so on) for each node.

Adding Digital Endpoints

For instructions to add digital endpoints, refer to the “Installation” chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

Creating Local IP Endpoints and Devices

You can create IP endpoints, IP softphones, or IP single line adaptors (SLAs) for the local node. When you create any IP endpoint or device, you must also configure IP endpoint settings. For more information about IP device settings, see “Endpoint and Device IP Settings” on [page 9-36](#).

WARNING

Possible Delay in Local Emergency Response to Remote Sites.

IP and SIP endpoint users should be alerted to the following hazardous situations:

- If an Emergency Call phone number is dialed from an IP or SIP endpoint located at a remote site that is **not** equipped with a correctly configured gateway, the call will be placed from the location where system chassis is installed rather than from the location where the emergency call is made.

In this situation, emergency responders may be dispatched to the wrong location. To minimize the risk of remote site users misdirecting emergency responders, Mitel recommends regular testing of MGCP/SIP gateway trunk(s) for dial tone.

- If uninterruptible power supply (UPS) protection has **not** been installed as part of the Mitel 5000 system, IP and SIP endpoints will **not** operate when electrical power fails either at remote sites or at the main system location.

To place calls during a power failure in this situation, IP and SIP endpoint users can only use a single line endpoint connected to one of the power failure bypass circuits built into the system chassis. If an endpoint connected to a power failure bypass circuit is not available, users should make emergency calls **from a local phone not connected to the system**. For more information about the Power Bypass feature, refer to the Installation chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

NOTES

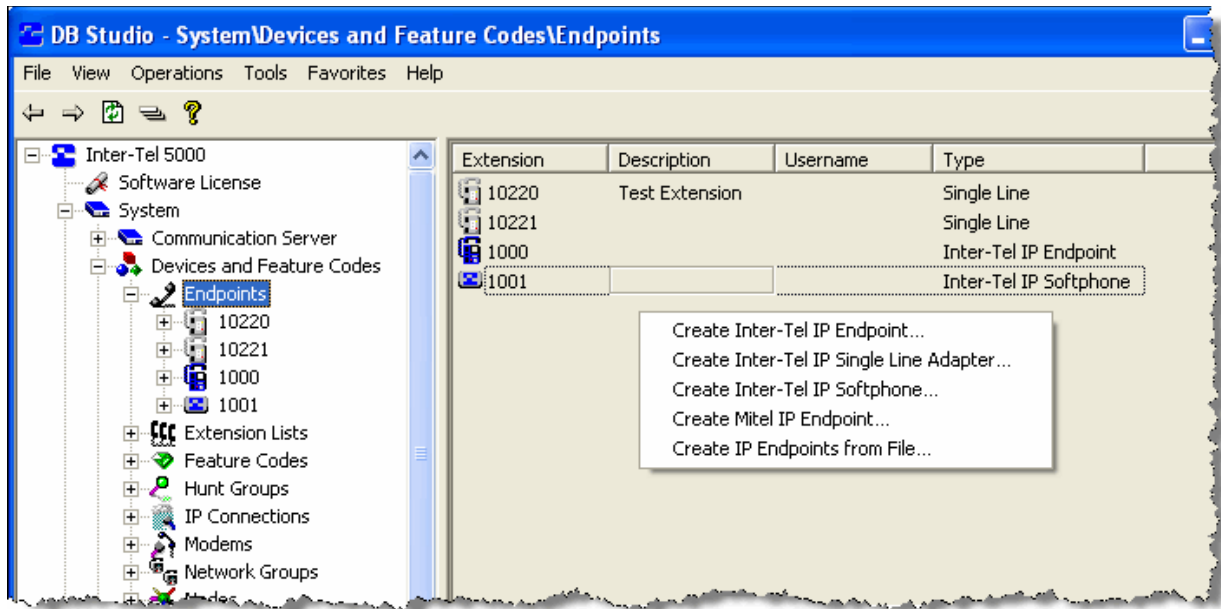
You can oversubscribe the IP resources by configuring more devices than can be active at the same time. Although you can create more IP endpoints or IP trunks than resources reserved, you *cannot* create more IP devices than the system supports. If you attempt to create more IP endpoints or IP trunks than the available value, an error message appears stating that you cannot exceed the system limit.

Fax over IP (FoIP) and modems are not supported through an IP SLA. To connect a fax machine, attach it to a single line port on one of the single line interfaces supported by the Mitel 5000 platform. Mitel currently supports T.38 FoIP only.

To create IP endpoints or Single Line Adapters:

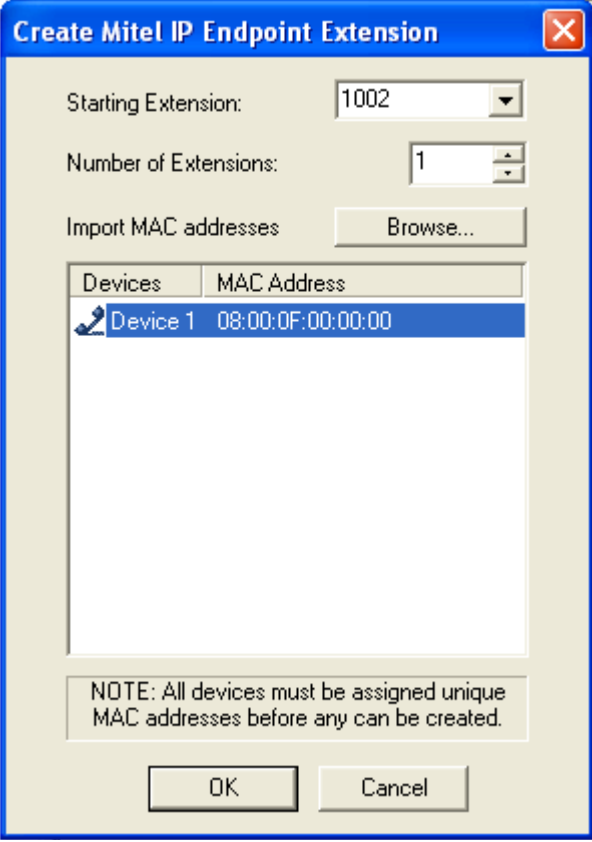
1. Select System – Devices and Feature Codes – **Endpoints**.
2. Right-click anywhere in the right pane to show device options, as shown in [Figure 7-1](#).

Figure 7-1. Create IP Device Options



3. Select one of the following device options:
 - **Create Inter-Tel IP Endpoint:** For all Inter-Tel 86xx-series hard IP endpoints.
 - **Create Inter-Tel IP Single Line Adapter:** For Inter-Tel single line adapters. The port addresses for the Single Line ports are 11.1.1 and 11.2.1.
 - **Create Inter-Tel IP Softphone:** For Inter-Tel IP Softphones. For example, the Inter-Tel Model 8602 Softphone.
 - **Create Mitel IP Endpoint:** For all Mitel 5000-series endpoints.
 - **Create IP Endpoints from File:** Create endpoints from a comma-separated value (CSV) file. "Creating Endpoints from CSV Files" on [page 7-8](#).

4. The following dialog box appears, depending on your selection.



The dialog box is titled "Create Mitel IP Endpoint Extension". It contains the following fields and controls:

- Starting Extension:** A dropdown menu with "1002" selected.
- Number of Extensions:** A spinner box with "1" selected.
- Import MAC addresses:** A button labeled "Browse..."
- Table:** A table with two columns: "Devices" and "MAC Address". It contains one row: "Device 1" with the MAC address "08:00:0F:00:00:00".
- NOTE:** A text box stating "NOTE: All devices must be assigned unique MAC addresses before any can be created."
- Buttons:** "OK" and "Cancel" buttons at the bottom.

5. From the **Starting Extension** list, select a starting extension from the list of available extensions, or type the extension number.
6. From the **Number of Extensions** list, select or type the number of extensions that you are creating.
7. Do one of the following:
- *If you are creating IP endpoints or IP SLAs:*
Click any endpoint with a red "X" and type a valid MAC address. You can also click **Browse**, and then import the MAC addresses from a batch file. The batch file can be a simple text file consisting of a list of MAC addresses. If you need only 20 addresses from the list, the first 20 addresses are imported.
 - *If you are creating IP softphones:*
Click the device value to enter an ID for the IP Softphone. For troubleshooting purposes, use the extension number as the last digits of the device ID. For example, if the extension number is 1001, the device ID could be 86.02.36.00.**10.01**.
8. After you have entered all of the MAC addresses, click **OK**. If you entered the same number as an existing extension, an error message appears and you must enter a new number. The new off-node device appears in the list without a description or username.

Creating Endpoints from CSV Files

A CSV file is an industry-standard format for text files containing data fields delimited by commas. DB Programming expects an endpoint information file to use either the TXT or CSV file extension and adhere to the other properties of a CSV file. Remember the following when creating a CSV file:

- Each line in the file represents information for a single endpoint. Information cannot be continued from one line to another.
- Data fields are delimited by commas.
- Only printable characters are considered part of a data field. Control characters within a data field are ignored.
- Each line contains the same number of data fields.
- If a comma is to be considered part of the data, that entire data field must be escaped by double-quotes at the beginning and end of the data field (for example, the data: Jones, Jim would be represented by the data field: "Jones, Jim").
- If a double-quote character is to be considered part of the data in a field, the entire field must be escaped by double-quotes at the beginning and end of the field and the double-quote character itself must be escaped by a preceding double quote (for example, the data: Sara "S" would be represented by the data field: "Sara ""S""").
- If no MAC addresses are read from the file, or if the MAC addresses contain invalid characters, a MAC address default of "00:00:00:00:00:00" is used for each IP endpoint imported. You must edit the MAC addresses in the dialog box.
- If no extensions are read from the file, the first available extension for a DB Programming endpoint is used for each endpoint to be imported. You must edit the extensions in the dialog box to resolve the conflicts.
- Regarding headers:
 - To use user-defined headers in a CSV file, the headers must be listed on the very first line. DB Programming reads the first line of the file and if no digits are identified, the first line is assumed to contain headers.
 - If the first line is identified as a header by DB Programming, DB Programming reads each field and tries to match the field with a pre-defined endpoint attribute. These include "Extension," "Username," "Description," and "MAC Address."

To identify a data field as a pre-defined endpoint attribute, DB Programming sets all of the characters to lower-case, and then reads the field. [Table 7-1](#) shows how DB Programming identifies substrings.

Table 7-1. Substrings and Headers

Substring	Header
ext	Extension
user	Username
desc	Description
mac	MAC Address

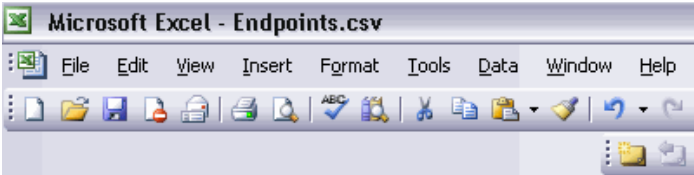
Headers are used when parsing the remaining fields in the CSV file. The order of the headers corresponds to the order of the fields in the remaining entries of the file. As DB Programming parses each field, it uses the header order to determine which type of attribute it is reading. For example, if "Extension" was the first data field read, the first data field of each successive line in the file is considered an endpoint extension.

- If any digits are present in the first line of the file, DB Programming assumes there is no header in the file and uses its predefined order of fields: "Extension," "Description," "Username," "MAC Address" (MAC Address is only assumed if importing IP endpoints, otherwise, only three fields are expected per endpoint).
- Additional fields and headers not associated with the predefined endpoint attributes, "Extension," "Username," "Description," or "MAC Address" are ignored.

Creating a CSV File

To create a CSV file:

1. Open the template file, `EndpointImport.csv`, located in `C:\InterTel\CS5000\Templates` on the DB Programming computer.
2. Type the information that you want to import to DB Programming. The following is an example of endpoint information listed in a Microsoft Excel® spreadsheet.



	A	B	C	D
1	Extension	Description	Username	MAC
2	1001	Arthur Macbeth	ARTHUR	00:10:36:15:19:AF
3	1002	Danielle Rose	DANI	00:10:36:15:19:AB
4	1003	Doug Joarczyk	DOUG	00:10:36:15:19:AC
5	1004	Vanessa Li	V	00:10:36:15:19:AD
6	1005	Tabitha Turner	Tabitha	00:10:36:15:19:AE
7	1006	Lisa Marie	Lisa	00:10:36:15:19:A2
8	1007	Lani Tyler	Lani	00:10:36:15:19:A5
9	1008	Lindsay Michaels	Lindsay	00:10:36:15:19:A6

3. Save the data as a CSV file. The following is an example of the file data after it is saved.

```
Extension,Description,Username,MAC
1001,Arthur Macbeth,ARTHUR,00:10:36:15:19:AF
1002,Danielle Rose,DANI,00:10:36:15:19:AB
1003,Doug Joarczyk,DOUG,00:10:36:15:19:AC
1004,Vanessa Li,V,00:10:36:15:19:AD
1005,Tabitha Turner,Tabitha,00:10:36:15:19:AE
1006,Lisa Marie,Lisa,00:10:36:15:19:A2
1007,Lani Tyler,Lani,00:10:36:15:19:A5
1008,Lindsay Michaels,Lindsay,00:10:36:15:19:A6
```

Creating IP Endpoints from CSV Files

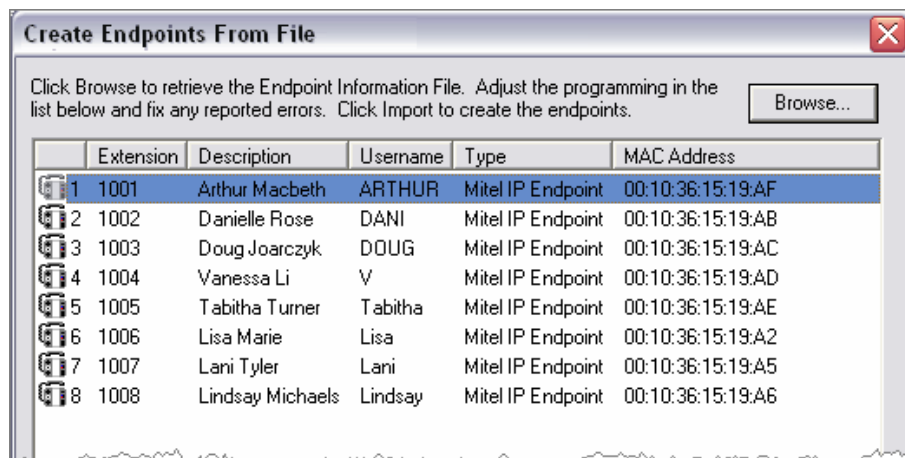
You can create IP endpoints from created CSV files (see [page 7-9](#)). For instructions to create digital endpoints from CSV files, see [page 7-11](#).

To create IP endpoints from a CSV file:

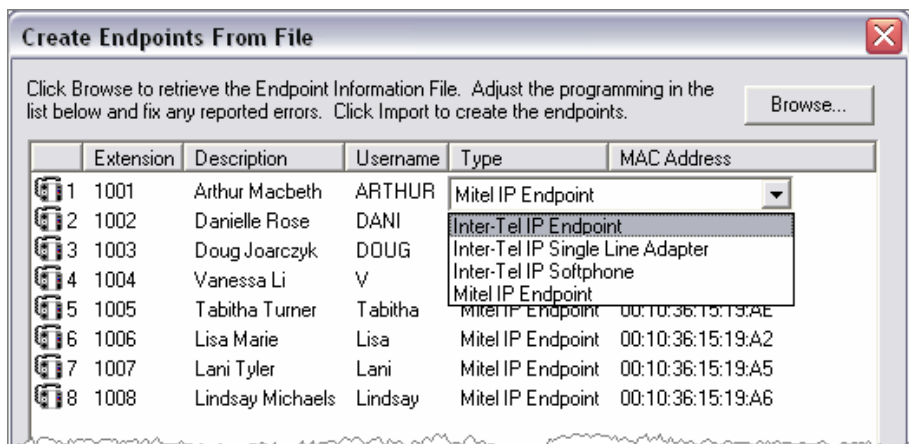
NOTE

You can also use the Configuration Wizard (beginning at the IP Device Setup dialog box) to import IP endpoints from a CSV file. For more information, refer to *Mitel 5000 DB Programming Help*.

1. Select System – Device and Feature Codes – Endpoints – **Local** or **Remote**.
2. Right-click in the right pane, and then select **Create IP Endpoints from File**.
3. Click **Browse** to select the file containing the CSV file. After DB Programming reads the file, the information appears in the list control, as shown in the following example.



4. Do one the following:
 - To change the type, left-click the field, and then select one of the other options. By default, the **Mitel IP Endpoint** type is selected for each imported endpoint.



- To batch change the type of several endpoints, select the fields, right-click, and then select **Batch Change Type**. The Batch Change Type dialog box appears. Select the type for the endpoints, and then click **OK**.
- To delete endpoints, select the endpoint that you want to delete, and then right-click and select **Delete**.

DB Programming validates the information and reports any issues. If there are no errors or conflicts, proceed to step 5. If any errors exist, the Import button is disabled. See [page 17-30](#) for a list of possible error messages and troubleshooting information.

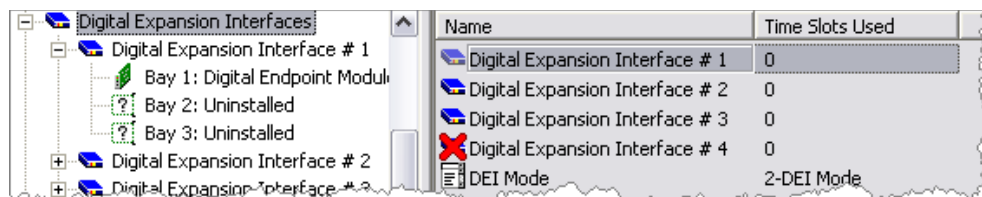
Edit the information in the list and after all entries are valid, the Import button becomes enabled. Then proceed to step 5.

5. Click **Import** to program the endpoints in the database. At any point, click **Cancel** or click on the red "X" at the top of the dialog box to cancel the creation of new endpoints and return to the prior view of DB Programming.

Creating Digital Endpoints from CSV Files

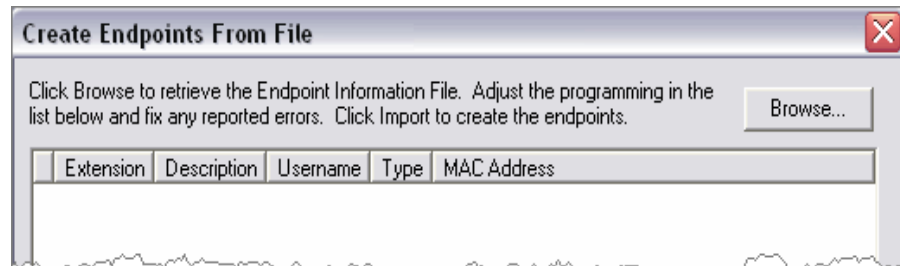
To create digital endpoints from a file:

1. Select System – Communication Server – **Digital Expansion Interface**, as shown in the following example.

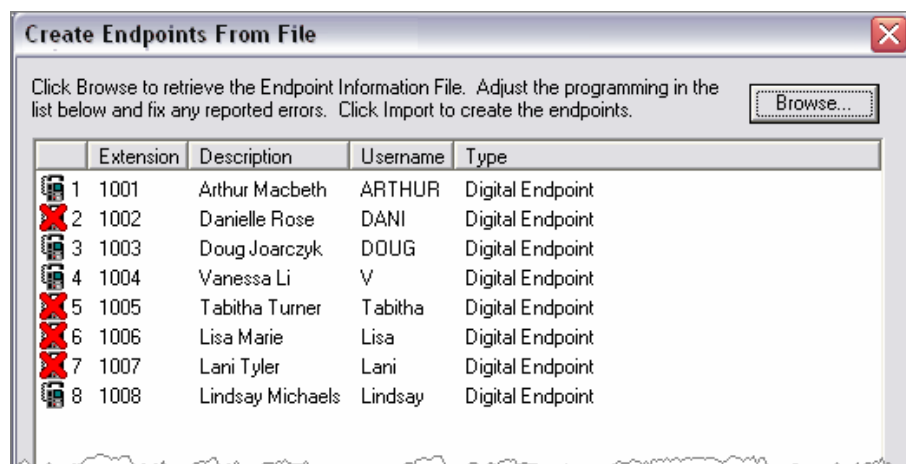


2. Double-click the Digital Expansion Interface that you are using, and then click **Digital Endpoint Module - 16**.
3. Right-click the port(s), and then select **Create Digital Endpoints from File**.

The Create Endpoints From File dialog box appears.



- Click **Browse** to select the file containing the information for the endpoints. After DB Programming reads the file, the information appears in the list control.



The Type fields are listed as “Digital Endpoints” because only digital endpoints may be programmed in the DEM-16 ports through this dialog box.

To delete endpoints, select the endpoint that you want to delete, and then right-click and select **Delete**.

DB Programming validates the information and reports any issues. If there are no errors or conflicts, proceed to step 5. If any errors exist, the Import button is disabled. See [page 17-30](#) for a list of possible error messages and troubleshooting information.

Edit the information in the list and after all entries are valid, the Import button becomes enabled. Then proceed to step 5.

- Click **Import** to program the endpoints in the database. At any point, click **Cancel** or click on the red “X” at the top of the dialog box to cancel the creation of new endpoints and return to the prior view of DB Programming.

Creating Off-Node Devices

Off-node devices give node users access to devices (for example, other system extensions) on other nodes. Each off-node device is identified with an extension number, description, username, device type (endpoint, hunt group, application, or page port), and node identification number. The description and username options are for directory features only. For more information about system nodes, see “Private Networking and System Nodes” on [page 4-1](#).

NOTICE

Possible System Instability. Do not create or delete more than 2000 off-node devices at a time. Batch creating more than 2000 off-node devices may cause problems with the system.

Only the local directory features are affected when you change the description and username of an off-node device—remote nodes do **not** send updates to other nodes when off-node device information is changed. Only the local node for that device sends out any updates. For example, if the device is programmed as John Doe on node 1, but you change the associated off-node device to Jane Smith on node 2, the node 2 IC directory reflects Jane Smith. The device on node 1, however, still displays John Doe.

You can create off-node devices for endpoints on the other nodes and program individual endpoints on the Local node.

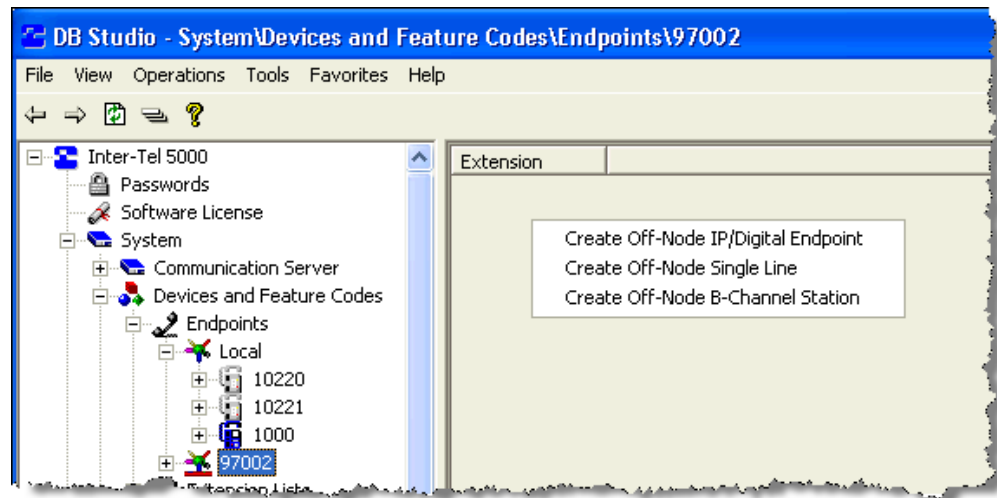
To select the node to program:

1. Select System – Devices and Feature Codes – **Nodes**.
2. Double-click the node number. The current list of off-node devices for that node appears.

To create off-node devices:

1. Select System – Devices and Feature Codes – **Endpoints**.
2. Right-click anywhere in the right pane to view the list of options, as shown in [Figure 7-2](#).

Figure 7-2. Off-Node Device Options



3. Select one of the following options:
 - Create Off-Node IP/Digital Endpoint
 - Create Off-Node Single-Line
 - Create Off-Node B-Channel Station
4. Depending on your selection, the Create <off-node device> dialog box appears.

5. Select the starting extension number or enter the wildcard extension for the devices. For more information about wildcard extensions, see the following section, [“Using the Wildcard Character in Off-Node Extensions”](#).
6. If applicable, enter the number of extensions.
7. Click **OK**. If you entered the same number as an existing extension, an error message appears, and you must enter a new number. The new off-node device appears in the list without a description or username.

Using the Wildcard Character in Off-Node Extensions

Wildcard extensions can only be used for off-node devices. You can use the wildcard character X in extension numbers to represent “any digit.” This allows you to include a range of extensions as one off-node device entry.

Wildcard extensions are made up of digits (1–9), followed by wildcard digit X. Examples of valid wildcard extensions are 1XXX (range of 1000–1999), 14XX (range of 1400–1499), 7X (range of 70–79). For example, if there is a 14XX wildcard, users can dial 1433 and be connected to that off-node device.

The following limitations apply to using wildcard extensions:

- There is no entry for wildcard extensions in the intercom directory. DSS buttons can be programmed for the individual devices the wildcard extension is representing.
- Voice Processing cannot create associated mailboxes for endpoints included in wildcard ranges. To have an associated mailbox, the off-node endpoint must have its own off-node device entry on the node where the external voice processing system is located.

Programming Device Descriptions and User Names

Device descriptions are used in the IC directory and user names appear on endpoint displays. Also, because the Intelligent Directory Search (IDS) feature (see the following section) searches for endpoint descriptions and user names, the information entered in the endpoint Description and Username fields affects how people search for information in the system.

NOTE

If you do not program the description and username for the endpoints on the local node, the local endpoints will not display in the IC directory.

Also, only the local directory features are affected when you change the Username and Description of an off-node device. Remote nodes do not send updates to other nodes when off-node device information is changed. Only the local node for that device sends out updates. For example, if the device is programmed as John Doe on node 1, but you change the associated off-node device to Jane Smith on node 2, the node 2 IC directory reflects Jane Smith. The device on node 1, however, still displays John Doe.

To enter a a device description or username:

1. Select System – Devices and Feature Codes – **Endpoints**.
2. In the **Extension** column, select **Description** or **Username**, and then enter the new information in the box. Descriptions can contain up to 20 characters and usernames can contain up to 10 characters. To ensure proper operation of voice pocessor directories, enter the full name in the form: Last name, First name. Do not use slash (/), backslash (\), vertical bar (|), or tilde (~) characters in user names. Do not use Control characters or punctuation marks in descriptions or usernames.
3. Click out of the field or press **ENTER** to save your change.

IDS Support

The Mitel 5000 supports Intelligent Directory Search (IDS), which is similar to the “text on 9 keys” (T9) predictive search feature used for mobile phones. For more information about IDS, refer to the System Features chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

Hiding User Names in Voice Mail Directories

You can hide programmed descriptions in the Voice Mail Directory. For example, a user may have a primary extension at the office programmed as “Bond, James.” However, the same user may have a secondary extension—for example, at home—that is not published from the Voice Mail Directory.

Because the IC directory is intended for internal use, both primary and secondary extension entries appear in the IC directory. There may be any number of primary (no tilde in description) and secondary extensions (first character of description is a tilde). To differentiate between these two, an asterisk appears immediately before the secondary extension entry—for example, “*James Bond”.

To hide an entry in the Voice Mail directory:

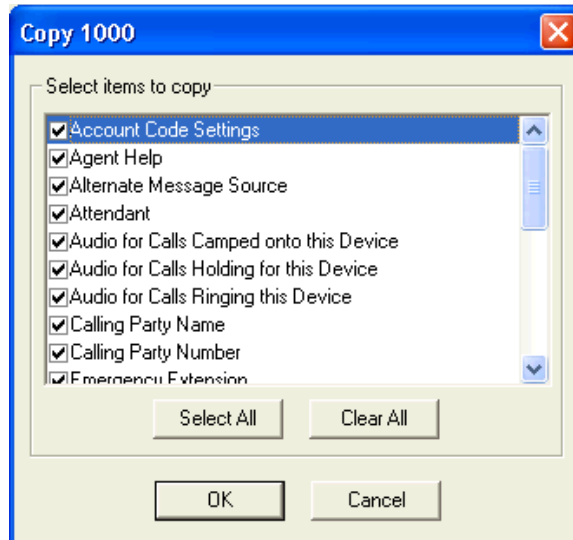
Enter a tilde (~) in the Description field immediately before the last name—for example, “~BOND, JAMES”. The tilde character (~) makes the entry inaccessible in the Voice Mail directory. Note that if someone knew the number of the secondary extension, they could dial that extension directly. Someone entering “BOND” (2 6 6 3) at the Voice Mail prompt, however, would find only the primary extension.

Copying Endpoint Programming

If you have multiple endpoints that use the same programming, you can copy the programming from one endpoint to the others.

To copy an endpoint:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Right-click the extension number that you want to copy, and then select **Copy**.
3. Right-click the endpoint in which you want the copied settings pasted, and then select **Paste**. A dialog box appears, similar to the one shown in the following example.



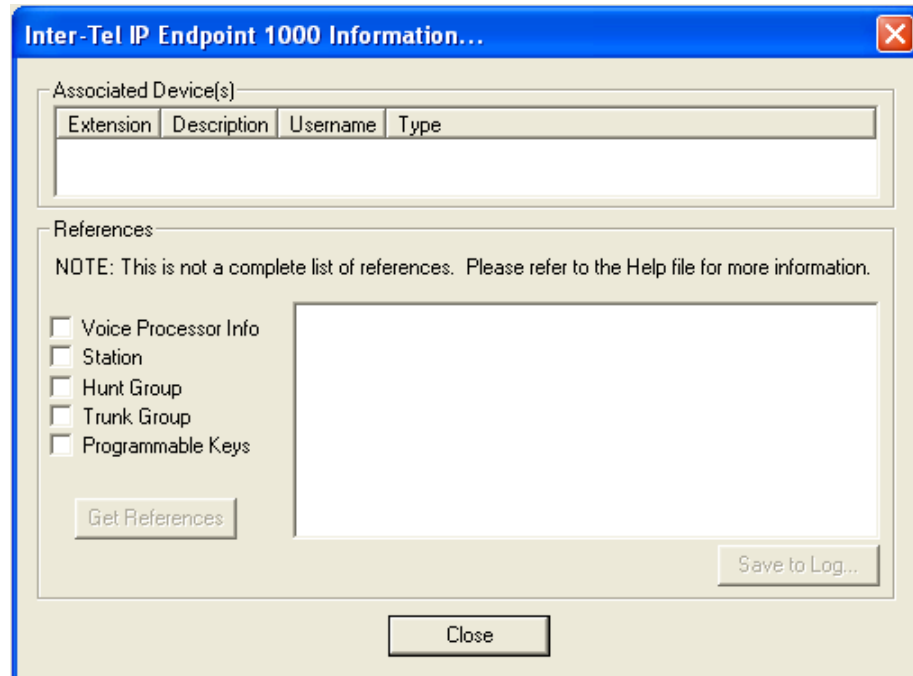
4. Select or clear the attributes that you want to copy to the endpoint.
5. Click **OK** to save the changes.

Viewing Associated Devices and References

You can use the Associated Devices and References feature to view the associated devices for an endpoint, mailbox, or hunt group. You can also use the Associated Devices and References feature to query various groups in the database to locate the associated endpoint to the extension.

To view Associated Devices:

1. Select – System – Devices and Feature Codes – **Endpoints**.
2. Right-click the endpoint, and then select **Associated Devices and References**. A dialog box similar to the following appears.



The dialog box is titled "Inter-Tel IP Endpoint 1000 Information...". It contains two main sections: "Associated Device(s)" and "References".

The "Associated Device(s)" section has a table with the following headers: Extension, Description, Username, and Type. The table is currently empty.

The "References" section contains a note: "NOTE: This is not a complete list of references. Please refer to the Help file for more information." Below the note is a list of checkboxes with labels: Voice Processor Info, Station, Hunt Group, Trunk Group, and Programmable Keys. All checkboxes are currently unchecked. Below the list is a button labeled "Get References".

At the bottom right of the dialog box is a button labeled "Save to Log...". At the very bottom center is a button labeled "Close".

Converting Usernames to Mixed Case

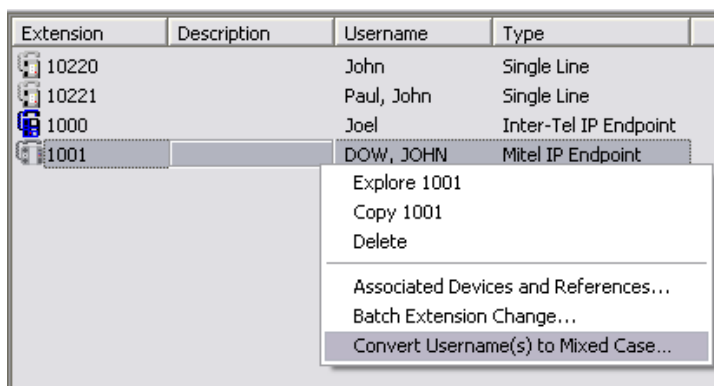
Previous versions of DB Programming allowed only uppercase letters for user names. You can convert uppercase user names to mixed case. When you convert user names to mixed case, DB Programming selects the first letter of the user name to be uppercase and converts the rest of the letters to lowercase. In addition to the first letter of a user name, the mixed case conversion also converts letters following a space or apostrophe to uppercase (for example, "o'neil, abc" is converted to "O'Neil, Abc").

NOTE

When changing user names or extensions, Mitel Model 5330 and 5340 self-labeling programmable buttons may need to be refreshed to display the new data. To reduce the load on the system, the self-labeling buttons do not refresh until 30 seconds after database changes have occurred.

To convert a user name:

1. Select System – Devices and Feature Codes – Endpoints – **(Local)**.
2. In the **Username** column, right-click the user name that you want to convert (for example, DOW, JOHN).
3. Select **Convert Username(s) to Mixed Case** from the list. The user name is converted to mixed case, for example, *Dow, John*, as shown in the following example.



After converting

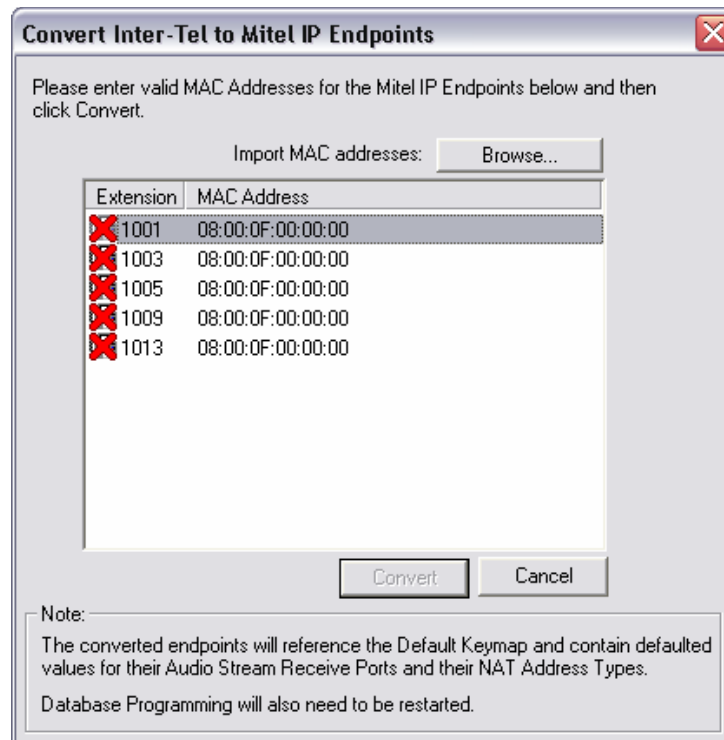
Converting Inter-Tel IP Endpoints to Mitel IP Endpoints

If you have replaced Inter-Tel endpoints with Mitel endpoints, you can convert the settings in DB Programming. The following are default settings for converted endpoints:

- Audio Stream Receive Port (defaults to **50100**)
- NAT Address Type (defaults to **Native**)
- Standard/Alternate Keymap Group (defaults to **Default Keymap**)

To convert Inter-Tel IP endpoints to Mitel IP endpoints:

1. In a local mode session, select System – Devices and Feature Codes – Endpoints – **Local**.
2. Select the extensions that you want to convert, right-click, and then select **Convert to Mitel IP Endpoint**. The following dialog box appears.



3. Before the Convert button becomes enabled, all endpoints in the list must have valid MAC addresses programmed. These MAC addresses must not conflict with one another or with any MAC addresses of devices programmed in the database. If the MAC addresses are invalid, a red 'X' appears. To edit a MAC address, see the following section, "Editing IP Device MAC Addresses" on [page 7-20](#).
4. After all of the MAC addresses are valid, the Convert button becomes enabled. Click **Convert** to initiate the conversion process and restart DB Programming.

Editing IP Device MAC Addresses

Some device settings may prompt you for a MAC address. If prompted, you can edit a single MAC address, or you can edit multiple MAC addresses, as described in the following sections.

Editing a Single MAC Address

To edit a single MAC address:

1. From the dialog box that shows the MAC address (see the example in step 2 on [page 7-19](#)), double-click the MAC address that you want to program. The following dialog box appears.



2. Type the new MAC address, and then click **OK**.

Editing Multiple MAC Addresses

To program batch MAC addresses:

1. From the dialog box that shows the MAC address (see the example in step 2 on [page 7-19](#)), click **Browse** to import the MAC addresses from a `.txt` file. The standard Windows Open dialog box opens. When you import the file, the MAC addresses are read from the top. This means that if there are six MAC addresses in the file, but there are eight endpoints, only the first six will be assigned an address. Also, if there are eight MAC addresses in the file, but only six endpoints, only the first six addresses will be used. All MAC addresses must be unique.
2. Click **OK** to accept the extensions and MAC addresses.

Changing Endpoint Extension Numbers

You can change endpoint extension numbers.

NOTE

When changing user names or extensions, Mitel Model 5330 and 5340 self-labeling programmable buttons may need to be refreshed to display the new data. To reduce the load on the system, the self-labeling buttons do not refresh until 30 seconds after database changes have occurred.

Changing a Single Extension Number

You can change endpoint extension numbers.

To change the endpoint extension number:

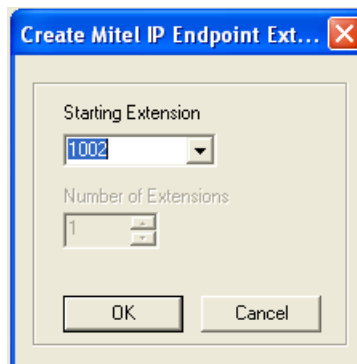
1. Select System – Devices and Feature Codes – **Endpoints**.
2. In the **Extension** column, select the current extension number that you want to change.
3. Select an available extension from the list, or enter the new number in the box. If you change the endpoint extension to match a previously existing unassociated mailbox, a warning window appears informing you that the new extension is the same as an unassociated voice mailbox.
4. Click **OK** to associate the mailbox with the current device.

Changing Multiple Extension Numbers at One Time

You can use the Batch Extension Change feature to change multiple extension numbers at one time.

To use Batch Extension Exchange:

1. Select System – Devices and Feature Codes – **Endpoints**.
2. In the **Extension** column, select the endpoints you want to change (you can use the SHIFT or CTRL key to select more than one endpoint), right-click, and then select **Batch Extension Change**. A dialog box similar to the following appears.



3. Select the number that you want to assign to the first selected endpoint; the other endpoints will be numbered consecutively after this number.
4. Click **OK**. The endpoints are automatically renumbered and resorted in the endpoint list.

Endpoint Flags

You can use endpoint flags to enable or disable endpoint features. Table 7-2 on [page 7-23](#) shows endpoint flags and descriptions. You can program endpoint flags for an individual endpoint, or you can program flags for multiple endpoints.

Programming Flags for Individual Endpoints

To program endpoint flags for an individual endpoint:

1. Select – System – Devices and Feature Codes – **Endpoints**.
2. Select the extension number.
3. Select **Flags**.
4. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
5. Click out of the field or press **ENTER** to save your change. Some flags require you to choose between two settings, such as Hunt Group Remove/Replace. For those flags, select the current value and use the scroll box to select the desired value. Then click out of the field or press **ENTER** to save your change.

Programming Flags for Multiple Endpoints

See Table 7-2 on [page 7-23](#) for endpoint flag descriptions.

To batch program flags for multiple endpoints:

1. Select System – Endpoint-Related Information – **Flags**.
2. Select the flag.
3. Right-click anywhere in the right side of the window (if there is no blank space, press **CTRL + N**). An option box appears.
4. Select **Add To <name of flag> List**. A window appears prompting for the device type to include. The choices are:
 - Digital Endpoint
 - Inter-Tel IP Endpoint
 - Inter-Tel IP Single Line Adapter
 - Mitel IP Softphone
 - Single Line
 - Phantom Device
 - Mitel Endpoint
5. Select the device type, and then click **Next**. The devices with details appear. To view devices in a list only, click **List**.
6. Select the desired endpoints, and then click **Finish**. The selection appears in the appropriate field. To select a series of items, hold down **SHIFT** while selecting the first and last item in the range. To select two or more items that are not consecutive, hold down **CTRL** while selecting the desired items.

Table 7-2. Endpoint Flags

Flag Name	Description
Administrator (Applies only to Inter-Tel and Mitel endpoints.)	An endpoint can be assigned as an administrator to permit use of the administrator feature codes at that endpoint. To assign the endpoint as an administrator endpoint, enable this flag.
All Transient Displays (Not used for single line endpoints.)	When this flag is enabled, it allows all transient call handling displays to appear on the endpoint display. If it is disabled, the CALL TRANSFERRED TO XXX and MESSAGE LEFT FOR XXX displays does not appear. In the default state it is <i>enabled</i> .
Alternate Hold Timer	For users' convenience, the system has two Hold timers: <i>Hold</i> and <i>Hold - Alternate</i> . In the default state, the Alternate timer is set for a longer time period than the Hold timer. However, both timers are programmable. The "Alternate Hold Timer" endpoint flag determines which timer each endpoint uses. If the flag is disabled, the endpoint uses the Hold timer. If it is enabled, the endpoint uses the Alternate timer. In the default state, the flag is <i>disabled</i> .
Alternate Keymap (Inter-Tel and Mitel endpoints only.)	If an alternate keymap is used on the endpoint, it can be enabled through programming or by the endpoint user. This flag shows the current state of the alternate keymap (enabled or disabled). In the default state, the alternate keymap is <i>disabled</i> and the standard keymap is used. The endpoint user can switch keymaps at any time by entering a feature code.
Alternate Transient Display Timer (Not used for single line endpoints.)	This flag, if enabled, allows the length of time that transient displays remain visible to be controlled by the "Digital/IP Alternate Transient Display" timer. If this flag is disabled, transient displays remain visible for 5 seconds. In the default state, it is disabled.
Attendant	An endpoint can be designated as an attendant. It then appears in the list of available endpoints when you are assigning Associated Extensions for other endpoints. <i>If you attempt to remove attendant status from the primary attendant</i> , a warning message appears. The primary attendant can only be changed using the programming options described in "System Forwarding Paths" on page 7-74 . Message centers and Attendant endpoints can serve endpoints located on other nodes. However, because there is not a common database for all nodes, the message center and attendant assignments for the off-node endpoints must be programmed using Associated Extensions for the individual endpoints on the remote nodes. Note that because the local node cannot see the databases of the other nodes, it is up to you to keep track of which attendants and message centers are serving off-node devices. Be careful not to remove those endpoints, leaving the off-node devices without an attendant or message center.
Audio Diagnostics	The Audio Diagnostics flag enables or disables the Audio Diagnostics feature for an endpoint. By default, this flag is enabled. To disable the Audio Diagnostics feature for the endpoint, set this flag to No . For a feature description, see "Audio Diagnostics" on page 16-19 .
Automatic Answer CO or Intercom (Not used for single line endpoints.)	The Automatic Answer features can be enabled so that ringing outside and intercom calls are answered by simply lifting the handset. If automatic answer is disabled, the user must press a button to answer the call. This can also be programmed by the endpoint user. In the default state, automatic access for both IC and CO are enabled.
Caller ID [CLIP] CO or Intercom (Single line endpoints only.)	If the Caller ID [CLIP] IC or CO flags are ON and there are available transmitters on the DSPs, Caller ID [CLIP] information is sent to single line endpoints for intercom and outside calls. By default, these flags are OFF. For more information about Caller ID, DNIS, and ANI requirements for single line endpoints, refer to the System Features chapter in the <i>Mitel 5000 Reference Manual</i> , part number 580.8007.

Table 7-2. Endpoint Flags (Continued)

Flag Name	Description
Caller ID CO or Intercom <i>(Single line endpoints only on built-in SL ports in the chassis.)</i>	<p>Caller ID is only available on the built in ports on the chassis. Caller ID is not available on SLAs or MDPMs. The Advanced CO Interfaces feature requires a software license. Single line endpoints can use ANI or Caller ID [CLID] to receive the calling party's number and name, if available, for outside and intercom calls. Because some single line devices require an extended ring cadence to receive Caller ID [CLID] information, you must first enable the Extended Ring Cadence flag to configure Caller ID [CLID] for IC calls. Without the Extended Ring Cadence set to Yes, the Caller ID [CLID] - IC flag cannot be set.</p> <p>If this flag is enabled, the single line endpoint will display the calling party's information. By default, this flag is disabled.</p>
Camp-On Indications	The tone and display that signal a user when a call has camped on can be enabled or disabled. However, the lamp in the CALL or trunk buttons <i>cannot</i> be disabled. In the default state, the tones are enabled. Hunt group Camp On tones can be disabled without disabling endpoint Camp On tones. See also the Hunt Group Camp-On Audio Indications flag on page 7-25 .
Camp-On to ARS	The endpoint can be permitted to camp on to a trunk when using Automatic Route Selection (ARS), or camp on to ARS can be disabled. In the default state, camp on to ARS is enabled.
CO/IC Reseize <i>(Inter-Tel and Mitel endpoints only.)</i>	The ability to immediately reseize a trunk or intercom channel, after disconnecting from a call, can be enabled. In the default state, it is disabled.
DID/E&M [DDI in Europe] Receive Busy Instead Of Camp On	E&M and DID callers can receive a busy signal, or receive ringback and camp on, when calling a busy endpoint. If this feature is enabled, the caller hears busy signals when the called endpoint is busy, and does not camp on. In the default state, busy tones are disabled and callers hear ringback while camped on to the called endpoint.
Different Alerting Cadence Intercom/CO Call	To allow users to easily differentiate between ringing intercom and outside calls, separate cadences can be enabled. In the default state, the different cadences are enabled.
Different Ringback Cadence Intercom/CO Call	The ringback heard when a user places a call can be different for intercom and outside calls, or both types of calls can use the CO ringback cadence. In the default state, the different cadences are enabled.
Display Outside Party Name <i>(Inter-Tel and Mitel endpoints only.)</i>	If this flag is enabled, the endpoint user can toggle the outside party name and number when connected to a CO call with outside party information. The endpoint user enters the Display Outside Party Name On/Off feature code (379). In addition, the enhanced ring-in displays will provide the user with more information such as both Caller ID [CLID] name and number if available, or tell the user if a Caller ID [CLID] number is blocked or out-of-area. This is an endpoint-only flag. In the default state, this flag is enabled.
Do-Not-Disturb Allowed	This field designates whether the endpoint can be placed in Do-Not-Disturb. In the default state, it is enabled.
Do-Not-Disturb Override <i>(Inter-Tel and Mitel endpoints only.)</i>	The endpoint can be given Do-Not-Disturb override privilege that allows the user to place an intercom call to an endpoint in Do-Not-Disturb. In the default state, it is disabled.
Expanded CO Call Information On Displays <i>(Inter-Tel and Mitel endpoints only.)</i>	This flag determines whether call information (trunk name or caller information) is displayed at the endpoint. If it is enabled, the Outside Call Party Information Has Priority flag (described on page 7-25) determines what is displayed. If it is disabled, the programmed trunk username will appear on the display. In the default state, this flag is enabled.

Table 7-2. Endpoint Flags (Continued)

Flag Name	Description
Extended Ring Cadence (Single line endpoint only.)	Extended ring cadence can be enabled or disabled. The extended setting lengthens the duration of the ring signal to meet the requirements of off-premise extension (OPX) and repeater applications. The default setting is disabled. For more information about the Extended Ring Cadence field, refer to the System Features chapter in the <i>Mitel 5000 Reference Manual</i> , part number 580.8007.
Handsfree On/Off (Not used on single line endpoints.)	The endpoint can be programmed to receive intercom calls handsfree, or handsfree answering can be disabled. This can also be programmed at the endpoint. In the default state, handsfree answering is enabled. IMPORTANT: This flag must be disabled for all SIP endpoints.
Headset Connect Tone	This flag, when enabled, sends a single tone to a headset instead of normal endpoint ring tones when a call is ringing at the endpoint (non-handsfree intercom call, outside call, queue callback, or reminder message). By default the flag is disabled.
Headset On/Off (Inter-Tel and Mitel endpoints only.)	If a headset is used on the endpoint, it can be enabled through programming or by the endpoint user. In the default state, it is disabled.
Hunt Group Remove/Replace	The endpoint Hunt Group Remove/Replace feature can be programmed using this flag or using the feature code at the endpoint. In the default state, this feature is set for replace, which allows the endpoint to receive hunt group calls.
Hunt Group Camp-On Audio Indications	The tone that signals a hunt group member when a call has camped on to the hunt group can be enabled or disabled. (However, the camp-on display and lamp in the CALL or trunk buttons cannot be disabled.) In the default state, the tones are enabled. If all endpoint camp-on tones are disabled using the Camp-On Indications flag, hunt group camp-on tone is disabled regardless of the Hunt Group Camp-On Audio Indications flag setting.
Immediate OHVA Transmit (Inter-Tel non-IP endpoints only)	Determines if the endpoint has immediate Off-Hook Voice Announce capability enabled. If it is not enabled, the OHVA call does not go through until the Off-Hook Voice Announce Screening timer expires. In the default state, this field is disabled. Not supported in IP endpoints.
Manual Forward to Public Network	When disabled, this flag prevents the endpoint from manually forwarding calls to the public network. This prevents users from calling in to a local endpoint and reaching toll numbers via forwarding. In the default state it is enabled.
OHVA Receive/Transmit (The OHVA Receive prompt does not apply to IP devices.)	Any non-IP device can be programmed to place Off-Hook Voice Announce calls. Digital endpoints can be programmed to receive Off-Hook Voice Announce calls. In the default state, receive and transmit are disabled. Note that the system-wide flag must also be enabled to use the feature.
OPX Gain Levels (T1 OPX single line endpoint and IP SLAs only.)	When a single-line circuit is used as an off-premises extension, this field can be enabled to set receive and transmit gain levels to better suit the OPX application. In the default state, OPX gain levels are disabled (the gain levels are set for on-premises use). <i>Although you can enable this flag for all single lines, the flag is ignored unless the single line set is a T1 OPX.</i>
Outside Party Call Information Has Priority (Not used on single line endpoints.)	If the Expanded CO Call Information flag is enabled (see page 7-22), this flag determines what information is displayed at the endpoint. If enabled, any call that is received on a trunk that provides outside caller information, Caller ID (CLID) or ANI, will be identified on the endpoint display with the caller information. If disabled, the display will show the DID or DNIS information for the call (if available). In the default state, it is enabled.

Chapter 7: Endpoints and Devices

Endpoint Flags

Table 7-2. Endpoint Flags (Continued)

Flag Name	Description
Page Mode (<i>Inter-Tel and Mitel endpoints only.</i>)	Pages to the endpoint can be enabled or disabled through programming or by the endpoint user (page remove/replace). In the default state, pages are enabled.
Propagate Original Caller ID on Transfer (For endpoints)	When enabled, if the endpoint is on a call with an outside trunk that had caller ID information, when the endpoint performs a transfer back to the PSTN, the endpoint will propagate the caller ID. To propagate the caller ID to the PSTN, the eventual trunk must be ISDN and the "Propagate Original Caller ID" flag in its CO trunk group must be set to Yes.
Receive Busy Instead of Do-Not-Disturb	The tone that a caller hears when an endpoint is in Do-Not-Disturb can be a busy signal or a Do-Not-Disturb signal. If this feature is enabled, the caller hears busy signals when the endpoint is in Do-Not-Disturb, but the caller cannot camp on. In the default state, busy tones are disabled.
Redial Mode	Endpoint users can use dialed or saved redial modes. This field can be programmed using this flag only, it cannot be changed by the endpoint user. In the default state, the endpoints are set for dialed mode.
Ring Intercom Always On/Off	When this feature is enabled, all calls placed to endpoints from this endpoint are received as private calls. The feature can be enabled or disabled through programming or by the endpoint user. In the default state, this feature is disabled.
Send Alert Burst To Headset (<i>Inter-Tel and Mitel endpoints only.</i>)	Some headsets have a power-saver mode that disables the headphone after a period of silence. To prevent these headsets from missing portions of incoming calls, enabling this flag allows the endpoint to generate a tone that activates the headset before connecting to an incoming call. In the default state, it is disabled.
Send T1 OPX Disconnect Flash (<i>T1 OPX Single-line endpoint only.</i>)	This flag, when enabled, sends a proprietary disconnect signal from the T1 OPX to the loop start trunk. (The "A" bit is toggled high for the duration of the SL Disconnect Flash Duration timer.) At default, this flag is disabled. Although you can enable this flag for all single lines, the flag is ignored unless the single-line set is a T1 OPX. This flag does not affect T1 channels configured for Loop Start. Therefore, a Mitel system can be on the receiving end with T1 Loop Start channels and will recognize the disconnect. However, it cannot send the disconnect.
Standard Tone Frequencies	The busy tones and dial tones can be pure system tones or they can be changed to more closely match the service provider standard tones. For more information about ringing signals, refer to the System Features chapter in the <i>Mitel 5000 Reference Manual</i> , part number 580.8007. In the default state, standard tones are enabled, which allows standard service provider-type tones.
System Forwarding	When this field is enabled, calls to the endpoint follow the system forwarding path that is programmed for the endpoint (if any). This field can be enabled in the database or at the endpoint. In the default state, it is enabled.
Transfer-To-Connect Allowed (<i>Inter-Tel and Mitel endpoints only.</i>)	If this flag is enabled, an announced transfer call (including an announced transfer from voice mail) connects immediately with the destination once the transferring party hangs up. (If the flag is disabled, the recipient must press a CALL button to answer the transferred call). If the user has a headset enabled, or if the endpoint user picks up the handset for the initial call and the transferring party disconnects, the transferred party hears a single tone and is then immediately connected without any further action from the endpoint user. Calls do not automatically connect in handsfree speakerphone mode; the user must press a CALL button to answer the call. This flag is disabled by default.
Transient Call Indication On Call Answer (<i>Inter-Tel and Mitel endpoints only.</i>)	This flag determines whether the endpoint user sees a call indication display when answering a call by pressing a secondary extension button or by reverse transferring. If enabled, the display indicates if the call was ringing, recalling, transferred, or holding at the other endpoint. In the default state, it is enabled.

Keymaps

You can view and program endpoint and Direct Station Select (DSS) keymaps.

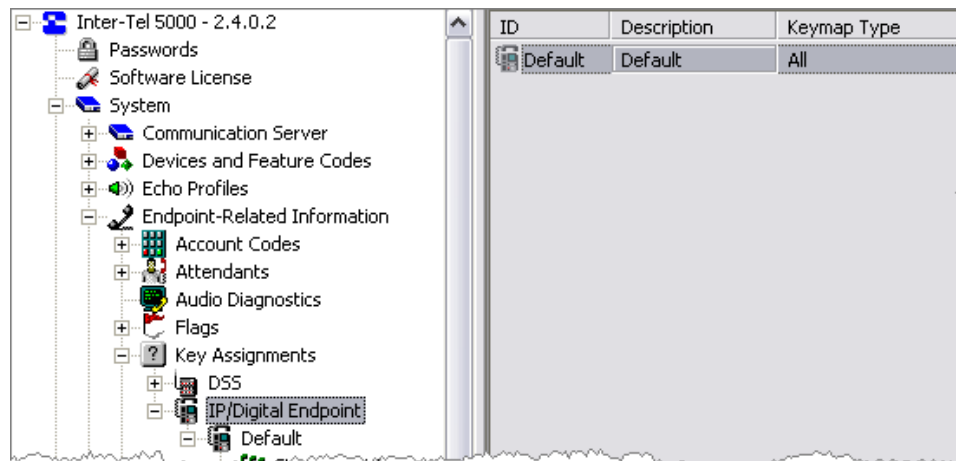
The Default keymap contains the default key programming for all IP/digital endpoint models. You cannot delete or edit key assignments in the Default keymap. All new keymaps created in DB Programming have a copy of the Default keymap keys.

For databases converted or upgraded to a new DB Programming version, existing keymaps are preserved, but their IDs are incremented by 1. Existing keymaps are assigned a Default keymap type, and changes to this field are saved. Existing endpoints retain their keymap association, and any new endpoints are created with reference to the Default keymap. For more information about the Database Converter Utility, see [page 14-23](#).

In a default database, the Default keymap is the only keymap programmed. Endpoints in the default database and any new endpoints are created with reference to the Default keymap.

[Figure 7-3](#) shows the main IP/Digital Endpoint keymap list for the default database.

Figure 7-3. Default Keymap



ID	Description	Keymap Type
Default	Default	All

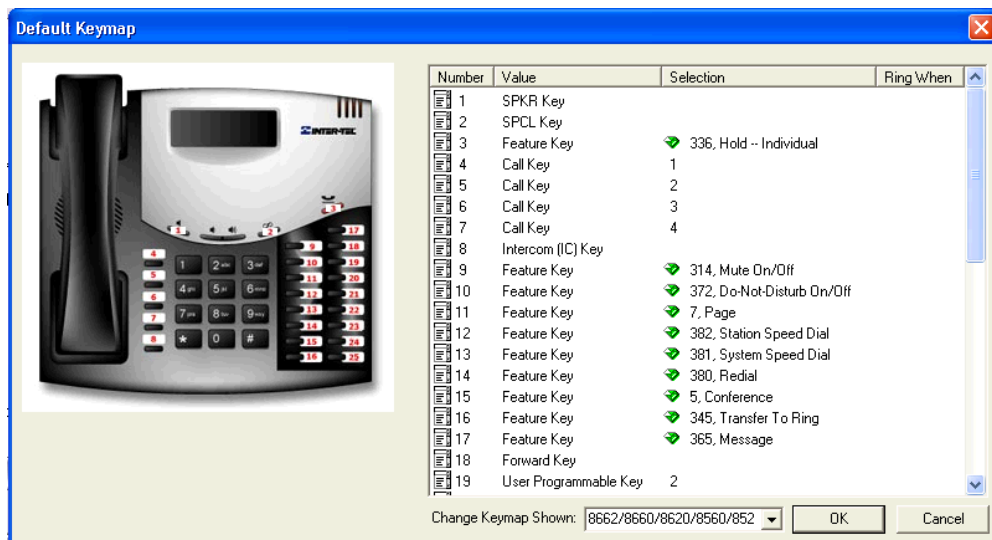
For the Default keymap, the Description, Keymap Type, and User Programmable Keys are read-only. However, you can move IP/digital endpoints to and from the Standard and Alternate Lists.

Viewing Default Keymaps

The Default keymap contains the default key programming for all IP/digital endpoint models. You cannot delete or edit key assignments in the Default keymap. All new keymaps created in DB Programming have a copy of the Default keymap keys.

To view a default endpoint keymap:

1. Do one of the following:
 - To view the default keymap available to a particular endpoint group: Select System – Endpoint-Related Information – Key Assignments – <endpoint type> – **Default**.
 - To view the keymap assigned to a particular endpoint: Select System – Devices and Feature Codes – Endpoints – (Local) – <extension> – **Keymaps**.
2. In the **Keymap** column, double-click **Default**.
3. Double-click **Keymap Type**. The selected keymap appears, as shown in the following example.



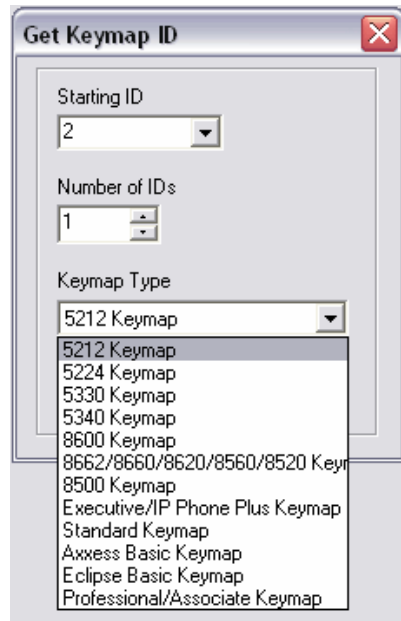
4. From the **Change Keymap Shown** list, select the endpoint type that you want to view. The endpoint image with key assignments appears. The endpoint image is view only—there are no operable controls in the image. See “Keymap Number Column” on [page 7-30](#) for more information about the Number, Value, Selection, and Ring When columns shown in the right pane.

Adding New Keymaps

You can add new keymaps and assign them as standard or alternate endpoint keymaps to a particular endpoint type.

To add a keymap to the IP/Digital Endpoint List:

1. Select System – Endpoint-Related Information – Key Assignments – **IP/Digital Endpoint**.
2. Right click in the right pane, and then click **Add to IP/Digital Endpoint List**. The following dialog box appears.



3. From the Starting ID list, select the starting ID (2-26) and the number of IDs. You can create up to 25 keymaps.
4. From the Number of IDs list, select the number of keymaps you are adding.
5. From the **Keymap Type** list, select a keymap type.
6. Click **OK** to save the changes.

Programming Endpoint Keymaps

Remember the following when programming keymaps:

- Keymaps can only be used for the endpoint type and model for which they are programmed. For example, you cannot use a digital endpoint keymap for an IP endpoint, and you cannot use an Inter-Tel endpoint keymap for a Mitel endpoint.
- Key assignments within a keymap are common to all endpoint types in that map. Modifying a button changes that button assignment for **all** endpoints assigned to that map, regardless of endpoint type. For example, if the top left button is changed to a user-programmable button for six-line display and Executive Display endpoints in Keyset Map Group 1, the corresponding button is also user-programmable on all other endpoints in Keyset Map Group 1.
- Users who have Standard and Alternate keymaps want to have their user-programmable buttons in the same positions in both keymaps. That way their user-programmable button locations do not change when they switch keymaps. Also, if a fixed feature button is created for the Switch Keymap feature code, make sure it is in the same position in both keymaps.

Keymap Number Column

The keymap number shown in the right pane is the number that corresponds to the red number in the image. It is not programmable. It simply associates the list control item with the key.

Keymap Value Column

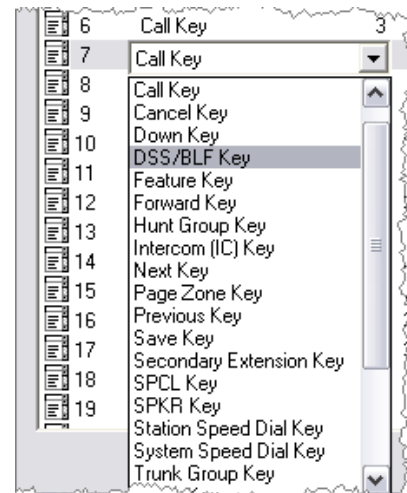
The keymap value shown in the right pane is the current key type assigned to the key. You can program the keymap value.

To change the key type:

1. Click the **Value** field. A list box appears as shown below.



2. Click again to see the list of choices, as shown at right.



3. Click the new key type, and then click **OK**. The new key type appears. When you change the value, the Selection and Ring When columns are reset, depending on the new value. For a System Speed Dial Key, the Selection is set to the first System Speed Dial Number. For a Hunt Group Key, it is set to the first hunt group. The Ring When column is inoperable for all key types (values) except the Secondary Extension. For more information about key types, see “Associated Extensions” on [page 7-51](#).

Keymap Selection Column

The Selection column includes additional information for the following key types:

- “Call Key” below
- “User Programmable Key” below
- “Station Speed Dial Key” on [page 7-32](#)
- “System Speed Dial Key” on [page 7-32](#)
- “Device Key” on [page 7-35](#)

For all other key types, the Selection column is blank and inoperable.

- **Call Key:** A call key number is shown. This is assigned automatically and is not programmable. Call keys are always numbered sequentially in the order created. If one is removed, the gap is closed by renumbering those with higher numbers. A new Call Key is always assigned the next available number.

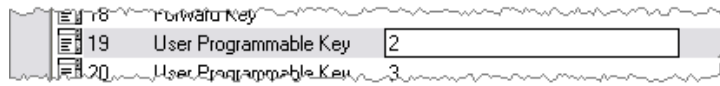
To the end user, the first non-IC call is associated with Call Key 1. If another non-IC call is made or received while the first call is still active, the second call is associated with Call Key 2. The next call is associated with Call Key 3, and so on. As soon as the first non-IC call is completed, Call Key 1 becomes available and is associated with the next non-IC call.

Because the Call Keys are used in the manner described above, if the key assignments are changed, create any new Call Keys in a thoughtful order, such that the numbering flows with the key positions.

- **User Programmable Key:** A key number is shown. The key is programmable, with a range of 1–45, and it always defaults to 1 when a new User Programmable Key is created. (You can program two User Programmable Keys with the same number, but this is not recommended.) The numbers correspond to the numbers that appear in two other folders: the “Endpoint User Programmable Keys” folder and the keymap “User Programmable Keys” folder.
 - In the System\Devices and Feature Codes\Endpoints\<extension>**Programmable Keys** folder, User Programmable Keys 1–45 can be programmed differently for each individual endpoint. These keys can also be programmed from the endpoint using a feature code. User Programmable Keys must be programmed and assigned with numbers in the keymap associated with the endpoint. The number assignment, 1–45, allows the key assignment made in the keymap to be associated with the programming in the Endpoint User Programmable Keys Folder.
 - In the System\Endpoint-Related Information\Key Assignments\IP/Digital Endpoint\<keymap ID>**User Programmable Keys** folder, defaults for these keys can be programmed. Default programming is included in the Default keymap, and changes can be made after keymaps are created. The programming in this folder is associated with the keymap. For endpoints associated with the keymap, the programming for those keys can be copied to the endpoint. This capability allows for newly created endpoints to get the default programming for these keys. It also allows for the programming for these keys at the endpoint to be reset to match the keymap. (This is accomplished through the shortcut menu in a Keymap folder or in the Standard List or Alternate List folder of a keymap.)

To edit the User Programmable Key number:

- 1.) Click the number in the Selection column. An edit box appears, as shown below.



- 2.) Enter the new number (1–45), and then click **OK**.

- **Station Speed Dial Key:** This number corresponds to the digit on the endpoint that is used to store or access this Station Speed Dial number. You can store up to 10 Station Speed Dial numbers for each endpoint, using digits 0–9. Programming a key to be a Station Speed Dial Key provides for station speed dial through a single key press. (Otherwise, the user dials the Station Speed Dial feature code, and then presses a digit 0–9 to indicate which Station Speed Dial Number to dial.) Station Speed Dial number programming must be done separately, using DB Programming or at the endpoint itself, by the Program Station Speed Dial feature code.

This number defaults to “0” when a Station Speed Dial key is created. You can program two Station Speed Dial Keys with the same number, but this is not recommended.

To edit the number:

- 1.) Click the number in the **Selection** column.
 - 2.) Type or select the new Station Speed Dial number, and then click **OK**.
- **System Speed Dial Key:** A System Speed Dial ID is shown, along with the programmed number, if any. When a new System Speed Dial Key is created, the ID is set to **0**. You can program two System Speed Dial Keys with the same ID, but it is not recommended.

There are three ways to edit the ID: (1) type the ID manually, (2) use a Selection Box, or (3) use a Selection Wizard. These methods are explained in the following pages.

To type the ID manually:

- 1.) Click the **Selection** column that you want to edit. An edit box appears, as shown below.



- 2.) Type the ID (000–999), and then click **OK**. If the ID entered corresponds to an existing System Speed Dial Number, when you click away and then click **OK**, the change is completed.

If the ID entered does not correspond to an existing System Speed Dial Number, an empty Select an Item box appears, as shown below.



- 3.) Click **Cancel**, and then try again. The title of this box has changed from “Select a Device” to “Select an Item” to describe the functionality better.

To use a Selection Box:

- 1.) Click the **Selection** column that you want to edit. An edit box appears, as shown below.



- 2.) Click **OK**. When the edit box is empty, the Select an Item box appears showing all of the available System Speed Dial numbers for the key.



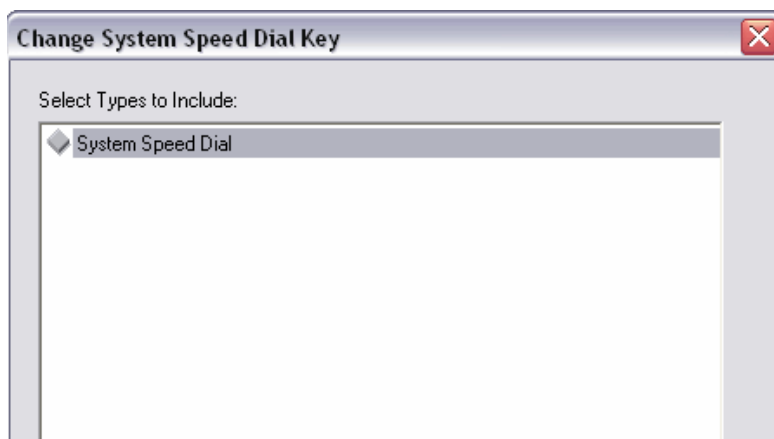
- 3.) Select the number that you want, and then click **OK**.

To use a Selection Wizard:

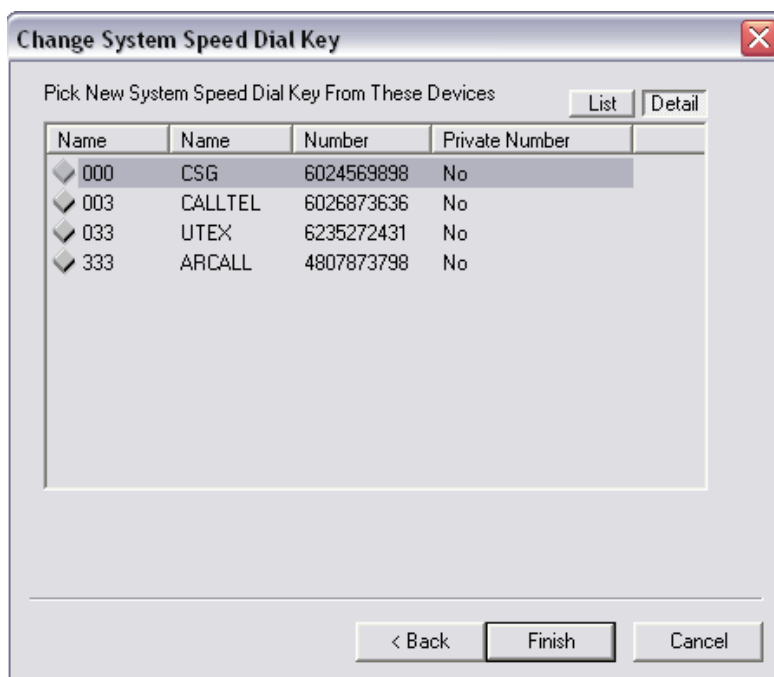
- 1.) Right-click the **System Speed Dial Key**, and then select **Change Selection**.



A Selection Wizard appears, presenting the available types of items that can be associated with the key.



- 2.) Click **Next** to accept the only choice of System Speed Dial. All of the available System Speed Dial numbers for the field appear in the box.



- 3.) Click the **System Speed Dial Number** that you want to edit, and click **Finish**. If a new System Speed Dial Number was selected, it now appears in the Selection column in the list control. Otherwise, the original number remains.

- **Device Key:** A “Device” key is any key type that is associated with a device (for example, DSS/BLF Key, Hunt Group Key, Trunk Key, Page Zone Key, etc.) For a “Device” key, the Selection column contains the extension and description (if any) of the associated device.

When a key of one of these types is created, a default choice is always stored in the Selection column. This is always the first device found in the database appropriate for the type of key. For example, for a Feature Key, it is 0, Call Attendant. For a Page Zone Key, it is the first Page Zone. For a Trunk Group Key, it is the first CO Trunk Group, and so on.

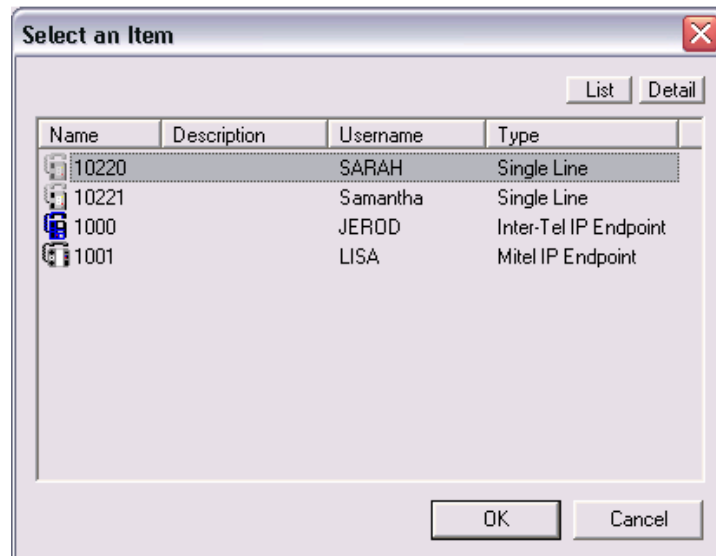
There are three ways to edit the ID: (1) type the extension manually, (2) use a Selection Box, or (3) use a Selection Wizard. These methods are explained below.

To type the extension manually:

- 1.) Click the **Selection** column that you want to edit. An edit box appears, as shown below.



- 2.) Type the extension that you want, and then click **OK**. If a complete, valid extension is entered, the change is completed, the Popup Edit Box is removed, and the extension is shown, along with the device description (if any).
- 3.) If the extension is incomplete or invalid, the Select an Item box appears as shown below.



For an incomplete extension, the box contains only the extensions of devices appropriate for the key that begins with the digits entered. For example, if you are editing a DSS/BLF Key Selection and enter “1” and then click **OK**, the Selection Box contains only devices with extensions beginning with “1” that can be placed under a DSS/BLF Key. You can then find and select the device that you want, and then click **OK**.

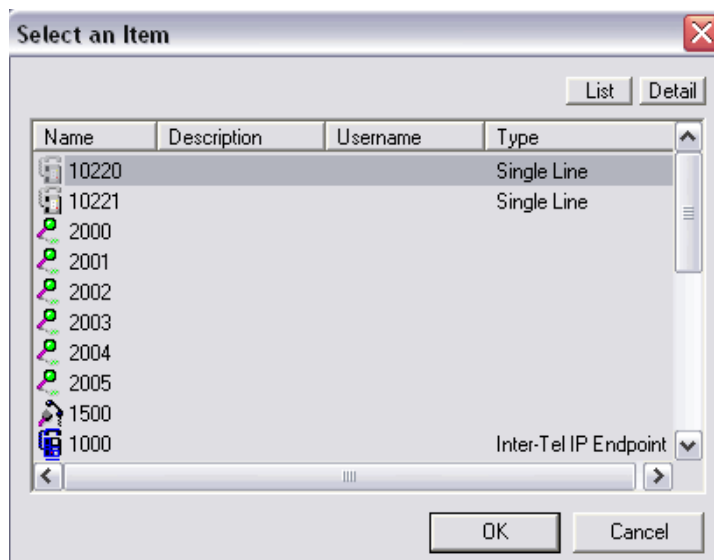
If the entered digits do not correspond to the beginning digits of any devices of the type(s) associated with the key type, the box clears. Click **Cancel**, and then try again.

To use a Selection Box:

- 1.) Click the **Selection** column that you want to edit. An edit box appears, as shown below.



- 2.) Click **OK**. When the edit box is empty, a Select an Item box appears showing all of the available endpoints, voice mail applications, hunt groups, and so on. For a Feature Key, all of the feature codes are shown. For a Hunt Group Key, just the hunt groups are shown, and so on.



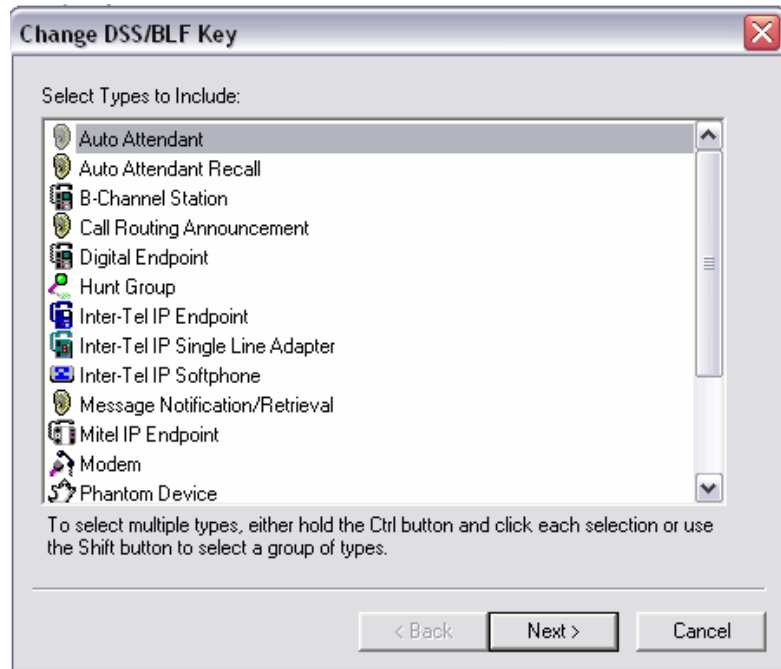
- 3.) Select the device that you want, and then click **OK**.

To use a Selection Wizard:

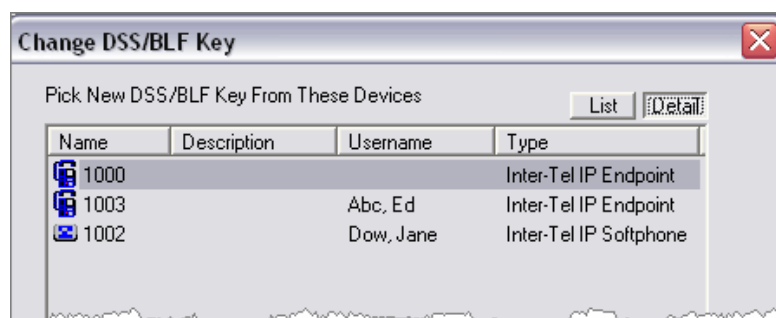
- 1.) Right-click the **DSS/BLF Key**, and then select **Change Selection**.



A Selection Wizard appears, presenting the available types of items that can be associated with the key.



Select the device types, and then click **Next**. A list of selected device types appears in the box. The example below illustrates when the Inter-Tel IP Endpoint and Inter-Tel IP Softphone types are selected.

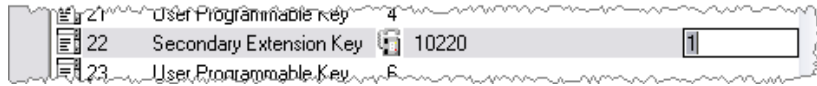


- 2.) Select the device you want, and then click **Finish**.

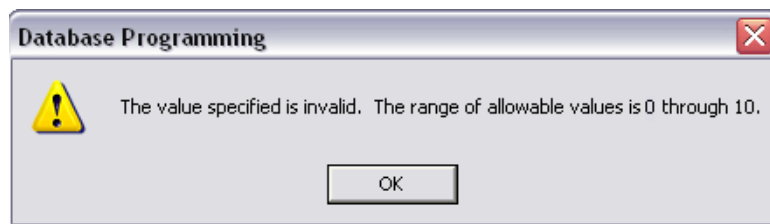
- **Ring When:** This field is blank and inoperable for all key types except for a Secondary Extension Key. When a key of that type is created, the Ring When column defaults to “1.” It can be set to any value from 0 to 10. The value indicates how many additional calls need to be ringing at the endpoint before the assigned secondary extension begins to ring. Setting the value to 0 turns off the ring indicator for the programmed key.

To edit this column:

- 1.) Click the number in the **Ring When** column. An edit box appears, as shown below.



- 2.) Edit the number as needed, and then click **OK**. Only digits (up to 10) are accepted in this box. If the number typed is out of range, the following message box appears, and the change is ignored.



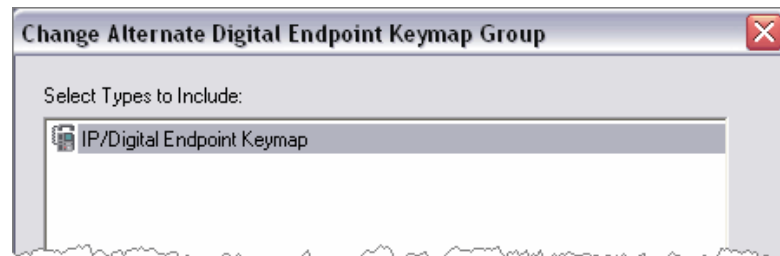
Selecting Standard or Alternate Keymaps

All digital and IP endpoints created in DB Programming are assigned to the Default keymap. To associate an endpoint with another keymap, either browse to the Keymap subfolder of the endpoint, or browse to the Standard or Alternate List subfolder of the keymap that you want to edit and move the endpoints to this folder using the shortcut menu.

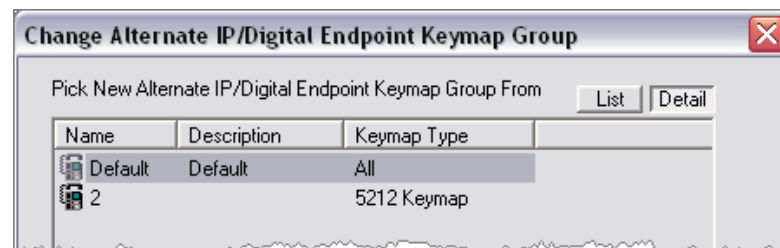
Because DB Programming differentiates between Mitel IP endpoints and Inter-Tel IP endpoints, only Mitel IP endpoints may be moved to a keymap that is programmed for a Mitel IP endpoint keymap type. Likewise, only Inter-Tel IP endpoints or digital endpoints may be moved to a keymap programmed for an Inter-Tel endpoint keymap type. When the keymap type is changed, either by moving endpoints from one list to another or by changing the keymap reference in the endpoint subfolder, the system prompts you to default the Programmable Keys of the endpoint to match the User Programmable Keys of the keymap. If you click **No**, the Programmable Keys of the endpoint(s) remain the same. If you click **Yes**, the User Programmable Keys of the keymap that the endpoint has been changed are copied over the Programmable Keys of the endpoint(s). This is the same functionality as the shortcut menu item "Default Selected User Keys" in the Standard/Alternate List folders.

To select a keymap for an endpoint:

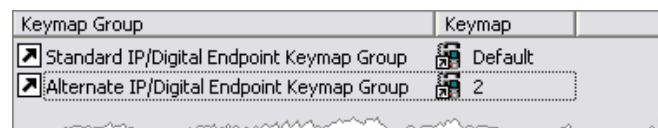
1. Select System – Devices and Feature Codes – Endpoints – (Local) – <extension> – **Keymaps**.
2. Right-click either Standard or Alternate IP/Digital Endpoint Keymap Group for the map you want to change, and then click **Change Standard/Alternate Digital Endpoint Keymap Group**. A dialog box similar to the one below appears, prompting you to select the type of keymap to include.



3. Select the appropriate keymap, and then click **Next**. The list of keymaps appears. To view keymap details, click **Detail**.



4. Highlight the keymap that you want to use, and then click **Finish**. The selected keymap appears in the Keymap column.

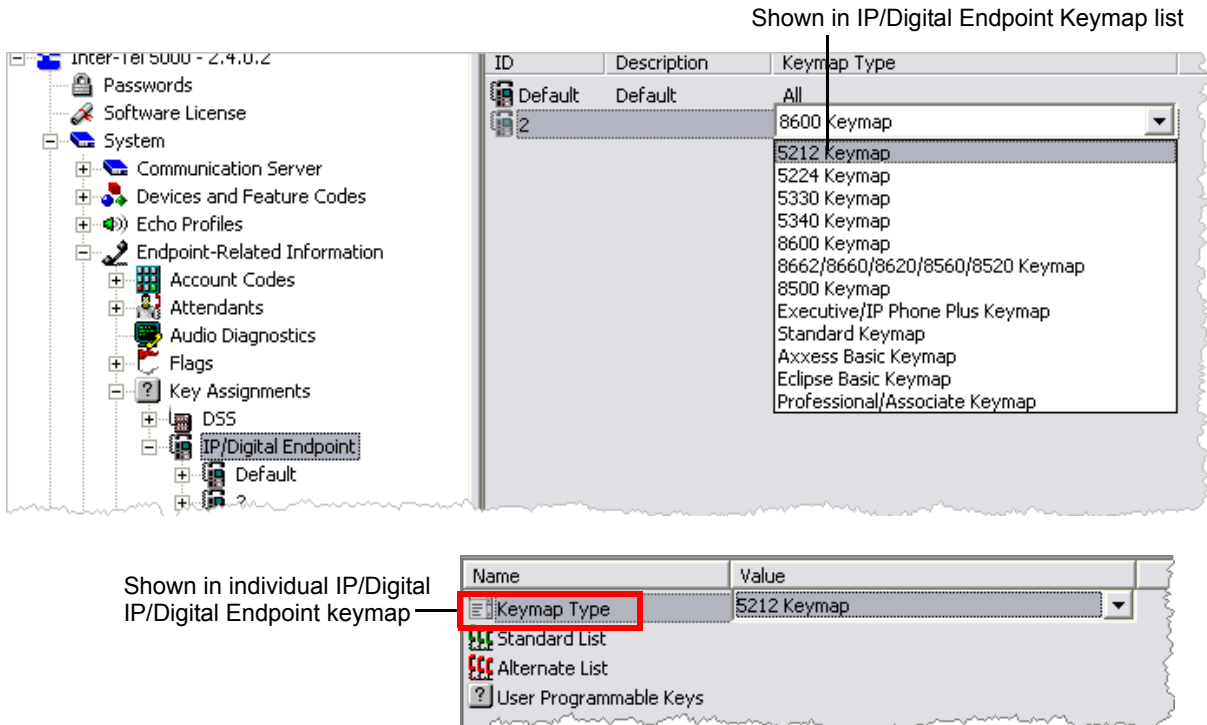


Changing Keymap Types

You cannot change default keymap types. When you change a keymap, the keymap key assignments themselves do **not** change.

Each keymap must have an associated “Keymap Type.” The Keymap Type column is in the IP/Digital Endpoint Keymap list and the individual IP/Digital Endpoint keymap folder. You can program the keymap type from either folder, as shown in [Figure 7-4](#).

Figure 7-4. Keymap Type Column



To change the Keymap type:

1. Do one of the following:
 - Select System – Endpoint-Related Information – Key Assignments – IP/Digital Endpoint – **<keymap>**.
 - Select System – Devices and Feature Codes – Endpoints – (Local) – <endpoint> – Keymaps – **Alternate** (or **Standard**) **IP/Digital Endpoint Keymap Group**.
2. Select the keymap box, which is either the Keymap Type column field in the main IP/Digital Endpoint keymap list or the Value column field in the individual IP/Digital Endpoint keymap folder.
3. From the **Keymap Type** list, select the keymap type. If the keymap type is changed from a Mitel model to an Inter-Tel model or vice versa, a warning message appears indicating that any endpoints referencing that keymap will reference the Default keymap instead. Click **Yes** to continue.

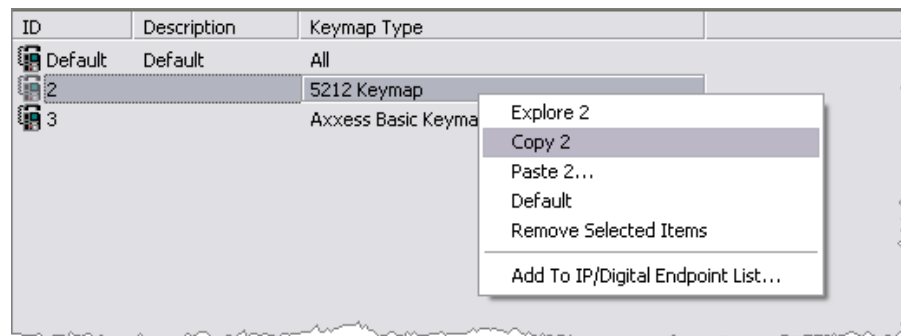
Copying and Pasting Keymaps

You can copy and paste keymaps. Remember the following when copying and pasting keymaps:

- The Description and the Standard and Alternate Lists are not copied or pasted with a keymap.
- The Default keymap is not a valid paste location. Attempting to paste to the Default keymap displays an error message.
- A keymap for an Inter-Tel keymap type may not be copied or pasted to a keymap with a keymap type for a Mitel Endpoint model and vice versa. If you attempt to copy or paste a different model keymap, an error message appears.

To copy and paste the entire keymap:

1. Right-click the keymap that you want to copy, and then select **Copy**. When selected, the database copies the keymap type and key assignments (including the User Programmable Keys) from that keymap to the Clipboard.



2. Select the keymap to which you are pasting.
3. Right-click, and then select **Paste**. The Paste option is available only when the Clipboard holds a copy of a keymap and you right-click on a keymap in the Keymaps folder. If a group of keymaps is selected, and you right-click in the group, the type and key assignments are pasted into each selected keymap. Otherwise, the type and key assignments are pasted into the single keymap.

If you attempt to paste a keymap of one type onto a keymap of another type, a confirmation message appears. Click **Yes** to confirm.

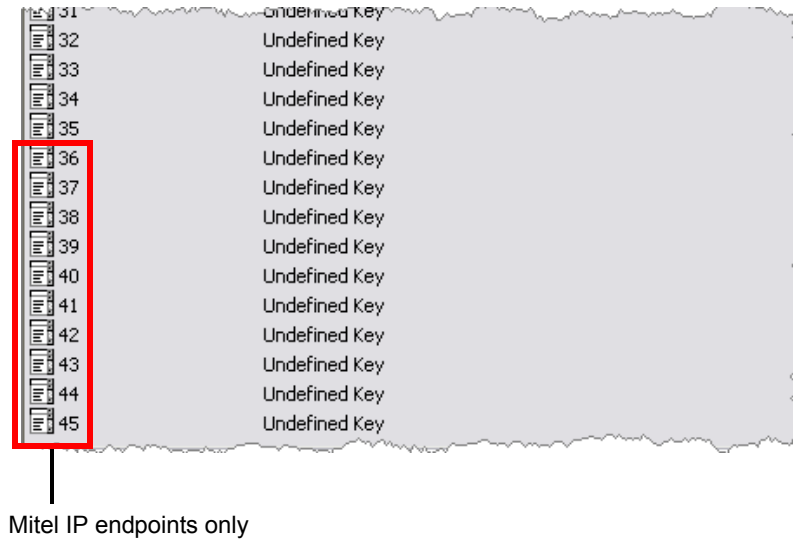
To return a keymap to its default key assignments:

1. Right-click the keymap that you want to modify, and then select **Default**.
2. When the confirmation message appears, click **Yes** to default both the key assignments and the User Programmable Keys. Click **No** if defaulting only the key assignments. Note that the Description, Keymap Type, and Standard and Alternate Lists will not be changed.

Programming Endpoint Keymap Buttons

All Programmable Key lists have 45 keys. Keys 36–45, as shown in [Figure 7-5](#), are used for Mitel IP endpoints only.

Figure 7-5. *Programmable Keys*



You can change the programmable keys assigned to a keymap for all endpoints assigned to the keymap, or you can edit the programmable keys for a particular endpoint.

To program endpoint keys:

1. Do one of the following:

To program keys for a keymap:

Select – System – Endpoint-Related Information – Key Assignments – IP/Digital Endpoint – <endpoint keymap> – **User Programmable Keys**.

To program keys for an individual endpoint:

Select – System – Devices and Feature Codes – Endpoints – (Local) – <extension> – **Programmable Keys**.

2. *To change the Key Type, Selection, or Ring When options, do the following:*
 - **Key Type:** Select the current Key Type for the button and scroll through the drop-down list box until the desired key type is selected.
 - **Selection:** The Selection options required for each of the key types are as follows:
 - **DSS/BLF Key:** Select the circuit or extension number of the station that will appear under the selected DSS/BLF button.
 - **Feature Key:** Enter the feature code that is activated when the button is pressed.
 - **Hunt Group Key:** Select the pilot number of the desired hunt group.
 - **Intercom (IC) Key:** No further programming is necessary. This button is used for seizing an intercom channel or answering a waiting intercom call.
 - **Page Zone Key:** Select the page zone 0–9 that will be used by selecting the page zone access code 9600–9609.
 - **Secondary Extension Key:** Select the primary endpoint that will be associated with this secondary extension button.
 - **Station Speed Dial Key:** Select the Station Speed Dial location (0–9) that will be assigned.
 - **System Speed Dial Key:** Select the System Speed Dial location (000–999) that will be assigned.
 - **Trunk Key:** Select the individual trunk that will be selected when this button is pressed.
 - **Trunk Group Key:** Select the trunk group that will be selected when this button is pressed.
 - **Undefined Key:** No further programming is necessary. This button can be programmed by the user.

To program the selection, right-click the Selection value, and then do the following:

- 1.) Select **Change Selection**. A window appears prompting for the type to include.
 - 2.) Select the type (feature code, endpoint, and so on), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
 - 3.) Select the appropriate item, and then click **Finish**. The selection appears in the Selection field.
- **Ring When:** (Secondary Extensions only). Allows the endpoint to receive a burst of ringing when a certain number of calls are present at a primary endpoint, and at least one call is ringing or camped on. The ring burst repeats periodically as long as the programmed number of calls are present at a primary endpoint. The period of repetition is determined by the Digital/IP Secondary Extension Key Alerting Tone timer. If this field is set to 0, the secondary endpoint never rings.

To set this number:

- 1.) Select the current Value and scroll to or enter the new value in the box.
- 2.) Click out of the field or press **ENTER** to save your change.

Programming DSS Keymaps

When you double-click a specific DSS keymap, you have the following options:

- **DSS Map:** The following DSS options are available:
 - *8450 DSS map:* Corresponds to the 50-key DSS Unit.
 - *60-key DSS Keymap 6-row and 12-row Model options:* correspond to the 60-key DSS Unit.
- **DSS Endpoint List:** When you double-click **Endpoint List**, you see the endpoints that are currently assigned to the DSS keymap. See “Programming DSS Endpoint Lists” on [page 7-48](#).

You can automatically or manually populate a keymap, as described in the following sections.

Automatically Populating DSS Keymaps

You can automatically populate DSS keymaps with system endpoints.

To automatically populate the DSS or keymap:

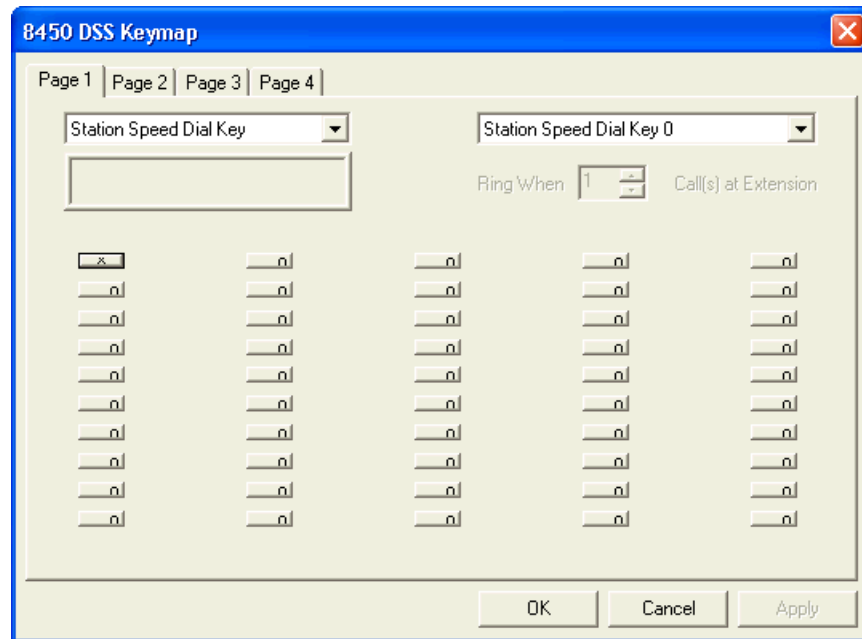
1. Do one of the following:
 - Select System – Endpoint-Related Information – Key Assignments – DSS – **<DSS number>**.
 - Select System – Devices and Feature Codes – Endpoints – (Local) – **<extension>** – Keymaps – DSS Keymap Group – **DSS Keymap**.
2. Right-click the DSS keymap, and then select **Populate DSS Keymap**. A message appears notifying you that DB Programming will automatically populate the keymap with the system endpoints. To do this, the system starts at the lowest extension value and populates every button in ascending order. If there are more DSS buttons than extensions, any buttons not assigned an extension are changed to “Undefined.” If you populate the keymap when there are no extensions available, all buttons are changed to “Undefined.”

Manually Populating DSS Keymaps

You can populate the DSS keymap with selected devices.

To manually populate the keymap:

1. Do one of the following:
 - Select System – Endpoint-Related Information – Key Assignments – DSS – <**DSS number**>.
 - Select System – Devices and Feature Codes – Endpoints – Local – <extension> – Keymaps – DSS Keymap Group – **DSS Keymap**.
2. Double-click **DSS Keymap** to view an illustration of the device, as shown in the following example. DSS button types are described in Table 7-3 on [page 7-46](#).



The DSS keymap shows four pages of buttons—one for each device that can be connected to the endpoint. To see the buttons on a particular page, select the tab at the top of the page.

3. Do one of the following:
 - *If you are changing a button requiring additional information, such as a feature code, extension number, and so on:*
 - a.) Click the button for which you want to assign a new value. A list window appears.
 - b.) Select the device type from list, and then select **Next**.
 - c.) Highlight the new value from the available list, and then select **Finish**. The new value appears in the box below the Key Type box.
 - *If you are changing a button that does not require additional information:* Use the arrow keys on your keyboard to move around the keymap. Once you have selected the desired button (selected buttons will have a line with an “x” in the center), click **Key Type** to scroll to the new key type. If you change the button type to one requiring additional assignments (for example, extension, hunt group, and so on), any previously programmed information for that button type remains. To change this information, you must click the button again and follow the directions detailed previously.

NOTE

Secondary extension buttons also have an additional option, “Ring When _ Calls At Extension. This option allows the station to receive a burst of ringing when a certain number of calls are present at a primary station, and at least one call is ringing or camped on. If this option is set to 0, **the secondary station will never receive the burst of ringing**. To set this number, select the current value and scroll to or enter the new value in the box. Click out of the field or press **ENTER** to save your change.

Types of keys, or buttons, and the selections that are required are described in [Table 7-3](#).

Table 7-3. DSS Button Types and Descriptions

Key	Description
Accept Key	No further programming is necessary. This button is used to accept an entry when using numeric mode. This button type is <i>not</i> required for digital endpoints. On digital endpoints you activate the VOLUME function by pressing both arrows at once
Call Key	The next CALL button number is automatically selected.
Cancel Key	No further programming is necessary. This button will be used to cancel a feature or cancel an entry when in numeric mode.
Down Key	No further programming is necessary. This button can be used to scroll backward through displays. When the endpoint is idle, it can be used for adjusting volume, in place of the VOLUME button. This button type is <i>not</i> required for digital endpoints. On digital endpoints you use the VOLUME DOWN button.
DSS/BLF Key	Select the circuit or extension number of the endpoint that appears under the selected DSS/BLF button. If this is assigned to an off-node device, the button can be used for dialing the endpoint, but the lamp will not show endpoint status (no BLF).
Feature Key	Select the feature code that will be entered when this button is pressed.
Forward Key	Select the desired Call Forward feature code.
Hunt Group Key	Select the pilot number of the desired hunt group.
Intercom (IC) Key	No further programming is necessary. This button will be used for seizing an intercom channel or answering a waiting intercom call.
Next Key	This button type is not required for digital endpoints. No further programming is necessary.
Page Zone Key	Select the page zone 0–9 that will be used by selecting the page zone access code 9600–9609.

Table 7-3. DSS Button Types and Descriptions (Continued)

Key	Description
Previous Key	(This button type is <i>not</i> required for digital endpoints.) No further programming is necessary.
Programmable Key	Select the desired programmable button number (1–20).
Save Key	No further programming is necessary. This button type is <i>not</i> required for digital endpoints. Does not apply to Mitel endpoints, because volume changes made on Mitel IP endpoints are automatically saved.
Secondary Extension Key	Two fields are programmed for this type of button: <ul style="list-style-type: none"> Selection: Select the primary endpoint that will be associated with this secondary extension button. The primary endpoint must be on the same node as the endpoint being programmed. Ring When __ Calls At Extension: This field allows the endpoint to receive a burst of ringing when “n” number of calls are present at a primary endpoint, and at least one call is ringing or camped on. That is, a setting of 2 causes the endpoint to ring when the primary endpoint receives a third call, while two other calls are ringing. The ring burst repeats periodically as long as “n” number of calls are present at a primary endpoint. This period is determined by the Digital/IP Secondary Extension Key Alerting Tone timer. If this field is set to 0, the secondary endpoint never receives the burst of ringing.
SPCL Key	No further programming is required.
SPKR Key	This button type is <i>not</i> required for digital endpoints. No further programming is necessary. This button will be used for turning the endpoint speaker or headset on and off. Digital endpoints come equipped with a non-programmable SPKR button and do not need this button in their keymap.
Station Speed Dial Key	Select the Station Speed Dial location (0–9) that will be assigned.
System Speed Dial Key	Select the System Speed Dial location (000–999) that will be assigned.
Trunk Group Key	Select the trunk group that will be selected when this button is pressed.
Trunk Key	Select the individual trunk that will be selected when this button is pressed.
Undefined Key	No further programming is necessary. This button can be programmed by the user.
Up Key	No further programming is necessary. This button can be used to scroll forward through displays. When the endpoint is idle, it can be used for adjusting volume, in place of the VOLUME button. This button type is <i>not</i> required for digital endpoints. For digital endpoints you use the VOLUME DOWN button.
VOLUME DN Key	No further programming is necessary. It can be used for adjusting volume.
VOLUME SAVE Key	No further programming is necessary. This button can be used to save the volume setting. Does not apply to Mitel endpoints, because volume changes made on Mitel IP endpoints are automatically saved.
VOLUME UP Key	No further programming is necessary. It can be used for adjusting volume.

Programming DSS Endpoint Lists

You can add or delete endpoints that are currently assigned to the DSS keymap.

To add to the Endpoint List:

1. Select System – Endpoint-Related Information – Key Assignments – DSS – <DSS number> – **Endpoints**.
2. Right-click the list. An option box appears.
3. Select **Move to Endpoint List**. A window appears that asks you to select the type of device to include.
4. Select the device types (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
5. Select the desired devices, and then select **Move Items**. When you have selected all the devices necessary, click **Finish**. Your selection appears in the station list. To highlight a series of items, hold down **SHIFT** while selecting the first and last item you want. To highlight two or more items that are not consecutive, hold down **CTRL** while selecting the desired items.

To remove an endpoint from the list:

1. Highlight the list, and then press **DELETE**. You are prompted to confirm that you want to delete the station.
2. Click **Yes**.

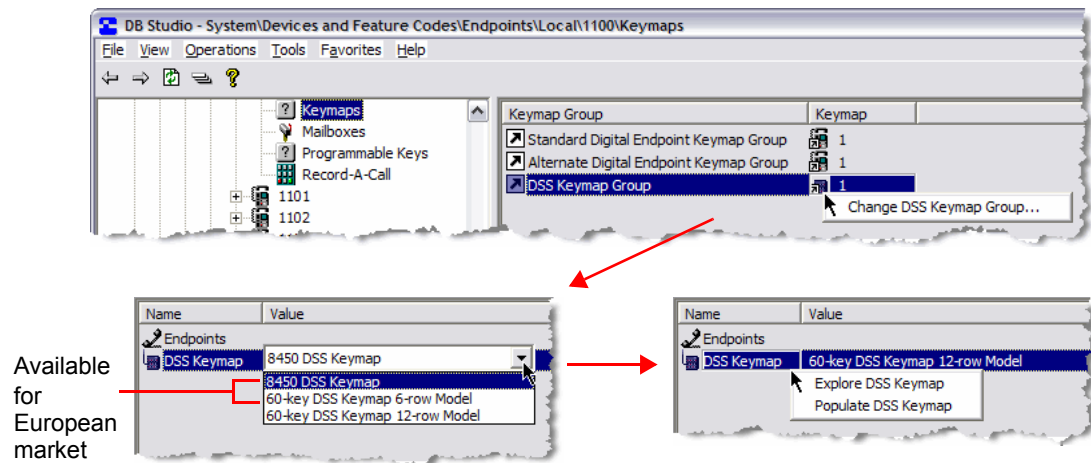
Programming DSS/BLF Devices for Digital Endpoints

You can add a DSS to a digital endpoint. Supported endpoints include Models 8520 and 8560, the Executive and Standard, Professional, and Associate.

To add and program a DSS for a digital endpoint:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the digital endpoint extension number.
3. Select **Attached Device**.
4. Select the digital endpoint to which you want to add the DSS.
5. Click **None** under the Value column, and then select **DSS** from the list.
6. Double-click **Keymaps**, located above the Attached Device option toward the top of the panel.
7. Double-click **DSS Keymap Group**. If desired, you can also right-click the shortcut and change the keymap group number, as shown in [Figure 7-6](#).

Figure 7-6. *Keymap Group Location*



8. Select the keymap type from the **Value** list.
9. Right-click the **DSS Keymap** to program. See “Programming DSS Keymaps” on [page 7-44](#).

Programming Endpoint Options

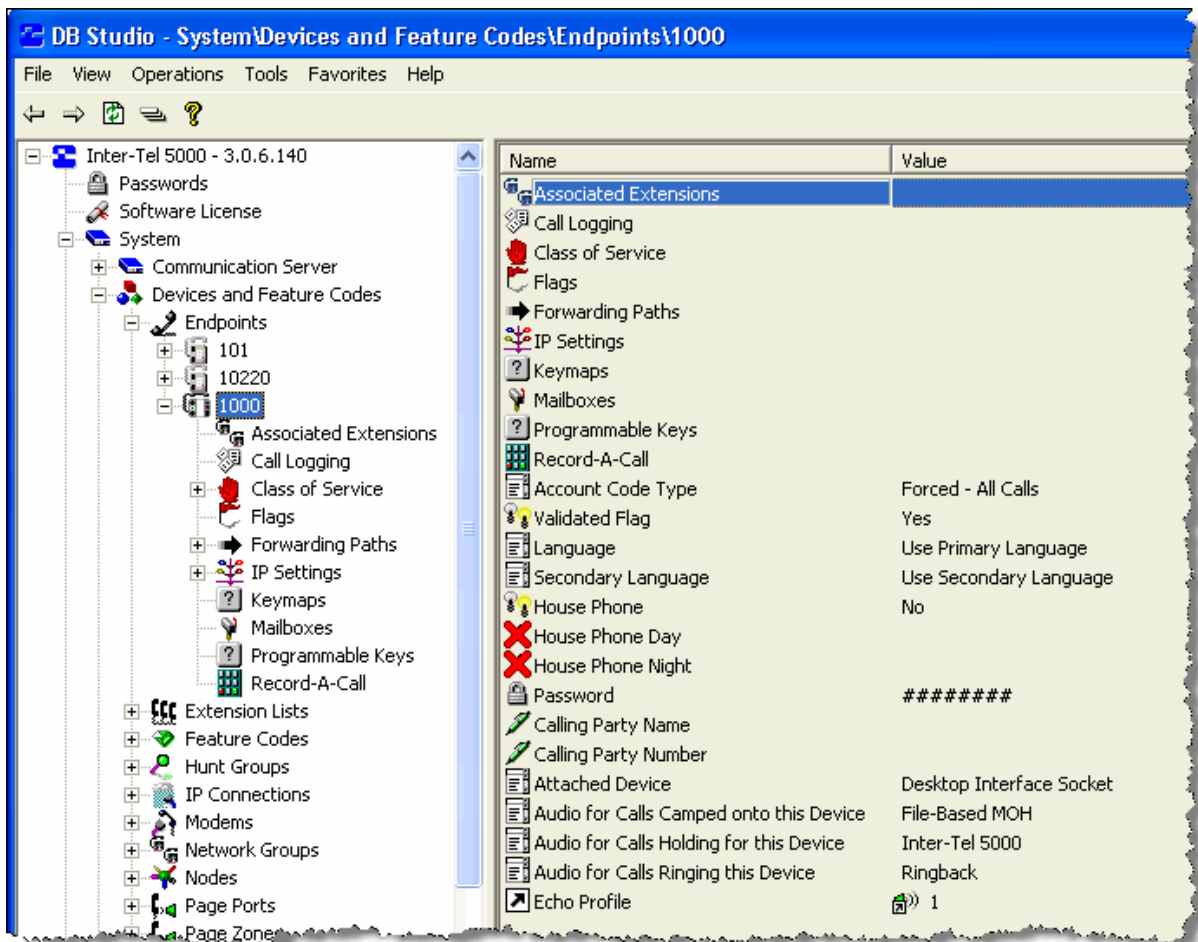
You can program the following endpoint options, as shown in [Figure 7-7](#).

NOTES

Endpoint options depend on the endpoint type.

For endpoint and device IP information and configuration instructions, see “Endpoint and Device IP Settings” on [page 9-36](#).

Figure 7-7. Endpoint Options



Associated Extensions

Associated extensions are system extensions used by the endpoints.

To program Associated Extensions:

1. Select – System – Devices and Feature Codes – Endpoints – (Local) – **<extension> – Associated Extensions.**
2. Configure the following the Associated Extensions:
 - **Agent Help and Agent Help User-Keyed Extension:** The Agent Help feature allows an endpoint user to request help from a supervisor during a call. The Agent Help Extension is the number that is called whenever the endpoint user enters the Agent Help feature code. The Agent Help Extension can be a single endpoint, or a hunt group, or it can be set to “None.” This can be a device located on another node if it is programmed as an off-node device. See “Creating Off-Node Devices” on [page 7-13](#). Optionally, the endpoint user can be allowed (or required) to enter the Agent Help Extension number, by setting the Agent Help User-Keyed Extension flag, described on [page 7-52](#).
 - **Alternate Message Source:** If an endpoint or application has an alternate message source and leaves a message at another endpoint, the alternate message source is called (instead of the endpoint or application) when the message recipient responds to the message waiting indications. The alternate message source can be a hunt group, endpoint, or application. This can be a device located on another node if it is programmed as an off-node device. See “Creating Off-Node Devices” on [page 7-13](#).
 - **Attendant:** This is the endpoint, application, or hunt group (if any) that serves as the attendant for this endpoint. This can be a device located on another node if it is programmed as an off-node device. See “Creating Off-Node Devices” on [page 7-13](#).
 - **Message Center:** The message center receives messages after the Message Wait timer expires. This can be a device located on another node if it is programmed as an off-node device. See “Creating Off-Node Devices” on [page 7-13](#).
 - **Emergency Extension:** The emergency extension determines which trunk access (trunk, trunk group, or ARS) this endpoint will use when the Emergency Call phone number is dialed. See the following Notice. This option defaults to Trunk Group 1 (92001). Endpoints cannot have direct emergency access to trunks on other nodes; they must use ARS to access off-node trunks.

NOTICE

Responsibility for Regulatory Compliance.

It is the responsibility of the organization and persons performing the installation and maintenance of Mitel Advanced Communications Platforms to know and comply with all regulations required for ensuring Emergency Outgoing Access at the location of both the main system and any remote communication endpoints. Remote IP and SIP endpoints may require gateway access to nearby emergency responders.

Emergency Call phone numbers include:

- 911, the default for Mitel systems located in the U.S.
- 999, the default for Mitel systems located in the European market and used primarily in the U.K.
- If applicable, 112, an emergency number used widely in Europe outside of the U.K.
- Any emergency number, such as for a police or fire station, that is appropriate for the location of the main system and/or remote endpoints.

NOTE

If an installation needs Emergency Outgoing Access across nodes, make sure the Local Trunk Group is the first member in the facility group. This allows cross-node emergency calls to use the Local Trunk Group first and not the Remote IP Trunk Group.

- **Outgoing Extension:** Determines which trunk access (trunk, trunk group, or ARS) this endpoint uses when an idle CALL button or the OUTGOING button is pressed, or when a System Speed Dial number is selected for dialing before a trunk is selected. Defaults to Trunk Group 1 (92001). Endpoints cannot have direct outgoing access to trunks on other nodes; they must use ARS to access off-node trunks.
- **Transfer Recall Destination:** The transfer recall destination receives transfer calls from this endpoint. This can be a device located on another node if it is programmed as an off-node device. See “Creating Off-Node Devices” on [page 7-13](#).
- **Voice Mail:** This is the voice mail destination that this endpoint uses for forwarding calls to voice mail. If this field is not programmed for an Executive or Professional Display endpoint or a Model 8560 endpoint, the endpoint will not have the voice mail-related options on the feature button menu display.
- **Agent Help User-Keyed Extension:** If desired, the endpoint user can be allowed (or required) to enter the Agent Help Extension number. Enable this flag to allow the endpoint user to enter the desired extension number. Or, disable the flag to automatically dial the Agent Help Extension programmed (or disable the Agent Help feature for the endpoint if there is no Agent Help Extension).
 - a. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
 - b. Click out of the field or press **ENTER** to save your change. The operation of the feature is determined by the programmed combination of these flags, as shown in [Table 5-14](#).

Table 7-4. User-Keyed Extension Examples for Agent Help

Agent Help	User-Keyed Extension	Result
Extension number	Disabled	The Agent Help Extension is called when the feature code is entered.
Extension number	Enabled	The user is prompted to enter the desired number after the feature code is entered. If a number is not entered before the dialing timer expires, the programmed Agent Help Extension number is dialed automatically.
None	Enabled	The user is prompted to enter the desired number after the feature code is entered.
None	Disabled	The user hears reorder tone if the feature code is entered.

- **Data Port Extension:** (*Applies to non-IP devices only.*) The data port extension determines which data port the digital endpoint uses. This is the extension number of the data port itself, not the endpoint to which it is attached. The data port may be attached to one endpoint and used by several other endpoints. The data port can be a device located on another node if it is programmed as an off-node device. If the endpoint has a DATA key, it shows the status of its associated data port. (Note that the endpoint does not have a DATA key by default. DATA keys must be programmed in the database or by the user.)
3. Change the assignment of one of the Associated Endpoints, using one of the following methods:

Method A

- a. Select the current value, then enter the new value in the text box.
- b. Press **ENTER**. A screen appears displaying what is associated with the number entered.
- c. Click **OK**. The new number appears in the field.

Method B

- a. Right-click the existing value. An option box appears.
- b. Select **Change**. A window appears prompting for the device type to include.
- c. Select the device types (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
- d. Select the device you want to assign as the associated extension, and then click **Finish**. The selection appears in the appropriate field.

NOTE

If the endpoint and voice mail administrator (refer to the *Mitel 5000 Endpoint and Voice Mail Administrator Guide*, part number 580.8001) adds or changes ring-in devices using the administrator endpoint, the system automatically changes the ring-in type to Multiple, even when only one device is selected. This occurs because the endpoint administrator can add multiple devices, which is prevented if the ring-in type is Single.

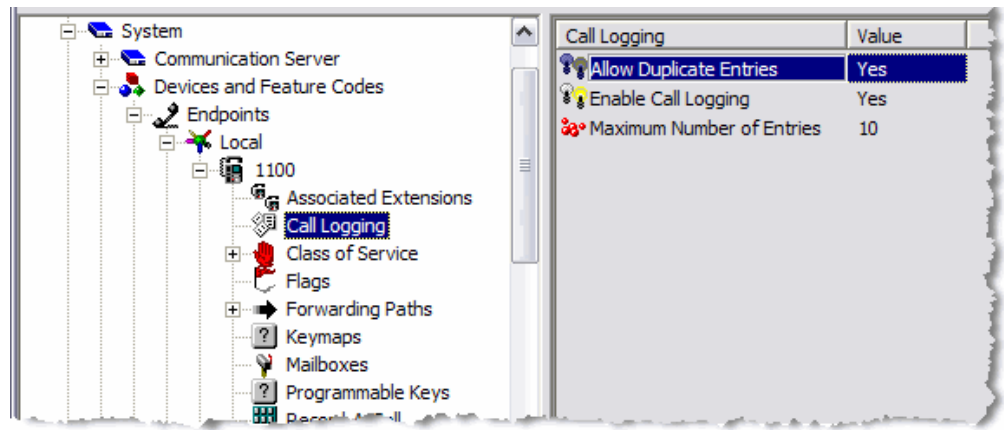
Call Logging

Table 7-5 shows Call Logging options. For more information about the Call Logging feature, refer to the System Features chapter in the *Mitel 5000 Reference Manual*, part number 580.8007. Single line endpoints do **not** support Call Logging.

Table 7-5. Call Logging Options and Descriptions

Field Name	Range	Default	Description
Allow Duplicate Entries	Yes/No	Yes	Determines whether or not duplicate entries may appear in the call logs.
Enable Call Logging			Determines whether or not Call Logging will be enabled for a particular endpoint.
Maximum Number of Entries	0–20	10	Describes the maximum number of entries that will be stored in each log.

When the **Enable Call Logging** field is set to “No,” the other two Call Logging fields display a red “X.” This indicates all features associated with Call Logging are also disabled. The following example shows the Call Logging fields for a digital endpoint.



The copy/paste functionality for endpoints includes a Call Logging option. This functionality will copy/paste the field values for the three Call Logging fields described in Table 7-5. Call Logging is not a copy/paste attribute for single line endpoints.

By default, a 1 is added to the beginning of returned CO calls. If needed, be sure to allow local Area Codes in User Group 1.

To change Call Logging options:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the extension number.
3. Select **Call Logging**.
4. Enable the options as described in Table 7-5.
5. Click out of the field or press **ENTER** to save your changes.

Day and Night Classes of Service

Each endpoint has Classes of Service (COS) which restrict or allow certain dialing patterns from being dialed on a call. For more information about COS, refer to the System Features chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

Programming Endpoint Toll Restrictions

To program endpoint toll restrictions:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the extension number.
3. Select **Day** (or **Night**) **Class of Service**.
4. Double-click the desired time period to view a list of current classes of service.

To add a class of service:

- a. Right-click in the window, and then select **Add To List**.
- b. A window appears that allows you to select toll restriction types. Select **ARS Only & Deny Area/Office** and/or **Classes of service**, and then click **Next**.
- c. The Classes of Service appear.
- d. Select the desired classes of service, then select **Add Items**. The selected classes of service appear in the list. Click **Finish** to exit.
- e. *(U.S. only)* If you selected *Deny Area/Office class of service*, the endpoint must also be assigned to a User Group. To change the user group, right-click **User Group**, then select **Change User Group**. In the first window that appears, select **User Groups**, then click **Next**. In the next window, select the desired user group, and then click **Finish** to exit and save the change.

Deleting Classes of Service

To delete one or more class of service:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the extension number.
3. Select **Day** (or **Night**) **Class of Service**.
4. Right-click, and then select **Remove Selected Items**. To select a series of items, hold down **SHIFT** while selecting the first and last item in the range. To select two or more that are not consecutive, hold down **CTRL** while selecting the desired items.

Forwarding Paths

Each endpoint can have up to three forwarding paths, and there can be 200 different programmed paths in the system, numbered 001–200. Path 000 (No Forwarding Path) can be assigned to disable system forwarding for the endpoint. For more details on system forwarding, refer to the System Features chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

The following are Forwarding Path types:

- **Forwarding Path:** Shown for reference only. To view the programming for the path, double-click Forwarding Paths to show Endpoint-Related programming.
- **Ring Principal Once:** If the system-forwarded device is an endpoint and the user wants to be notified each time a call is sent to the system forwarding path, enable this option. The endpoint user hears a single ring tone each time a call is system forwarded and the display endpoint shows CALL SENT TO FORWARD PATH. In the default state, this is disabled.
- **Endpoint Conditions (Busy, DND, No Answer, and Immediate):** The endpoint can be programmed to use the path to forward calls when the endpoint condition is busy, in Do-Not-Disturb, and/or no answer. Or, calls can be forwarded immediately after they are received at the endpoint. In the default state, all options but Immediate are selected. Determine which endpoint conditions will cause the calls to follow the forwarding path and enable them. Note that if any condition other than Immediate is selected, Immediate will appear dimmed and cannot be selected.
- **System Conditions (Day and Night Mode):** You can program the endpoint to use the forwarding path when the system is in day mode and/or night mode. By default, both day and night mode are selected. Indicate whether calls follow the forwarding path in day and/or night mode by enabling the desired system conditions.
- **Forwarding Call Types:** The types of calls that can be forwarded are listed below. The forwarding endpoint can be programmed to forward any or all of these call types. (In the default state, call routing, ring-in, DISA, and transferred calls are enabled.) Determine the types of calls that will follow the forwarding path by enabling each desired call type. Available options include:
 - *Call Routing Table:* Outside calls received through a call routing table, including DID and E&M [DDI] calls, but not including DISA calls.
 - *CO Ring-In:* Ringing outside calls, including calls received through network connections.
 - *CO Transfer/AA/VM:* Transferred outside calls, including automated attendant and voice mail transfers and transfers from other nodes.
 - *CO Recall:* Recalling outside calls, including calls from other nodes.
 - *DISA:* DISA calls, including DISA calls received through a call routing table.
 - *IC Calls:* Intercom calls, including calls from other nodes.

Adding Forwarding Paths

To add a forwarding path:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the extension number.
3. Select **Forwarding Paths**.
4. Right-click anywhere in the right side of the window, and then click **Add To Forwarding Paths List**. A window appears prompting for the device types to include.
5. Select the forwarding paths (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
6. Select the appropriate paths, then select **Add Items**. When you have added all the paths you want, click **Finish**. The selections appear in the list.

Deleting Forwarding Paths

To delete a path:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the extension number.
3. Select **Forwarding Paths**.
4. Select the path, right-click, and then select **Remove Selected Items**.

Programming Specific Forwarding Paths

NOTE

Call forwarding paths are checked in numerical order when they apply to the same call type (for example, multiple forwarding paths for outside calls). If one forwarding path is for the “No Answer” call condition, it should be last on the list of endpoint forwarding paths. If No Answer is the condition in the first path, the system always waits for the System Forward Initiate timer to expire before forwarding, even if the endpoint is in Do-Not-Disturb mode or busy.

To program a specific Forwarding Path:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the extension number.
3. Select **Forwarding Paths**.
4. Double-click the forwarding path to view the following options:

Enabling Forwarding Path Options

To enable a Forwarding Path option:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the extension number.
3. Select **Forwarding Paths**.
4. Select the option.
5. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
6. Click out of the field or press **ENTER** to save your change.

Mailboxes

If the endpoint being programmed serves as the message notification endpoint for one or more mailboxes, the mailboxes appear in the Mailboxes list.

To view the Mailboxes list:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the extension number.
3. Select **Mailboxes** to see the list of mailboxes assigned to this endpoint. You cannot program the mailbox here.
4. Double-click the mailbox. The screen jumps to the Mailbox programming area.

Record-A-Call

You must create the Record-A-Call application the Voice Processor database before you can enable the feature. See “Record-A-Call” on [page 11-38](#).

There are three fields for the Record-A-Call feature: Mailbox, Mailbox User-Keyed Extension Flag, and Application. The application and mailbox might not be on the same node as the endpoint. If so, you must program the voice processor applications as off-node devices on the local node, and the endpoint must be an off-node device on the Voice Processor node. See “Creating Off-Node Devices” on [page 7-13](#).

Determine which mailbox, if any, is dialed automatically when the Record-A-Call feature is used. The Record-A-Call Mailbox can be set to “This Endpoint’s Associated Mailbox” to call the mailbox assigned to that endpoint, or it can be set to any valid mailbox number. If you do not want a mailbox number dialed automatically when the Record-A-Call feature is used at this endpoint, enable the User-Keyed Mailbox flag. This overrides the automatic entry and allows the endpoint user to enter the desired mailbox number. The operation of the feature is determined by the programmed combination of these flags, as shown in [Table 7-6](#).

Table 7-6. *Record-A-Call Operation*

Record-A-Call Mailbox	User-Keyed Mailbox	Result
“Associated” or mailbox number	Disabled	The Record-A-Call Mailbox is automatically called when the feature code is entered.
“Associated” or mailbox number	Enabled	The user is prompted to enter the desired mailbox number after the Record-A-Call feature code is entered. If a number is not entered before the dialing timer expires, the programmed Record-A-Call Mail box number is dialed automatically.

Programming the Record-A-Call Mailbox

You can assign the mailbox to which Record-A-Call mailbox records and saves calls.

To program the Record-A-Call mailbox:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the extension number.
3. Select **Record-A-Call**.
4. Use one of the following methods:

Method A

- a. Select the current value, then enter the new value in the text box.
- b. Press **ENTER**. A screen appears displaying what is associated with the number entered.
- c. Click **OK**. The new number appears in the field.

Method B

- a. Right-click the current Value. An option box appears.
- b. Select **Change Mailbox**. A window appears prompting for the mailbox type to include.
- c. Select **Mailbox**, **This Endpoint's Associated Mailbox**, **Off-Node Mailbox**, or **Unassociated Mailbox Off-Node Device**, then click **Next**. The list of mailboxes appears. You can view them in a list by selecting the List button or view details by selecting the Details button.
- d. Select the desired mailbox, then click **Finish**. The selection appears in the Mailbox field.

Programming the Mailbox User-Keyed Extension

The Mailbox User-Keyed Extension option determines the mailbox destination for recorded calls. If the value is "No" (disabled), the system uses the mailbox stored in the Record-A-Call "Mailbox" field (see the previous section). If enabled, the system prompts the user for a mailbox number when Record-A-Call is activated. The default value is "No" (disabled).

To set the Mailbox User-Keyed Extension option:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the extension number.
3. Select **Mailbox User-Keyed Extension**.
4. In the Value column, select the check box. The field changes to **Yes**. To disable the flag, clear the check box.
5. Click out of the field or press **ENTER** to save your change.

Programming the Record-A-Call Application

The voice processor must have one or more applications created for the Record-A-Call feature. You can choose the application that is used by the endpoint. If you choose **None**, the endpoint will not have access to the Record-A-Call feature.

To set the Application:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the extension number.
3. Select **Application**.
4. Use one of the following methods:

Method A

- a. In the Value column, select the current value, then enter the new value in the box.
- b. Press **ENTER**. A screen appears displaying information associated with the number entered.
- c. Click **OK**. The new number appears in the field.

Method B

- a. Right-click the current value. An option box appears.
- b. Select **Change Application**. A window appears prompting for the application type to include.
- c. Select **None**, **Record-A-Call**, or **Off-Node Record-A-Call**, then click **Next**. The list of applications with details appear. To view the applications in a list only, click **List**.
- d. Select the desired application, and then click **Finish**. The selection appears in the Application field.

Languages

You can set the (primary) languages that display for the voice prompts and endpoint displays. This field can be set to any specific language so that the system can support more than two languages. The language choices are Use Primary Language, Use Secondary Language, American English, British English, Japanese, or Spanish. End users can also select the primary or secondary language, if enabled. See “Secondary Language” on [page 7-61](#).

NOTE	Mitel IP endpoints do not support the Japanese Language.
-------------	--

To select a primary language:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the extension number.
3. Select **Language**.
4. In the **Value** column, select the option from the list.
5. Click out of the field or press **ENTER** to save your change.

Secondary Language

The Secondary Language option corresponds to the Change Language feature (301). The Change Language feature is used to toggle between the system Primary Language and the system Secondary language.

NOTE Mitel IP endpoints do not support the Japanese Language.

It toggles between the System Primary Language and the endpoint Secondary Language, or can specify a language. This allows any endpoint in the system to have its own secondary language or use the System Secondary Language, giving the system the ability to support more than two languages.

- If the endpoint Secondary Language field is programmed to be Use Primary Language the Change Language feature will do nothing because the endpoint will toggle between the System Primary Language and the endpoint Secondary Language, which is the System Primary Language.
- If the endpoint Secondary Language field is programmed to be Use Secondary Language the Change Language feature will toggle between the System Primary Language and the endpoint Secondary Language, which is the System Secondary Language. This is the system default.
- If the endpoint Secondary Language field is programmed to be Japanese the Change Language feature toggles between the System Primary Language and the endpoint Secondary Language, which is Japanese.

The Language field for endpoints indicates what language the endpoint is currently set to. This field is used to toggle between the Use Primary Language and Use Secondary Language. It can be set to any specific language along with the Use Primary Language and Use Secondary Language.

The side-effect of changing the Language field is that if you change it to Japanese and the endpoint Secondary Language field is set to Spanish, then the user will have no way to get back to Japanese if they enter the Change Language feature code. This is because the first time the user enters the feature code, the system toggles the endpoint to the Use Primary Language option. The next time the user enters the feature code, the system toggles the language to the endpoint Secondary Language, which is Spanish. To avoid this situation, simply change the endpoint Secondary Language to Japanese and the endpoint Language field to Japanese.

To select a secondary language:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the extension number.
3. Select **Secondary Language**.
4. In the **Value** column, select the option from the list.
5. Click out of the field or press **ENTER** to save your change.

House Phones

An endpoint designated as a House Phone automatically dials a predetermined number when the handset is lifted.

Assigning an Endpoint as a House Phone

You can assign an endpoint as a house phone.

To enable the House Phone flag and assign an endpoint as a House Phone:

1. Select – System – Devices and Feature Codes – Endpoints – (**Local**).
2. Select the extension number.
3. Select **House Phone**.
4. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
5. Click out of the field or press **ENTER** to save your change.

Assigning House Phone Day and Night Extension Numbers

The assigned day number is dialed when the system is in day mode and the assigned night number is dialed when the system is in night mode. You can also program the day or night House Phone numbers using the House Phone Speed Dial locations.

To program House Phone day and night numbers:

1. Select – System – Devices and Feature Codes – Endpoints – *<extension>* – **House Phone Day (or Night)**.
2. In the **Value** column, enter the extension or outside number (up to 16 digits, including pauses and hookflashes [recalls] that are dialed when the House Phone is used during the day and/or night mode).
3. Click out of the field or press **ENTER** to save your change. You can use the extension number of an off-node device, if desired. These numbers are also endpoint speed-dial locations codes 0 (day) and 1 (night).

Remote Programming Password

You can change the Remote Programming Password. The default password is the extension number of the endpoint. The password can also be changed by entering the Program Endpoint Password feature code at the endpoint or when using the Remote Programming feature. For more information about the Remote Programming feature, refer to the System Features chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

To program a password for the endpoint:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the extension number.
3. Double-click **Password**. The Edit Password dialog box appears.
4. In the **New Password** box, type the new password (up to 8 digits). Typed characters appear as asterisks (***).
5. Retype the password exactly as before in the Confirm Password box.
6. Click **OK** to exit and save the password. If the entered passwords match, you will return to the Password field. If not, you must re-enter the new password and verify it again. If you make a mistake while entering the password or want to leave it unchanged, select Cancel. To prevent unauthorized use of call forward to the public network, all endpoints using Remote Programming should have a password. To make the passwords difficult to guess, they should not match the extension number or consist of one digit repeated several times.

Calling Party Name

This option is similar to the existing Calling Party Number option described in the following section. It is used only for ISDN calls to the public network (non-private networking). If this option is enabled, the system may use this information for the outgoing ISDN setup request message. You can program up to 20 alphanumeric characters in the box. This field is not used when the “Send Station Caller ID to Attached PBX,” “Propagate Original Caller ID,” and/or “Propagate Original Caller ID on Transfer” (for voice mail) flags are enabled.

To enter a Calling Party name:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the extension number.
3. Select **Calling Party Name**.
4. In the **Value** column, select the current value, and then type the name in the box.
5. Click out of the field or press **ENTER** to save your change.

Calling Party Number

Each endpoint can be programmed to send an identifying number when a call is placed. This is called the “Calling Party Number.” In the U.S., this information is required for emergency 911 calls in some states. You can program any number up to 48 digits in the Calling Party Number field. However, check with your service provider to determine their specific requirements for this field. This number will be sent in the ISDN setup message in the Calling Party Number Information Element. In addition, the System will also send the extension number of the endpoint in the Calling Party Number Subaddress Information Element. The CO should ignore this information element if it does not support it.

NOTE

There is no default number for this field. It is up to you to supply the correct Emergency Calling Party Number for each endpoint.

To enter a number to display as the Calling Party Number:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the extension number.
3. Select **Calling Party Number**.
4. In the **Value** column, select the current value, and then type the number in the box.
5. Click out of the field or press **ENTER** to save your change.

Emergency Party Calling Number

You can specify the Caller ID [CLID] to use when an endpoint makes an outgoing emergency call. Call Processing propagates the appropriate calling party number to the PSTN.

To enter an Emergency Calling Party Number:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the extension number.
3. Select Emergency **Calling Party Number**.
4. In the **Value** column, select the current value, and then type the number in the box.
5. Click out of the field or press **ENTER** to save your change.

Attached Device

(**Not** used for single line endpoints.) Indicate the type of attached device connected to the endpoint. Or, if nothing is connected, select **None**. The other option is **Desktop Interface Socket**.

To set the attached device field:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the extension number.
3. Select **Attached Devices**.
4. In the **Value** column, select the option from the list.
5. Click out of the field or press **ENTER** to save your change.

Device Audio for Calls Settings

You can program the following audio options that callers hear when waiting for system users:

- “[Audio for Calls Camped onto this Device](#)” below
- “[Audio for Calls Holding for this Device](#)” below
- “[Audio for Calls Ringing this Device](#)” on [page 7-66](#)

Audio for Calls Camped onto this Device

You can select the audio that callers hear when camped-on to the endpoint.

To program the Audio for Calls Camped onto this Device:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the extension number.
3. Select **Audio for Calls Camped onto this Device**.
4. Select one of the following options from the list:
 - **Silence:** Callers hear no Music-On-Hold.
 - **Tick Tone:** Callers hear tick tone.
 - **Ringback:** Callers hear ringback.
 - **Inter-Tel 5000:** Callers hear an external music source. This is the default value.
 - **File-Based MOH:** Callers hear the MOH file selected in DB Programming. For more information, see “File-Based Music-On-Hold (MOH)” on [page 10-9](#).
5. Click out of the field or press **ENTER** to save your change.

Audio for Calls Holding for this Device

You can select the audio that callers hear when placed on hold at the endpoint.

To program Audio for Calls Holding for this Device:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the extension number.
3. Select **Audio for Calls Holding for this device**.
4. Select one of the following options from the list:
 - **Silence:** Callers hear no Music-On-Hold.
 - **Tick Tone:** Callers hear tick tone.
 - **Ringback:** Callers hear ringback.
 - **Inter-Tel 5000:** Callers hear an external music source. This is the default value.
 - **File-Based MOH:** Callers hear the MOH file selected in DB Programming. For more information, see “File-Based Music-On-Hold (MOH)” on [page 10-9](#).
5. Click out of the field or press **ENTER** to save your change.

Audio for Calls Ringing this Device

You can select the audio that callers hear when ringing the endpoint.

NOTE

The Audio for Calls Ringing this Device option only works when the call goes through a trunk group and also when used in conjunction with the Use Next Device's Audio Source field. IC calls do not apply to the use of this field when this field is set to a music source. For a hunt group in which the primary purpose is to support IC callers (for example, an internal help desk), you should set all of the "Audio for Calls..." fields to something other than a music source, such as Ringback.

To program Audio for Calls Ringing this Device:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the extension number.
3. Select **Audio for Calls Ringing this device**.
4. Select one of the following options from the list:
 - **Silence**: Callers hear no Music-On-Hold.
 - **Tick Tone**: Callers hear tick tone.
 - **Ringback**: Callers hear ringback. This is the default value.
 - **Inter-Tel 5000**: Callers hear an external music source.
 - **File-Based MOH**: Callers hear the MOH file selected in DB Programming. For more information, see "File-Based Music-On-Hold (MOH)" on [page 10-9](#).
5. Click out of the field or press **ENTER** to save your change.

Phantom Devices

Phantom devices are fully functional virtual devices on the system. Phantom devices can function with Unified Communicator (UC) to perform advanced call routing tasks without the need for a real desk phone. They can also have a true status, such as idle, Do-Not-Disturb (DND), ringing, and so on. This allows them to be placed in hunt groups and actually ring.

For information about programming phantom devices, refer to the DB Programming Online Help files. For more information about phantom devices, refer to the System Features chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

To create a phantom device:

1. Select System – Devices and Feature Codes – **Phantom Devices**.
2. Right-click in a blank area of the right pane, and then select **Create Phantom**.
3. In the Create Phantom Device Extension dialog box, enter the desired extension number or scroll to the desired number and also enter the number of extensions.
4. Click **OK** to continue. This is the same method used to create other off-node device types.

After you create the phantom device, double-click the device to program the following associated fields:

- **Associated Extensions:** Allows you to view the list of extensions used by the phantom being programmed. The following Associated Extensions options apply to phantoms:
 - Attendant
 - Message Center
 - Alternate Message Source
 - Transfer Recall Destination
 - Voice Mail Extension
 - Outgoing Extension
- **Class of Service:** Each phantom device has Classes of Service (COS), which restrict or allow certain dialing patterns from being dialed on a call.
- **Flags:** The phantom flags that can be programmed include:
 - Alternate Hold Timer
 - Attendant
 - DID/E&M Receive Busy Instead of Camp-On
 - Do-Not-Disturb Allowed
 - Hunt Group Remove/Replace
 - Manual Forward to Public Network
 - Receive Busy Instead of DND
 - System Forwarding
- **Forwarding Paths:** When created, phantoms are automatically added to the All Endpoints (PP051) extension list. Phantoms can be forwarded and follow the rules for endpoint manual and system forwarding.
- **Mailboxes:** If the phantom being programmed serves as the message notification endpoint for one or more mailboxes, the mailboxes appear in the Mailboxes list. Select **Mailboxes** to see the list of mailboxes assigned to this phantom. You cannot program the mailbox here, but if you double-click the mailbox, the Mailbox programming area appears.
- **Password:** This password is used for the Remote Programming feature. The Phantom password can be up to eight digits long. The default password is the extension number of the Phantom. The password can also be changed by entering the Program Endpoint Password feature code at the endpoint or when using the Remote Programming feature.

- **Audio for Calls Camped onto this Device:** This option defines the audio that a caller hears when camped onto the device. The default is Inter-Tel 5000. Other options include Silence, Tick Tone, and Ringback.
- **Audio for Calls Holding for this Device:** This option defines the audio that a caller hears when holding for the device. The default is **Inter-Tel 5000**. Other options include Silence, Tick Tone, and Ringback.
- **Audio for Calls Ringing this Device:** This option defines the audio that a caller hears when ringing the device. The default is **Ringback**. Other options include Silence, Tick Tone, and Inter-Tel 5000.

NOTE

The Audio for Calls Ringing this Device option only works when the call goes through a trunk group and also when used in conjunction with the Use Next Device's Audio Source field. IC calls do not apply to the use of this field when this field is set to a music source. For a hunt group in which the primary purpose is to support IC callers (for example, an internal help desk), you should set all of the "Audio for Calls..." fields to something other than a music source, such as Ringback.

Account Codes

You can use account codes to force system users to enter a preprogrammed code when placing calls of a certain type. The default database does not contain any account codes, but you add up to 512 account codes. In a networked system, the system validates account codes against the account code table on the user's node. The account code follows the call as it moves from node to node and appears on every SMDR record associated with the call. You cannot use account codes for phantom devices (see [page 7-67](#)).

You can assign each endpoint a standard or forced account code, of which four (two in Europe) are ARS dependent. Or, if desired, the endpoint can have no associated account code. If you assign a standard account code, you must also designate a specific code (001–512). [Table 7-7](#) shows account code types.

Table 7-7. Account Codes Available for U.S. and Europe

Account Code	Description	U.S.	Eur.
None	Does not require the user to enter an account code. The user may still use optional account codes or enable the Account Code For All Calls Following feature, as desired.	✓	✓
Standard	Automatically appear in the SMDR printout to identify calls from this endpoint. The endpoint user is not required to enter any digits during the call.	✓	✓
Forced – All Calls Validated	Requires the user to enter a forced account code before placing an outside call. If the code matches one of the forced account codes in the database, the call is allowed. If the code does not match, the call is blocked.	✓	✓
Forced – All Calls Non-Validated	Requires the user to enter an account code before placing any outside call. The code is not checked against any lists, and the call is allowed as soon as the code is entered.	✓	✓
Forced – Local Toll Calls Validated	Requires the user to enter an account code after dialing a local toll call number when using ARS. If the code matches one of the forced account codes in the database, the call is allowed. If the code does not match, the call is blocked.	✓	
Forced – Local Toll Calls Non-Validated	Requires the user to enter an account code after dialing a local toll call or long distance number when ARS is used. The code is not checked against any lists and the call is allowed as soon as the code is entered.	✓	
Forced – Long-Distance Toll Calls Validated	Requires the user to enter an account code if the system detects that a long distance call has been dialed when ARS is used. If the code matches one of the forced account codes in the database, the call is allowed. If the code does not match, the call is blocked.	✓	
Forced – Long-Distance Toll Calls Non-Validated	Requires the user to enter an account code if the system detects that a long distance call has been dialed when ARS is used. The code is not checked against any lists and the call is allowed as soon as the code is entered.	✓	
Forced – Toll (National) Calls Validated	Requires the user to enter an account code after dialing a national call number when using ARS. If the code matches one of the forced account codes in the database, the call is allowed. If the code does not match, the call is blocked.		✓
Forced – Toll (National) Calls Non-Validated	Requires the user to enter an account code after dialing a national call when using ARS. The code is not checked against any lists, and the call is allowed as soon as the code is entered.		✓

Viewing Account Codes

To view account codes:

Select System – Endpoint-Related Information – **Account Codes**.

Programming Forced Account Code Options

To program forced account code options:

1. Select System – Endpoint-Related Information – Account Codes – **Forced**.
2. Select one of the following options:
 - **Non-Validated or Validated:** Select either of these options to view a list of account code types. Select an account code type to view a list of endpoints that have been assigned to that account code list.
 - **Account Codes 001–512:** To enter a new account code, select the current value for the code, and then enter the new digits in the box. The maximum account code length is 12 digits. Account codes can be of varying lengths of the same digits as long as they do not exceed the maximum. For example, if the maximum length is four digits, 1, 11, 111, and 1111 can be entered as separate account codes. Click out of the field or press **ENTER** to save your change.

Adding Devices to an Account Code List

To add a device to an account code list:

1. Select System – Endpoint-Related Information – **Account Codes**.
2. Right-click anywhere in the right pane of the window. An option box appears.
3. Select **Add To List**. A window appears prompting for the device type to include.
4. Select the device types (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
5. Select the appropriate items, then select **Add Items**. When you have added all the devices, click **Finish**. The selections appear in the list. To view programming options, double-click the extension number.

Deleting Devices from Account Code Lists

To delete a device from a list:

1. Select System – Endpoint-Related Information – **Account Codes**.
2. Select the device.
3. Right-click, and then select **Remove Selected Items**.

Assigning an Account Code Type to an Individual Endpoint

You can assign an account code type to an individual endpoint:

To assign an Account Code Type to an individual endpoint:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the extension number.
3. Select **Account Code**, and then select the option (None, Standard, Forced).
4. Click out of the field or press **ENTER** to save your change. Each endpoint can be assigned *either* a forced or standard account code—or no account code. If you select an endpoint for standard or forced account code that was previously programmed to require an account code, the previous account code type is replaced by the new code type.

Setting the Forced Account Code Validated Flag

If you assign a forced Account Code Type to an endpoint (see the previous section), you can set the Validated flag to check the code entered (flag turned on) or accept any code (flag disabled).

To set the Validated flag:

1. Select – System – Devices and Feature Codes – Endpoints – **(Local)**.
2. Select the extension number.
3. Select **Validated Flag**.
4. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
5. Click out of the field or press **ENTER** to save your change.

Endpoint Messages

Endpoints use Do-Not-Disturb and Reminder messages. You can change the default messages that display on node endpoints. For more information about using Do-Not-Disturb and Reminder messages, refer to the System Features chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

Changing Do-Not-Disturb Messages

Endpoints show Do-Not-Disturb messages in English, British English, Spanish, and Katakana (Japanese) characters.

NOTES

The Japanese language is not supported on Mitel 5000-series endpoints. You must use an administrator endpoint to program Japanese messages. For more information, refer to the *Mitel 5000 Endpoint and Voice Mail Administrator Guide*, part number 580.8001.

When changing DND messages, you should keep the meanings for the messages in all languages the same. This allows endpoint users to select the message in the same location for either primary or secondary languages. For example, if you change the DND message "02" to "PAGE ME" in the English language, you should program a similar message for message "02" in the other languages.

The default Do-Not-Disturb messages are shown in [Table 7-8](#).

Table 7-8. Default DND Messages

Code	Default Message	Code	Default Message
01	Do-Not-Disturb	11	Out of Town 'Til
02	Leave a Message	12	Out of Office
03	In Meeting Until	13	Out Until
04	In Meeting	14	With a Client
05	On Vacation/ Holiday 'Til	15	With a Guest
06	On Vacation/ Holiday	16	Unavailable
07	Call Me At	17	In Conference
08	At the Doctor	18	Away from Desk
09	On a Trip	19	Gone Home
10	On Break	20	Out to Lunch

To change a DND message:

1. Select System – Endpoint-Related Information – **Messages**.
2. Double-click the language for the DND messages that you want to change.
3. Double-click **DND**.
4. In the **Value** column, type the new message in the text box (up to 16 characters, including spaces).
5. Click out of the field or press **ENTER** to save your change.

Changing Reminder Messages

Endpoints show Reminder messages in English, British English, Spanish, and Katakana (Japanese) characters.

NOTES

The Japanese language is not supported on Mitel 5000-series endpoints. You must use an administrator endpoint to program Japanese messages. For more information, refer to the *Mitel 5000 Endpoint and Voice Mail Administrator Guide*, part number 580.8001.

When changing Reminder messages, you should keep the meanings for the messages in all languages the same. This allows endpoint users to select the message in the same location for either primary or secondary languages. For example, if you change the Reminder message “02” to “PAGE ME” in the English language, you should program a similar message for message “02” in the other languages.

The default Reminder messages are shown in [Table 7-9](#).

Table 7-9. Default Reminder Messages

Code	Default Message	Code	Default Message
01	Meeting	11	Call Engineering
02	Staff Meeting	12	Call Marketing
03	Sales Meeting	13	Call Accounting
04	Cancel Meeting	14	Cancel DND
05	Appointment	15	Cancel Call Fwd
06	Place Call	16	Take Medication
07	Call Client	17	Make Reservation
08	Call Customer	18	Review Schedule
09	Call Home	19	Lunch
10	Call Corporate	20	Reminder

To change a Reminder message:

1. Select System – Endpoint-Related Information – **Messages**.
2. Double-click the language for the DND messages that you want to change.
3. Double-click **Reminder**.
4. In the **Value** column, type the new message in the text box (up to 16 characters, including spaces).
5. Click out of the field or press **ENTER** to save your change.

System Forwarding Paths

You can program up to 200 unique forwarding paths (001–200). When System Forwarding is selected from the Endpoint-Related Information programming area, the list of forwarding paths 1–200 appears. For more information about System Forwarding Paths, refer to the System Features chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

NOTE

After programming, end users must enable and disable this feature from their endpoints using feature code 354 (System Forwarding on/off). Refer to the applicable endpoint user guide for more information.

This area is used for assigning forwarding points to the system forwarding paths. You can then program endpoints to use the forwarding paths in endpoint programming (see [page 7-56](#)).

Each forwarding path can have a distinctive description (of up to 20 characters) and four forwarding points. The forwarding points can be local endpoints, voice mail ports, or hunt groups, or they can be off-node devices. Program the fields for the forwarding paths as follows:

To program a forwarding path description:

1. Select System – **Endpoint-Related Information**.
2. Double-click **System Forwarding Paths**.
3. In the applicable **Description** column, type a name for the forwarding path, up to 20 characters, in the box.
4. Click out of the field or press **ENTER** to save your change.

To program a forwarding point:

Use one of the following methods:

Method A

- a. Select the current value, and then enter the new value in the text box.
- b. Press **ENTER**. A screen appears displaying what is associated with the number entered.
- c. Click **OK**. The new number appears in the field.

Method B

- a. Right-click the existing Forwarding Point. An option box appears.
- b. Select **Change Forwarding Point**. A window appears prompting for the device type to include.
- c. Select the desired device, and then click **Next**. The devices with details appear. To view devices in a list only, click **List**.
- d. Select the desired device, and then click **Finish**. The selection appears in the appropriate Forwarding Point field.

System Speed Dial

The Mitel 5000 platform supports up to 1000 System Speed Dial numbers. The default database contains only System Speed Dial bin #000 because this is used by the system to establish links to other Speed Dial bins. You may create new bins, individually or in batches, as needed, through DB Programming.

System Speed Dial bins may also be programmed from an administrator endpoint, using the System Speed Dial feature code (9801). If the user enters a bin that is currently not equipped, one will be automatically equipped and ready for programming. This is transparent to the user at the endpoint.

When converting from an older software version to a newer version, the conversion program will automatically unequip all System Speed Dial bins that have an empty name and number, with the exception of bin #000.

A user at an endpoint cannot program System Speed Dial bins when there is an active DB Programming session, and no one can log into DB Programming when System Speed Dial bins are being programmed from an endpoint.

System Speed Dial numbers can only be used on the node where they are programmed. Each node in the network must have its own System Speed Dial numbers.

To program a System Speed Dial number:

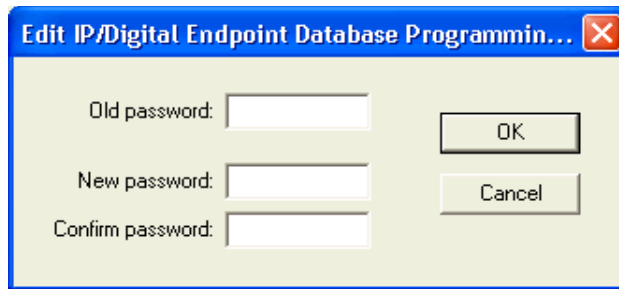
1. Select System – **Endpoint-Related Information**.
2. Double-click **System Speed Dial**.
3. Complete the following options:
 - **Name:** If desired, you can program a name for the speed-dial number. Each name can have up to 16 characters.
To program the name:
 - a. Select the current value, and then enter the new name in the text box.
 - b. Click out of the field or press **ENTER** to save your change.
 - **Number:** Numbers can include up to 48 digits and can include digits (0–9, *, and #), timed pauses, or hookflashes/recalls. Timed pauses and/or hookflashes/recalls are used when entering a series of numbers, such as access codes, security codes, and numbers for specialized common carrier (SCC) dialing (U.S. only). To include a pause in the number, enter the letter P for a pause. To include a hookflash/recall, enter F. The pause length represented by the P is determined by the Pause timer. Each pause or hookflash (recall) is considered one of the 32 digits.
To program the number:
 - a. Select the current value, and then enter the new digits in the text box.
 - b. Click out of the field or press **ENTER** to save your change.
 - **Private Number:** Determine which System Speed Dial number locations may be viewed on display endpoints. Non-display numbers do not appear on display endpoints when dialed and cannot be redialed at display endpoints. Non-display numbers will appear in the SMDR when dialed. To allow the speed-dial number to be displayed when dialed, enable the flag. Disable the flag to make it a non-display number.
To enable the Private Number flag:
 - a. Select the current value, and then select the check box. The field changes to **Yes**. To disable the option, clear the check box.
 - b. Click out of the field or press **ENTER** to save your change.

Administrator Endpoint DB Programming Password

This password is used when programming through an administrator endpoint. For more information about using the administrator endpoint, refer to the *Mitel 5000 Endpoint and Voice Mail Administrator Guide*, part number 580.8001.

To program the password:

1. Select System – **Endpoint-Related Information**.
2. Right-click **IP/Digital Endpoint Database Programming Password**, and then click **Edit Password**. The following dialog box appears.



3. Enter the old password, if one exists, in the Old password box.
4. In the **New Password** box, type the new password (up to 8 digits, using digits 0–9). Typed characters appear as asterisks (***) .
5. Retype the password in the **Confirm password** box.
6. Click **OK** to exit and save the password. If the entered passwords match, you return to the Password field. If not, you must re-enter the new password and verify it again. If you make a mistake while entering the password or want to leave it unchanged, click **Cancel**.

NOTE

To provide system security and prevent unauthorized access to the system database, you should enter a password for the administrator endpoint that is difficult to guess. For example, you should not use the endpoint extension number or several repeated digits. You or the endpoint user should periodically change the password.

Message Centers

An endpoint can be designated as a message center and assigned a list of endpoints that it will serve. When you select **Message Centers** from the Endpoint-Related Programming area, you can view a list of the existing message centers.

If you double-click a specific message center, you can view the list of endpoints it serves.

To assign the endpoints served by the message center:

1. Select System – Endpoint-Related Information – **Message Centers**.
2. Double-click the Message Center extension.
3. Right-click anywhere in the right side of the window. An option box appears.
4. Select **Move To List**. A window appears prompting for the device type to include.
5. Select the device type(s), and then click **Next**. A list appears. You can view them in a list by selecting the List button or view details by selecting the Details button. To select a series of items, hold down **SHIFT** while selecting the first and last items in the range. To select two or more items that are not consecutive, hold down **CTRL** while selecting the desired items.
6. Select the appropriate items, then select **Move Items**. When you have added all the devices, click **Finish**. The selections appear in the list. To view programming options, double-click the extension number.

To delete a device from the list:

1. Select the item(s)
2. Right-click and select **Move to NONE List**.

You can also assign message centers in endpoint programming by selecting the endpoint Associated Extensions and Message Center options and selecting the endpoint that will serve as the message center. See [page 7-51](#).

Attendants

An endpoint can be designated as an attendant and assigned a list of endpoints that it will serve. When you select Attendants from the Endpoint-Related Programming area, you can view a list of the existing attendants.

If you double-click a specific attendant, you can view the list of endpoints it serves.

To create an attendant:

Enable the endpoint Attendant flag, as described on [page 7-23](#).

To assign the endpoints served by the attendant:

1. Select System – Endpoint-Related Information – **Attendants**.
2. Select the extension number.
3. Right-click anywhere in the right pane. An option box appears.
4. Select **Move To List**. A window appears prompting for the device type include.
5. Select the device type(s), and then click **Next**. A list appears. You can view them in a list by selecting the List button or view details by selecting the Details button. To select a series of items, hold down **SHIFT** while selecting the first and last items in the range. To select two or more items that are not consecutive, hold down **CTRL** while selecting the desired items.
6. Select the appropriate items, then select **Move Items**. When you have added all the devices, click **Finish**. The selections appear in the list. To view programming options, double-click the extension number.

To delete a device from an attendant list, select the item, right-click, and select **Move to NONE List**.

You can also assign attendants in endpoint programming by selecting the endpoint Associated Extensions and Attendant options, and then selecting the endpoint that will serve as the attendant (see [page 7-51](#)).

Primary Attendants

When you select Primary Attendants from the Endpoint-Related Programming list, you see fields for programming the Primary Attendant endpoint and the Local Attendant endpoint. Those fields are programmed as described below.

- **Primary Attendant:** This is the network primary attendant.
- **Local Attendant:** This is the attendant for the node being programmed.

If an attendant is set to None, calls that would normally go to the attendant are handled as follows:

- If the system has seized the call, but it has not been sent to an endpoint, the call is disconnected.
- If the call has been sent to an endpoint, it remains at the endpoint and rings until answered.
- If the call is not seized and not sent to an endpoint, the caller will hear ringing until he or she hangs up. The call will not ring at any endpoint.

To program an attendant:

1. Select System – Endpoint-Related Information – **Primary Attendant**.
2. Select the extension number.
3. Select one of the following methods:

Method A

- a. In the **Value** column, select the current value, and then enter the new value in the box.
- b. Press **ENTER**. A screen appears displaying what is associated with the number entered.
- c. Click **OK**. The new number appears in the field.

Method B

- a. Right-click the existing Primary Attendant Endpoint or Local Attendant Endpoint, and then click **Change Attendant**. A dialog box appears prompting for the device type to include.
- b. Select the desired device or **None**, and then click **Next**. The list of devices with details appears. To view items in a list only, click **List**.
- c. Select the desired device, and then click **Finish**. The selection appears in the applicable Attendant field.

Single Line Endpoint CLID Timers

Single line endpoints in European systems only. The system supports the transmission of CLID to single line sets in Europe. This feature uses the calling party information that the system receives from the local network provider. Once programmed, on-hook single line endpoints display the calling party information when receiving an incoming outside call. The CLID information is also displayed if the single line set receives a transferred call from another endpoint that has calling party information. CLID is not transmitted to Single-Line Adapters (SLAs).

To use CLID for single line endpoints:

Enable the Caller ID flag as described on [page 7-23](#).

You must also program the following timers:

- *Caller ID Alerting Tone:* To set this timer:
 - a. Click the number in the **Value** column.
 - b. Enter the number of milliseconds that the system will send Caller ID [CLID] alert tones to the single line endpoint. These tones are not audible to the end user and are used strictly to notify the endpoint that information will be transmitted. This value may differ for various endpoints. The valid range is 88–110 ms, and the default is 100 ms.
- *Caller ID Line Reversal:* To set this timer:
 - a. Click the number in the **Value** column.
 - b. Enter the number of milliseconds that the system reverses the line polarity so that the single line endpoint can receive Caller ID [CLID] information. This value may differ for various endpoints. The valid range is 0–200 ms, and the default is 30 ms.

NOTE	CLIP is not transmitted to Single-Line Adapters (SLAs).
-------------	---

Extension Lists and System Groups

Introduction	8-4
Extension Lists	8-4
Viewing Extension Lists	8-5
Creating Extension Lists	8-5
Adding Devices to Extension Lists	8-5
Deleting Extension Lists	8-6
CO Trunk Groups	8-7
Viewing Trunks in a Trunk Group	8-7
Adding CO Trunk Groups	8-8
Changing CO Trunk Group Extension Numbers	8-8
Moving Trunks Between CO Trunk Groups	8-9
Programming CO Trunk Group Options	8-10
Day or Night Multiple Ring-In Types	8-12
Day or Night Answer Access	8-13
Day or Night Emergency Outgoing Access	8-14
Day or Night Outgoing Access	8-15
Toll Restrictions	8-16
Search Algorithm	8-18
Audio for Calls Camped onto this Device	8-18
Music-On-Hold	8-19
Audio on Transfer To Ring	8-19
Audio On Transfer To Hold	8-20
Audio On Hold For Transfer Announcement	8-21
PRI Call By Call Service	8-21
One-Way Incoming Only	8-22
Echo Trunk Number	8-22
Enable Hookflash	8-23
Camp-Ons Allowed	8-23
ISDN Data Calls Allowed	8-24
Day and Night Ring-In Types	8-24
Send Station Caller ID to Attached PBX	8-26
Propagate Original Caller ID	8-26
Calling Party Name	8-26
Calling Party Number	8-26
Force Trunk Group Calling Party Name and Number	8-27
Wait for ISDN Caller ID Information	8-27

Node Trunk Groups	8-28
Viewing Node Trunk Group Trunk Lists	8-28
Viewing or Changing Node Trunk Group Information	8-28
Programming Node Trunk Group Options	8-28
Emergency Outgoing Access	8-29
Day or Night Outgoing Access	8-30
Search Algorithm	8-30
Camp-Ons Allowed	8-31
ISDN Data Calls Allowed	8-31
Hunt Groups	8-32
ACD Hunt Groups	8-33
Viewing Agent ID Lists	8-33
Creating ACD Agent IDs	8-34
Deleting ACD Agent IDs	8-34
Local Hunt Groups	8-35
Creating Hunt Groups	8-35
Deleting Hunt Groups	8-35
Changing Hunt Group Extensions Numbers	8-36
Local Hunt Group Options	8-37
Agents	8-38
Members	8-40
Supervisors	8-41
Timers	8-42
ACD Agent No Answer – DND Message Additional Text	8-43
ACD Agent No Answer – DND Message Number	8-43
ACD Hunt Group	8-44
Analog Voice Mail Hunt Group	8-44
Announcement and Overflow Endpoints	8-45
Audio for Calls Camped onto this Device	8-45
Audio for Calls Ringing this Device	8-46
Audio for Camped-On Announcement Calls	8-46
Camp-Ons Allowed	8-47
Group Call Pick-Up	8-47
Priority Level	8-47
Recall Destination Endpoint	8-48
Restart ACD Idle Time Upon Login	8-48
Return ACD Calls to Hunt Group	8-49
Search Type	8-49
Send Camp On Notifications to Members in DND	8-50
Use ACD Agent IDs	8-51

Node-Spanning Hunt Groups	8-51
Remote (Off-Node) Hunt Groups	8-51
Network Groups	8-52
Hardware Upgrades	8-52
Network Group Assignments	8-52
Creating Network Group Endpoints and Trunks	8-53
Network Group IP Endpoints	8-53
Network Group Trunks	8-53
Node IP Connection Groups for Remote Nodes	8-54
Node IP Connection Group IP Call Configurations	8-55
Local Music Source	8-55
Music-On-Hold Encoding Setting	8-55
Day/Night Emergency Outgoing Access	8-56
Day/Night Outgoing Access	8-56
Remote Node	8-57
Camp-Ons Allowed	8-57

Introduction

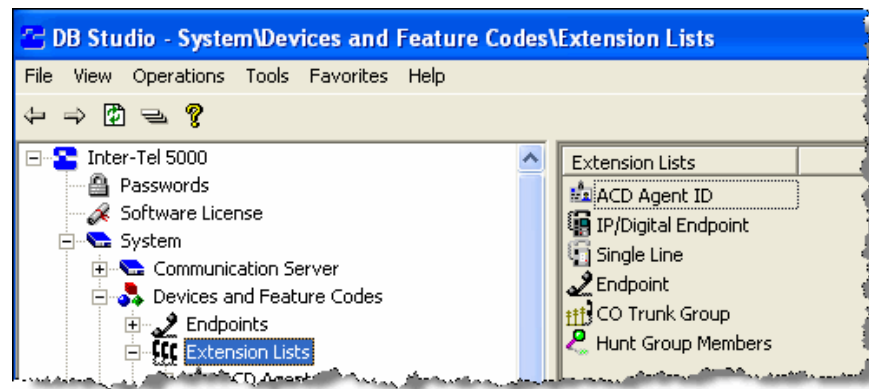
This chapter includes programming instructions for Mitel 5000 groups and lists. Groups and lists can be composed of system users, trunks, or system features. This chapter covers the following system groups and lists:

- “Extension Lists” below
- “CO Trunk Groups” on [page 8-7](#)
- “Network Groups” on [page 8-52](#)
- “Node Trunk Groups” on [page 8-28](#)
- “Hunt Groups” on [page 8-32](#)

Extension Lists

An extension list, as shown in [Figure 8-1](#), is a group of intercom extensions or trunk group extensions. You can use extension lists when you use program features that use common lists. For example, a group of endpoints could be assigned to the same paging zone and have ring-in for the same trunk groups. With an extension list, you would have to enter only one list number instead of entering all of the extensions. Extension lists of endpoints can also be included in hunt groups.

Figure 8-1. *Extension Lists*



The following are Extension List types:

- **ACD Agent ID:** Includes only ACD hunt group Agent IDs. If no Agent IDs have been created, as described on [page 8-33](#), this option cannot be used.
- **IP/Digital Endpoint:** Includes only endpoint extension numbers. The Auto: All IP/Dgtl Endpts (PP052) extension list is provided by default and cannot be deleted. This list contains all of the endpoints programmed and is automatically updated when endpoints are added/deleted.
- **Single Line:** Includes only single line endpoint and MDPM extension numbers.
- **Endpoint:** Can include endpoints, MDPMs, and/or single line extension numbers. The Auto: All Endpoints (PP051) extension list is provided by default and cannot be deleted. This list contains all of the endpoints programmed and is automatically updated when endpoints are added or deleted.

NOTE

You cannot change or delete the Auto: All Endpoints or Auto: All IP/Digital Endpoints extension lists.

- **CO Trunk Group:** Includes only trunk group access numbers.
- **Hunt Group Members:** Includes only endpoints that are members of hunt groups.

Viewing Extension Lists

To view the available lists:

1. Select System – Devices and Feature Codes – **Extension Lists** – *<extension list type>*.
2. Select the extension list.

Creating Extension Lists

NOTICE

Adding a large extension list can result in slowing down system performance. Adding an Extension List that contains more than 60 members may cause a system slowdown because when the list is called, ALL members of the list are called at the same time.

When using an extension list for ring-in or hunt groups, do not exceed 30 endpoints per list. The system can send ring signal to up to 30 endpoints.

The number of entries in individual lists limits the total number of extension lists allowed on the system. In all of the extension lists combined, a maximum of 2500 endpoint or trunk extensions entries is allowed.

To create an extension list:

1. Select System – Devices and Feature Codes – **Extension Lists**.
2. Select the type of list you want to create.
3. Right click in the right pane, and then click **Create <type> Extension List**. The Create Extension List dialog box appears.
4. In the **Starting Extension** box, select or enter the starting extension for the new list.
5. In the **Number of Extensions** box, select or enter the number of extensions that you want to add.
6. Click **OK**.
7. The new list automatically appears in the list for that extension list type.
8. Select **Description**, and type the name, up to 20 characters, in the box.
9. When finished, press **ENTER** or click out of the field to save the change.

Adding Devices to Extension Lists

You can add devices to extension lists.

To program a list:

1. Select System – Devices and Feature Codes – Extension Lists – *<extension list type>*.
2. Select the extension list.
3. Right-click anywhere in the right pane, and then click **Add To List**. A window appears prompting for the device types to include.
4. Select the device types (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The devices with details appear. To view devices in a list only, click **List**.
5. Select the devices you want to add to the list, and then click **Finish**. The selection appears in the extension list window.

Deleting Extension Lists

To delete an extension list:

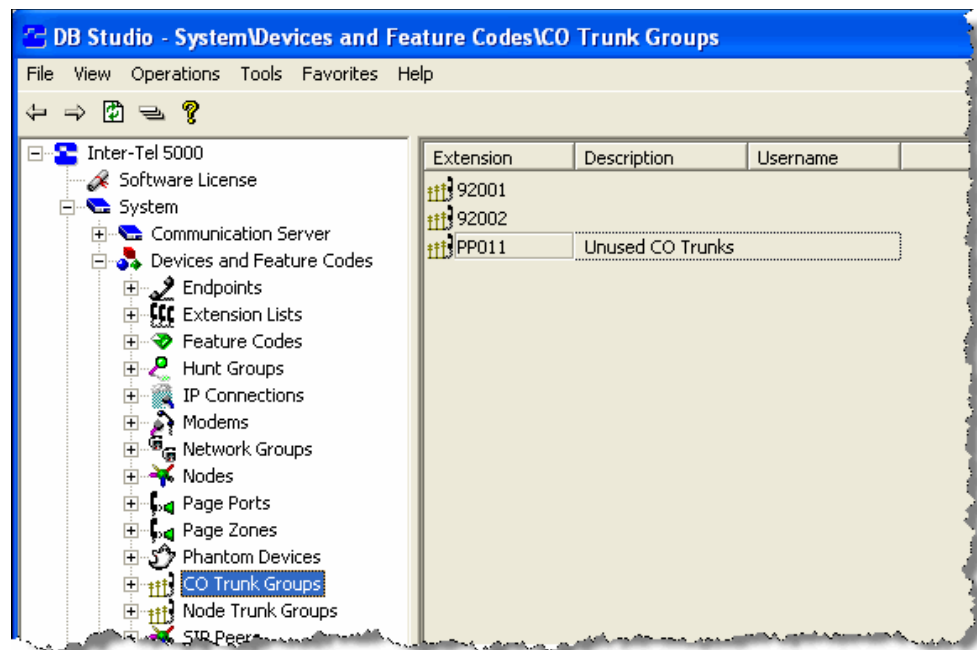
1. Select System – Devices and Feature Codes – Extension Lists – *<extension list type>*.
2. Select the extension list.
3. Right-click and select Delete. The extension list is removed.

CO Trunk Groups

Central Office (CO) trunk groups bundle system trunks into one group, or trunk group. Whenever a call is placed from a trunk in a CO trunk group, the system hunts for an available trunk to route the call out to the CO. Calls placed to CO trunk groups are routed according to the first available trunk.

Because MGCP and SIP trunks are CO trunks, they can also be in a CO Trunk group and need the applicable IP resources to be able to place calls. For more information, see “SIP Gateways” on [page 6-6](#) or “MGCP Gateways, Devices, and Trunks” on [page 6-9](#). 92001 is the default baseline extension used for CO Trunk Groups; PP011 the default CO trunk group for unused trunk groups. You can view CO trunk groups programmed for the local node, as shown in [Figure 8-2](#).

Figure 8-2. CO Trunk Groups



To view CO trunk groups:

Select System – Devices and Feature Codes – **CO Trunk Groups**.

Viewing Trunks in a Trunk Group

Individual trunks are assigned to trunk groups. You can view and edit the trunks in each trunk group.

To view the trunks assigned to a trunk group:

Select System – Devices and Feature Codes – CO Trunk Groups – *<trunk group number>* – **Trunks**.

Adding CO Trunk Groups

You can add CO trunk groups.

To add a CO trunk group:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Right-click in the right pane, and then select **Create CO Trunk Group**. The Create CO Trunk Group Extension dialog box appears.
3. Enter the starting extension and number of extensions for the new trunk group, and then click **OK**.
4. Program the **Description** and **Username** fields. All trunk groups should have a description and a username. The description appears in all trunk group lists in the database and can be up to 20 characters long. The username appears on endpoint displays and can have up to 10 characters.

To program the Description and Username fields:

- a. Select the box that you want to program.
- b. Type the entry.
- c. Press **ENTER** or click out of the field to save your changes.

Changing CO Trunk Group Extension Numbers

You can change either individual or multiple trunk group extension numbers.

To change an individual trunk group extension number:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the current extension number.
3. Select the new number from the list or type the number in the list box.
4. Press **ENTER** or click out of the box to save your changes.

To change multiple trunk group extension numbers at one time:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group extensions that you want to change. You can use the SHIFT or CTRL key to select more than one extension.
3. Right-click, and then select **Batch Extension Change**. The Create CO Trunk Group dialog box appears.
4. Select the number you want to assign to the first selected trunk group (the other trunk groups will be numbered consecutively after this number).
5. Click **OK**. The trunk groups are automatically renumbered and resorted in the endpoint list.

Moving Trunks Between CO Trunk Groups

You can move trunks between trunk groups.

To move trunks to from another trunk group into the selected trunk group:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Double-click **Trunks**, and then right-click in a blank area in the right pane.
4. Click **Move To Trunks List**. A window appears prompting for the device type to include.
5. Select the trunk types, and then click **Next**. A list of available trunks with details appears. To view trunks in a list only, click **List**.
6. Select the appropriate trunks, and then select **Move Items**.
7. When you have added all the desired trunks, click **Finish**. The selections appear in the list.

To move trunks out of the selected trunk group to another trunk group:

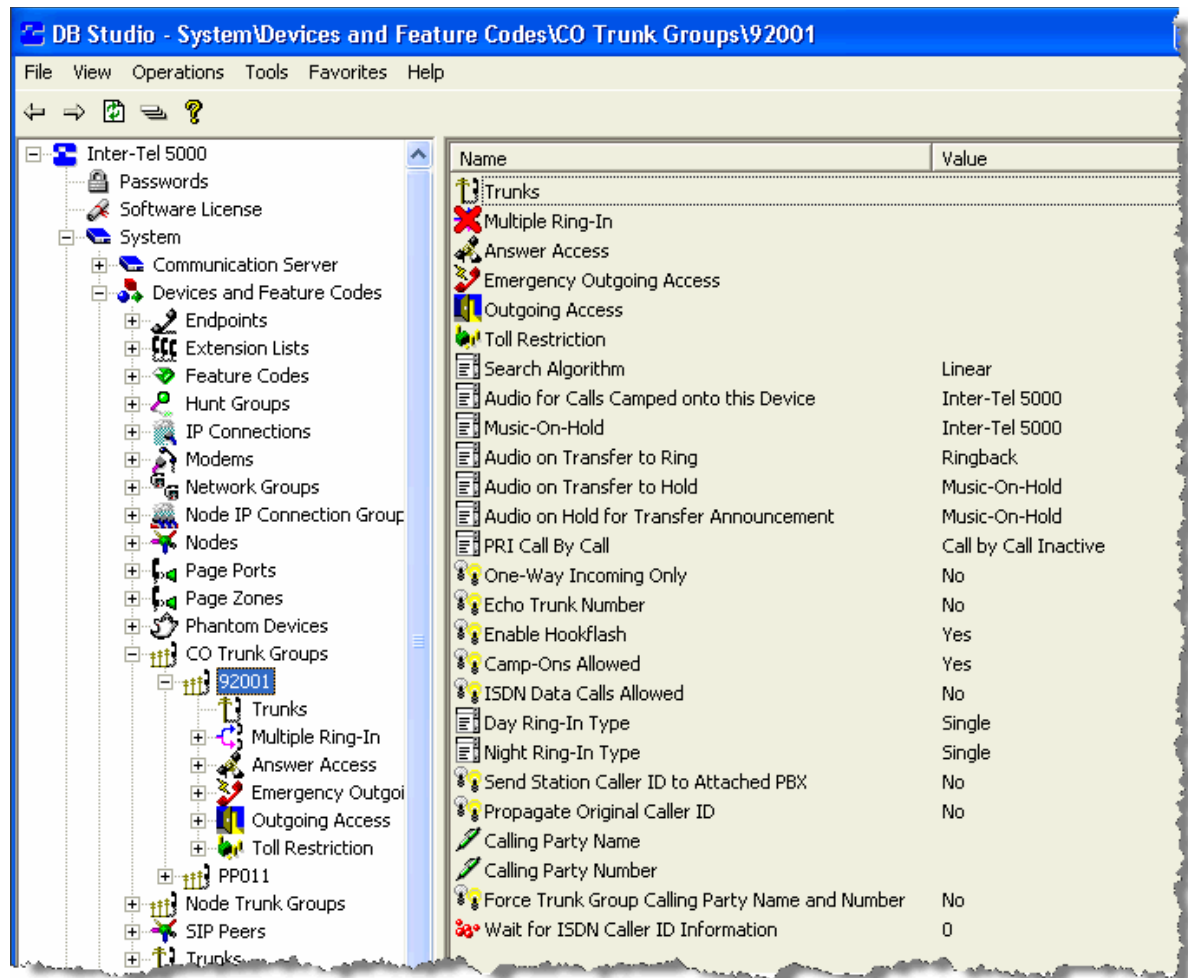
1. Select System – Devices and Feature Codes – CO Trunk Groups – *<trunk group>*.
2. Double-click **Trunks**.
3. Drag and drop the trunks into the trunk list of the new trunk group. Use the **CTRL** or **SHIFT** keys to select several trunks at a time.

Programming CO Trunk Group Options

You can program the following CO trunk group options, as shown in Figure 8-3 on [page 8-11](#). To assign trunks to CO trunk groups, see “Assigning Trunks to CO Trunk Groups” on [page 6-5](#).

- “Day or Night Multiple Ring-In Types” on [page 8-12](#)
- “Day or Night Answer Access” on [page 8-13](#)
- “Day or Night Emergency Outgoing Access” on [page 8-14](#)
- “Day or Night Outgoing Access” on [page 8-15](#)
- “Toll Restrictions” on [page 8-16](#)
- “Search Algorithm” on [page 8-18](#)
- “Audio for Calls Camped onto this Device” on [page 8-18](#)
- “Music-On-Hold” on [page 8-19](#)
- “Audio on Transfer To Ring” on [page 8-19](#)
- “Audio On Transfer To Hold” on [page 8-20](#)
- “Audio On Hold For Transfer Announcement” on [page 8-21](#)
- “PRI Call By Call Service” on [page 8-21](#)
- “One-Way Incoming Only” on [page 8-22](#)
- “Echo Trunk Number” on [page 8-22](#)
- “Enable Hookflash” on [page 8-23](#)
- “Camp-Ons Allowed” on [page 8-23](#)
- “ISDN Data Calls Allowed” on [page 8-24](#)
- “Day and Night Ring-In Types” on [page 8-24](#)
- “Send Station Caller ID to Attached PBX” on [page 8-26](#)
- “Propagate Original Caller ID” on [page 8-26](#)
- “Calling Party Name” on [page 8-26](#)
- “Calling Party Number” on [page 8-26](#)
- “Force Trunk Group Calling Party Name and Number” on [page 8-27](#)
- “Wait for ISDN Caller ID Information” on [page 8-27](#)

Figure 8-3. CO Trunk Group Options



Day or Night Multiple Ring-In Types

If the Ring-In Type (see [page 8-24](#)) is set to “Multiple,” you can determine the ring-in destinations for day and night modes. The trunk group can ring in to a list of endpoints, extension lists, or applications, (but not hunt groups). The list can include local or off-node device extension numbers. When using an extension list for ring-in, do not exceed 30 endpoints for each list.

To set the ring-in destination:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Double-click **Multiple Ring-In**, and then double-click **Day** or **Night**.
4. Add destinations to the list:
 - a. Right-click anywhere in the right pane, and then click **Add to Day** (or **Night**) **List**. The Add to Day (or Night) dialog box appears.
 - b. Select the device types (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
 - c. Select the appropriate items, and then click **Add Items**.
 - d. Click **Finish**. The selections appear in the list. To view programming options, double-click the extension number.

To delete destinations from the list:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **Multiple Ring-In**, and then select **Day** or **Night**.
4. Select the item, right-click, and then select **Remove Selected Items**.

Day or Night Answer Access

This feature is not available for DISA trunks. Day or Night Answer Access allows endpoint users to answer incoming calls on the trunks in that trunk group (even if the endpoint does not have ring-in assignment for that trunk group). Endpoints cannot have allowed-answer assignment for trunk groups on other nodes.

To program trunk-group extensions for allowed-answer permission in day or night mode:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **Answer Access**, and then select **Day Mode** or **Night Mode**.
4. To add extensions to the list:
 - a. Right-click anywhere in the right side of the window. An option box appears.
 - b. Select **Add To List**. A window appears prompting for the device type to include.
 - c. Select the device types (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
 - d. Select the appropriate items, then select **Add Items**. When you have added all the desired devices, click **Finish**. The selections appear in the list. To view programming options, double-click the extension number.

To delete destinations from the list:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **Answer Access**, and then select **Day Mode** or **Night Mode**.
4. Select the extension number.
5. Right-click, and then select **Remove Selected Items**.

Day or Night Emergency Outgoing Access

You can program emergency outgoing access for day or night mode. For loop start trunks that are connected to paging equipment, the emergency outgoing access designation does *not* keep the endpoint from seizing the trunk for paging. Trunks used for paging should not allow any endpoint to have emergency outgoing access. By default, the automatic endpoint list (Auto: All Endpoints) is assigned to Day/Night Emergency Outgoing Access.

To add endpoints with emergency outgoing access for the trunk group:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **Emergency Outgoing Access**, and then select either **Day Mode** or **Night Mode**.
4. Right-click anywhere in the right side of the window. An option box appears.
5. Select **Add To List**. A window appears prompting for the device type to include.
6. Select the device types (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
7. Select the appropriate items, then select **Add Items**. When you have added all the desired devices, click **Finish**. The selections appear in the list. To view programming options, double-click the extension number.

To delete destinations from the list:

1. Select **Emergency Outgoing Access**, then select either **Day Mode** or **Night Mode**.
2. Select the item, right-click, and then select **Remove Selected Items**.

NOTICE

Responsibility for Regulatory Compliance.

It is the responsibility of the organization and person(s) performing the installation and maintenance of Mitel Advanced Communications Platforms to know and comply with all regulations required for ensuring Emergency Outgoing Access at the location of both the main system and any remote communication endpoints. Remote IP and SIP endpoints may require gateway access to nearby emergency responders.

Emergency Call phone numbers include:

- 911, the default for Mitel systems located in the U.S.
- 999, the default for Mitel systems located in the European market and used primarily in the U.K.
- If applicable, 112, an emergency number used widely in Europe outside of the U.K.
- Any emergency number, such as for a police or fire station, that is appropriate for the location of the main system and/or remote endpoints.

Day or Night Outgoing Access

There are separate lists for endpoints with outgoing access in day and night modes. On loop start trunks that are connected to paging equipment, the outgoing access designation does not keep the endpoint from seizing the trunk for paging. Trunks used for paging should not allow any endpoint to have outgoing access for placing outside calls. By default, the automatic endpoint list (Auto: All Endpoints) is assigned to Day/Night Outgoing Access when a CO trunk group is created.

To add endpoints that will have outgoing access for the trunk group:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **Outgoing Access**, and then select either **Day Mode** or **Night Mode**.
4. Right-click anywhere in the right side of the window. An option box appears.
5. Select **Add To List**. A window appears prompting for the device type to include.
6. Select the device types (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
7. Select the appropriate items, then select **Add Items**. When you have added all the desired devices, click **Finish**. The selections appear in the list. To view programming options, double-click the extension number.

To delete destinations from the list:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **Outgoing Access**, and then select either **Day Mode** or **Night Mode**.
4. Select the item, right-click, and then click **Remove Selected Items**.

Toll Restrictions

You can program toll restrictions for each trunk group. For more information about toll restrictions and classes of service, refer to the System Features chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

To program toll restriction for the trunk group:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **Toll Restriction**.
4. Program the following toll restriction parameters for each trunk group. For loop start trunks that are connected to paging equipment, toll restriction does not keep the endpoint from seizing the trunk for paging.
 - **Class Of Service:** Each trunk group has Classes of Service (COS), which restrict or allow certain dialing patterns from being dialed on a call.

NOTE

When determining toll restriction for an ARS outgoing call, the network only checks the endpoint toll restriction for the node on which the calling endpoint resides. The system does not check the trunk class of service for ARS calls. To program the toll restrictions, double-click **Classes of Service**, you then have the option of choosing Day or Night. Double-click the desired time period to view a list of current classes of service.

To add a class of service:

- a.) Right-click in the window and select **Add To List**.
- b.) A window appears prompting for the toll restriction types you want to program. Select **ARS Only & Deny Area/Office** and/or **Classes of service**, and then click **Next**.
- c.) Another window appears displaying a list of available classes of service with details. To view items in a list only, click **List**.
- d.) Select the classes of service, and then select **Add Items**. The selected classes of service appear in the list. Click **Finish** to exit.
- e.) *(U.S. only)* If you selected **Deny Area/Office** class of service, the trunk group must also be assigned to a User Group. To change the user group, right-click **User Group** and select **Change User Group**. In the first window that appears, select **User Groups**, then click **Next**. In the next window, select the desired user group, and then click **Finish** to exit and save the change.

To delete one or more classes of service:

- a.) Select the items.
 - b.) Right-click, and then select **Remove Selected Items**. To select a series of items, hold down SHIFT while selecting the first and last item in the range. To select two or more that are not consecutive, hold down CTRL while selecting the desired items.
- **Subject to toll restriction:** If the trunk group is not subject to toll restriction, the endpoint and trunk classes of service (except ARS-Only restriction) are not checked when a trunk in the group is used.

To enable this option:

- a.) Select the current value, and then select the check box. The field changes to **Yes**. To disable the flag, clear the check box.
- b.) Press **ENTER** or click out of the field to save your changes.

- **Exempt from ARS only:** The trunk group can be exempt from, or subject to, the ARS-only restriction. If exempt from ARS-only, endpoints with that restriction can directly select the trunks. If subject to ARS-only, ARS-restricted endpoints can use the trunk group only if it is part of an ARS route group.

To enable this option:

- a.) Select the current value, and then select the check box. The field changes to **Yes**. To disable the flag, clear the check box.
- b.) Press **ENTER** or click out of the field to save your changes.

- **Assigned Call Cost:** For trunk groups that are not subject to toll restriction, the call cost rate to be used for calls placed on the trunks can be free, local, toll local, toll long distance, operator-assisted, or international rate for the U.S. and free, local, toll (national), international, or operator rate for Europe.

To change the Call Cost setting:

- a.) Select the Assigned Call Cost value, then scroll to the desired setting.
- b.) Press **ENTER** or click outside the field to save the change.

- **Absorbed Digits:** Trunk groups can be programmed to absorb digits in areas where the first digit(s) of the office code are absorbed. There can be up to 50 patterns with up to 48 digits each.

To enable the option:

- a.) Select the current value, and then select the check box. The field changes to **Yes**. To disable the flag, clear the check box.
- b.) Press **ENTER** or click out of the field to save your changes.

- **Absorbed Patterns:** If the Absorbed Digits and PBX Line flags are enabled, use this field to enter the absorbed digit patterns. There can be up to 50 patterns with up to 48 digits each. The only characters allowed in the pattern are digits (0-9), pound (or hash) sign (#), parentheses (), brackets ([]), greater than (>) and less than (<) symbols, and the wildcards. (See [page 7-14](#) for wildcard information.) Double-click **Absorbed Patterns** to view the current list of patterns, if any.

To add a pattern, do the following:

- a.) Right-click anywhere in the right side of the screen and select **Add To Absorbed Patterns List**. A new, blank pattern appears on the list.
- b.) Select the pattern to display the text box, then enter the desired pattern.
- c.) Press **ENTER** or click outside the field to save the change.
- d.) Repeat these steps if you need additional patterns.

- **PBX Line:** Trunk groups can be programmed to absorb a digit string (defined above) for PBX installations.

To enable this option:

- a.) Select the current value, and then select the check box. The field changes to **Yes**. To disable the flag, clear the check box.
- b.) Press **ENTER** or click out of the field to save your changes.

- **Absorbed Digit String:** If the PBX Line flag, described above, is enabled, use this field to enter the absorbed digit string.

To change the Absorbed Digit String:

- a.) Click the current value, then enter the new digit string, up to 32 digits.
- b.) Press **ENTER** or select another field to save the change. The only characters allowed in the string are digits (0–9), pound (or hash) sign (#), parentheses (), brackets ([]), greater than (>) and less than (<) symbols, and the wildcards. For more information about wildcards, see “Using the Wildcard Character in Off-Node Extensions” on [page 7-14](#).

Search Algorithm

You can program trunk groups to search trunk availability in either linear or distributed order:

- **Linear:** Requests for an outgoing trunk are always processed beginning with the highest numbered trunk on the list and moving down the list until an available trunk is found.
- **Distributed:** The first request will be processed beginning with the highest numbered trunk on the list. The next request will begin with the second trunk, and each subsequent request will begin one trunk lower on the list. When the end of the list is reached, requests begin again with the highest numbered trunk on the list.

To change the trunk group searching algorithm:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **Search Algorithm**.
4. In the **Value** column, select the setting.
5. Press **ENTER** or click outside the field to save the change.

Audio for Calls Camped onto this Device

You can select the audio that callers hear when camped-on to the trunk group.

To select the Audio for Calls Camped onto this Device:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **Audio for Calls Camped onto this Device**.
4. In the **Value** column, select one of the following options from the list:
 - **Silence:** Callers hear no Music-On-Hold.
 - **Tick Tone:** Callers hear tick tone.
 - **Ringback:** Callers hear ringback.
 - **Inter-Tel 5000:** Callers hear an external music source. This is the default value.
 - **File-Based MOH:** Callers hear the MOH file selected in DB Programming. For more information, see “File-Based Music-On-Hold (MOH)” on [page 10-9](#).
5. Press **ENTER** or click outside the field to save the change.

Music-On-Hold

You can select the audio that callers hear when placed on hold for the trunk group.

To select the Music-on-Hold audio:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **Music-On-Hold**.
4. In the **Value** column, select one of the following options from the list:
 - **Silence**: Callers hear no Music-On-Hold.
 - **Tick Tone**: Callers hear tick tone.
 - **Ringback**: Callers hear ringback.
 - **Inter-Tel 5000**: Callers hear an external music source. This is the default value.
 - **Use Next Device's Audio Source**: Callers hear the audio programmed at individual endpoints. See “Audio for Calls Holding for this Device” on [page 7-65](#).
 - **File-Based MOH**: Callers hear the MOH file selected in DB Programming. For more information, see “File-Based Music-On-Hold (MOH)” on [page 10-9](#).
5. Press **ENTER** or click outside the field to save the change.

Audio on Transfer To Ring

You can select the audio that outside callers (except those using DISA) hear while their call is being transferred. The audio that DISA callers hear is determined by how the DISA Transfer tone system flag is programmed (see [page 10-20](#)).

To select the Audio on Transfer to Ring:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **Audio on Transfer to Ring**.
4. In the **Value** column, select one of the following options from the list:
 - **Silence**: Callers hear no Music-On-Hold.
 - **Tick Tone**: Callers hear tick tone.
 - **Ringback**: Callers hear ringback. This is the default value.
 - **Inter-Tel 5000**: Callers hear an external music source.
 - **Music-On-Hold**: Callers hear the default system Music-On-Hold source.
 - **Use Next Device's Audio Source**: Callers hear the audio programmed at individual endpoints. See “Device Audio for Calls Settings” on [page 7-65](#).
 - **File-Based MOH**: Callers hear the MOH file selected in DB Programming. For more information, see “File-Based Music-On-Hold (MOH)” on [page 10-9](#).
5. Press **ENTER** or click outside the field to save the change.

Audio On Transfer To Hold

You can select the audio that outside callers (except those using DISA) hear when they are transferred to and held at a different extension. The audio that DISA callers hear is determined by how the DISA Transfer tone system flag is programmed (see [page 10-20](#)).

To select the Audio on Transfer To Hold:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **Audio on Transfer to Hold**.
4. In the **Value** column, select one of the following options from the list:
 - **Silence**: Callers hear no Music-On-Hold.
 - **Tick Tone**: Callers hear tick tone.
 - **Ringback**: Callers hear ringback.
 - **Inter-Tel 5000**: Callers hear an external music source.
 - **Music-On-Hold**: Callers hear the default Music-On-Hold source. This is the default value.
 - **Use Next Device's Audio Source**: Callers hear the audio programmed at individual endpoints. See "Device Audio for Calls Settings" on [page 7-65](#).
 - **File-Based MOH**: Callers hear the MOH file selected in DB Programming. For more information, see "File-Based Music-On-Hold (MOH)" on [page 10-9](#).
5. Press **ENTER** or click outside the field to save the change.

Audio On Hold For Transfer Announcement

You can select the audio that outside callers (except those using DISA) hear while on transfer hold. After the transfer is completed, the caller hears the Audio On Hold For Transfer Announcement selection. The audio that DISA callers hear is determined by how the DISA Transfer tone system flag is programmed (see [page 10-20](#)).

If the trunk group audio field, including Music-On-Hold, is set to Use Next Device's Audio Source, the system uses the programming for the next device as programmed for the Day/Night trunk group destination. If the field is set to any other option, the system uses the trunk group audio source, overriding endpoint programming.

To select the Audio On Hold For Transfer Announcement:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **Audio On Hold for Transfer Announcement**.
4. In the **Value** column, select one of the following options from the list:
 - **Silence**: Callers hear no Music-On-Hold.
 - **Tick Tone**: Callers hear tick tone.
 - **Ringback**: Callers hear ringback.
 - **Inter-Tel 5000**: Callers hear an external music source.
 - **Music-On-Hold**: Callers hear the default Music-On-Hold source. This is the default value.
 - **Use Next Device's Audio Source**: Callers hear the audio programmed at individual endpoints. See "Device Audio for Calls Settings" on [page 7-65](#).
 - **File-Based MOH**: Callers hear the MOH file selected in DB Programming. For more information, see "File-Based Music-On-Hold (MOH)" on [page 10-9](#).
5. Press **ENTER** or click outside the field to save the change.

PRI Call By Call Service

This feature applies to U.S. installations only. If your trunk group uses PRI B-channels, you can select the PRI Call By Call service for outgoing calls. For a list of supported services, refer to the *Mitel 5000 Reference Manual*, part number 580.8007.

To select the PRI Call By Call Service:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **PRI Call By Call**, and then select the service from the list.
4. Press **ENTER** or click outside the field to save the change.

One-Way Incoming Only

You must designate certain types of trunks, such as incoming Wide Area Telecommunications Service (WATS), as "incoming-only," so the system recognizes the lines during power-up or testing. On these types of trunks, battery is not returned when the line is seized and the system cannot power up the trunk *unless* this option is enabled.

To program a trunk as One-Way Incoming Only:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **One-Way Incoming Only**.
4. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.

NOTE

When the check box is selected, the system checks to determine whether any endpoints have outgoing access for that trunk group. If there are endpoints with outgoing access, a message prompts you to delete the outgoing-access assignments for those endpoints. Select **Yes** to remove the outgoing-access assignments, or select **No** to allow outgoing access.

5. Press **ENTER** or click out of the field to save the change.

Echo Trunk Number

When the Echo Trunk Number option is enabled, the system echoes the trunk number, DNIS, DID (or DDI in Europe), and so on, if the call is being routed out on a trunk. The base digits are combined with the collected trunk number to create an outside number. If the trunk rings into another trunk in the system through an individual trunk, trunk group, or ARS, the trunk number is dialed as the outgoing number.

NOTE

If the collected trunk number is incomplete or invalid, the collected digits are not used for the outside number, to avoid the system from dialing the wrong outside number.

To program the Echo Trunk Number:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **Echo Trunk Number**.
4. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
5. Press **ENTER** or click out of the field to save the change.

Enable Hookflash

You can enable or disable the Hookflash [Recall] feature for each trunk group. If disabled, endpoint users cannot use the Hookflash feature code (330) while using the trunks in the trunk group. Hookflashes [Recalls] dialed through ARS are ignored by the trunk groups with hookflash [recall] disabled.

To enable hookflash:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **Enable Hookflash**.
4. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
5. Press **ENTER** or select another field to save the change.

Camp-Ons Allowed

The Camp On feature can be enabled or disabled for each trunk group. If disabled, users placing outgoing calls will hear busy signals when all trunks in the group are in use or unavailable. If enabled, users will be able to camp on and wait for an available trunk.

To enable Camp-Ons Allowed:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **Camp-Ons Allowed**.
4. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
5. Press **ENTER** or select another field to save the change.

ISDN Data Calls Allowed

This is a BRI-only trunk. This option allows you to prevent ISDN data calls from being routed to trunk groups containing trunks that cannot support data calls, such as loop start trunks.

- When set to **Yes**, the system can route ISDN data calls to this trunk group, and you are allowed to add B-channel trunks only to the group.
- If the flag is set to **No**, the system will not route ISDN data calls to this trunk group, and you can add any type of trunk, except private networking B-channel trunks, to the group. Any non-B-channel trunks must be removed from the CO trunk group before the flag can be set to Yes. If you move multiple trunks into a CO trunk group that has this flag enabled, you will be warned that none of the trunks will be added to the group if any of the trunks to be added are non-B-channel trunks.

To enable ISDN Data Calls Allowed:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **ISDN Data Calls Allowed**.
4. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
5. Press **ENTER** or select another field to save the change.

Day and Night Ring-In Types

Ring-in type is determined separately for day and night modes.

To set the Ring-In Type:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **Day** (or **Night**) **Ring-In Type**, and then select the option from the list.
4. Press **ENTER** or click out of the field to save the change. When using an extension list for ring-in or hunt groups, do not exceed 30 endpoints per list. The system can send ring signal to up to 30 endpoints simultaneously. The Ring-In Type can be the same for both modes, or any combination of the following can be used:
 - **Single**: The trunk group can ring at a single extension number or a hunt group. This can be a local or off-node extension number. When you select Single, you must also enter the destination extension in the Ring-In column. Use one of the following methods:

Method A

- a.) Select the current Value, then enter the new value in the text box.
- b.) Press **ENTER**. A screen displays what is associated with the number entered.
- c.) Click **OK**. The new number appears in the field.

Method B

- a.) Right-click the existing value. An option box appears.
- b.) Click **Change Extended Value**. The Change Extended Value dialog box appears.
- c.) Select the appropriate device type, and then click **Next**. The list of devices appears. To view devices in a list only, click **List**.
- d.) Select the device you want to use, then click **Finish**. The selection appears in the Ring-In field.

- **Multiple:** The trunk group can ring in to a list of endpoints, extension lists, and/or applications (but not hunt groups). The list can include local or off-node device extension numbers. Set the ring-in destination as described on [page 8-12](#).
- **DISA:** If the trunk group is to be used for DISA, a security code can be assigned by selecting the Ring-In field and entering the code in the text box. To prevent unauthorized access to the public network, **all** trunk groups using DISA should have a security code.
- **Call Routing Table:** If the trunk is used for Caller ID [CLID in Europe], DID/DNIS, or ANI, the calls can be routed according to the information sent by the CO. For more information about Call Routing Tables, refer to the "System Features" chapter in the *Mitel 5000 Reference Manual*, part number 580.8007. When you select Call Routing Table, you must also enter the destination table in the Ring-In column, using one of the following methods:

Method A

- a.) Select the current Value, then enter the new value in the text box.
- b.) Press **ENTER**. A screen appears displaying what is associated with the number entered.
- c.) Click **OK**. The new number appears in the field.

Method B

- a.) Right-click the existing value. An option box appears.
 - b.) Click **Change Extended Value**. The Change Extended Value dialog box appears.
 - c.) Select **Call Routing Table**, and then click **Next**. The list of tables appears. To view tables in a list only, click **List**.
 - d.) Select the table you want to use, then click **Finish**. The selection appears in the Ring-In field. Loop start trunks that are connected to paging equipment should not have any ring-in designations. They should be reserved for internal use only.
- **Collected Digits:** This ring-in type indicates that the collected DID [DDI in Europe] or DNIS digits (plus the base digits) should be used as the destination extension. This helps to keep the number of call routing table entries down to a minimum when routing calls to extensions.

Both trunk groups and call routing table entries can use the new ring-in type. When the new Ring-In Type of Collected Digits is selected, the Ring-In Destination field is empty.

If the collected digits plus the base digits do not make up a valid ring-in destination, the call is routed to the primary attendant. Valid ring-in destinations include on- or off-node endpoints, on- or off-node hunt groups, trunk groups, individual trunks, voice mail applications, automated attendants, and ARS.

Send Station Caller ID to Attached PBX

ISDN trunks only. Send Station Caller ID to Attached PBX allows the username and extension in the ISDN setup request message to be sent on an outgoing ISDN call. All intercom calls that route externally from the system via an ISDN circuit will send the username and extension for the caller ID name and number instead of the Calling Party Number or Name information. For more information, refer to the System Features chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

To propagate a calling endpoint username and extension to an attached PBX:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **Send Station Caller ID to Attached PBX**.
4. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
5. Press **ENTER** or click another field to save the change.

Propagate Original Caller ID

Propagate Original Caller ID allows the system to pass the caller ID name or number on an outgoing ISDN call if the call has not been answered by the system (extension, voice mail, hunt groups, or OAI application) or for transfer announcement calls. This option is for customers that want to route incoming calls from the Mitel 5000 platform back to the PSTN through ISDN lines. For more information, refer to the System Features chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

To route incoming calls from the Mitel 5000 platform back to the PSTN via ISDN lines:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **Propagate Original Caller ID**.
4. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
5. Press **ENTER** or click another field to save the change.

Calling Party Name

You can program the Calling Party Name option for the trunk group. For more information about the Calling Party name option, see “Calling Party Name” on [page 7-63](#).

Calling Party Number

You can program the Calling Party Number option for the trunk group. For more information about the Calling Party name option, see “Calling Party Number” on [page 7-64](#).

Force Trunk Group Calling Party Name and Number

When selected, the system uses the trunk group Calling Party Name and Calling Party Number. When cleared, the system follows the Caller ID forwarding option enabled for the trunk group. This allows the Caller ID to be the callback number (for example, a main number, cell number, and so on) without losing the ability to identify the location of the emergency call.

To enable the Force Trunk Group Calling Party Name and Number option:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **Force Trunk Group Calling Party Name and Number**.
4. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
5. Press **ENTER** or click another field to save the change.

Wait for ISDN Caller ID Information

The Wait for ISDN Caller ID Information timer determines the amount of time the system waits (in seconds) for the incoming ISDN Facility message that contains the caller ID name before routing the call to the ring-in destination. This timer only applies to incoming ISDN calls that use Facility messages instead of Display messages for providing caller ID name. For more information, refer to the System Features chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

To set the Wait for ISDN Caller ID Information timer:

1. Select System – Devices and Feature Codes – **CO Trunk Groups**.
2. Select the trunk group number.
3. Select **Wait for ISDN Caller ID Information**.
4. In the **Value** column, enter the time (in seconds).
5. Press **ENTER** or click another field to save the change.

Node Trunk Groups

Node trunk groups are created when the T1/PRI, or E1/PRI Switch Type is set to Private Networking or IP Private Networking. For more information, refer to the Installation Chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

At the main level, you can program the description and user name for each node trunk group. You can also see which bay contains the circuits used for this network connection.

Viewing Node Trunk Group Trunk Lists

When the T1/PRI or E1/PRI module Switch Type is programmed for Private Networking, all of its B-Channels are automatically assigned to a node trunk group. You can double-click Trunks to view this list, but you cannot change it. For more information about T1 or E1 programming, refer to the Installation chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

To view a Node Trunk Group List:

1. Select System – Devices and Feature Codes – **Node Trunk Groups**.
2. Select the trunk group number.

Viewing or Changing Node Trunk Group Information

Node trunk group trunks show the following information:

- **Description and User name:** All node trunk groups should have a description and a user name.
- **Associated Bay Number:** This is the bay number where the module associated with this node trunk group is located. This field is for reference only and cannot be changed.

When the T1/E1/PRI or Dual T1/E1/PRI module's Switch Type is programmed for Private Networking, all of its B-Channels are automatically assigned to a node trunk group. You can view the list but you cannot change it.

To program the Description or Username fields:

1. Select System – Devices and Feature Codes – **Node Trunk Groups**.
2. Select the trunk group number.
3. Select the **Description** or **Username** field, and then type the new name in the box. The description that appears in all node trunk group lists in the database can be up to 20 characters long. The username, that appears on display endpoints, can have up to 10 characters.
4. Press **ENTER** or click another field to save the change.

Programming Node Trunk Group Options

You can program the following Node Trunk Group options:

- "Emergency Outgoing Access" on [page 8-29](#)
- "Day or Night Outgoing Access" on [page 8-30](#)
- "Search Algorithm" on [page 8-30](#)
- "Camp-Ons Allowed" on [page 8-31](#)
- "ISDN Data Calls Allowed" on [page 8-31](#)

Emergency Outgoing Access

There are separate lists for endpoints with emergency outgoing access in day and night modes. By default, the automatic endpoint list (Auto: All Endpoints) is assigned to Day/Night Emergency Outgoing Access.

To add endpoints that will have emergency outgoing access for the node trunk group:

1. Select System – Devices and Feature Codes – **Node Trunk Groups**.
2. Select the trunk group number.
3. Select **Emergency Outgoing Access**, and then select either **Day Mode** or **Night Mode**.
4. Right-click anywhere in the right side of the window. An option box appears.
5. Select **Add To List**. A window appears prompting for the device type to include.
6. Select the device types (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
7. Select the appropriate items, then select **Add Items**. When you have added all the desired devices, click **Finish**. The selections appear in the list. To view programming options, double-click the extension number.

To delete items or destinations from the list:

1. Select **Emergency Outgoing Access**, then select either **Day Mode** or **Night Mode**.
2. Select the item, right-click, and then select **Remove Selected Items**.



WARNING

Responsibility for Regulatory Compliance.

It is the responsibility of the organization and person(s) performing the installation and maintenance of Mitel Advanced Communications Platforms to know and comply with all regulations required for ensuring Emergency Outgoing Access at the location of both the main system and any remote communication endpoints. Remote IP and SIP endpoints may require gateway access to nearby emergency responders.

Emergency Call phone numbers include:

- 911, the default for Mitel systems located in the U.S.
- 999, the default for Mitel systems located in the European market and used primarily in the United Kingdom U.K.
- If applicable, 112, an emergency number used widely in Europe outside of the U.K.
- Any emergency number, such as for a police or fire station, that is appropriate for the location of the main system and/or remote endpoints.

Day or Night Outgoing Access

There are separate lists for endpoints with outgoing access in day and night modes. By default, the automatic endpoint list (Auto: All Endpoints) is assigned to Day/Night Outgoing Access when a node trunk group is created.

To add endpoints that will have outgoing access for the node trunk group:

1. Select System – Devices and Feature Codes – **Node Trunk Groups**.
2. Select the trunk group number.
3. Select **Outgoing Access**.
4. Select either **Day Mode** or **Night Mode**.
5. Right-click anywhere in the right pane. An option box appears.
6. Select **Add To List**. A window appears prompting for the device type to include.
7. Select the device types (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
8. Select the appropriate items, then select **Add Items**. When you have added all the desired devices, click **Finish**. The selections appear in the list. To view programming options, double-click the device.

To delete destinations from the list:

1. Select System – Devices and Feature Codes – **Node Trunk Groups**.
2. Select the trunk group number.
3. Select **Outgoing Access**.
4. Select either **Day Mode** or **Night Mode**.
5. Select the destinations, right-click, and then select **Remove Selected Items**.

Search Algorithm

See “Search Algorithm” on [page 8-18](#) for a feature description.

To change the trunk group searching algorithm:

1. Select System – Devices and Feature Codes – **Node Trunk Groups**.
2. Select the trunk group number.
3. Select **Search Algorithm**.
4. In the **Value** column, select the setting.
5. Press **ENTER** or click outside the field to save the change.

Camp-Ons Allowed

The Camp On feature can be enabled or disabled for each node trunk group. If disabled, users placing outgoing calls will hear busy signals when all trunks in the group are in use or unavailable. If enabled, users will be able to camp on and wait for an available trunk.

To enable or disable the Camp On Allowed option:

1. Select System – Devices and Feature Codes – **Node Trunk Groups**.
2. Select the trunk group number.
3. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
4. Press **ENTER** or click out of the field to save the change.

ISDN Data Calls Allowed

This is a BRI-only trunk. When set to Yes, it allows you to add only B-channel trunks to the trunk group. With the flag set to No, you may add any types of trunk, except private networking B-channel trunks. Any non-B-channel trunks must be removed from the node trunk group before the flag can be set to Yes. If you move multiple trunks into a node trunk group that has this flag enabled, you will be warned that none of the trunks will be added to the group if any of the trunks to be added are non-B-channel trunks. By default, the flag is set to No.

To enable or disable the ISDN Data Calls Allowed option:

1. Select System – Devices and Feature Codes – **Node Trunk Groups**.
2. Select the trunk group number.
3. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
4. Press **ENTER** or click out of the field to save the change.

Hunt Groups

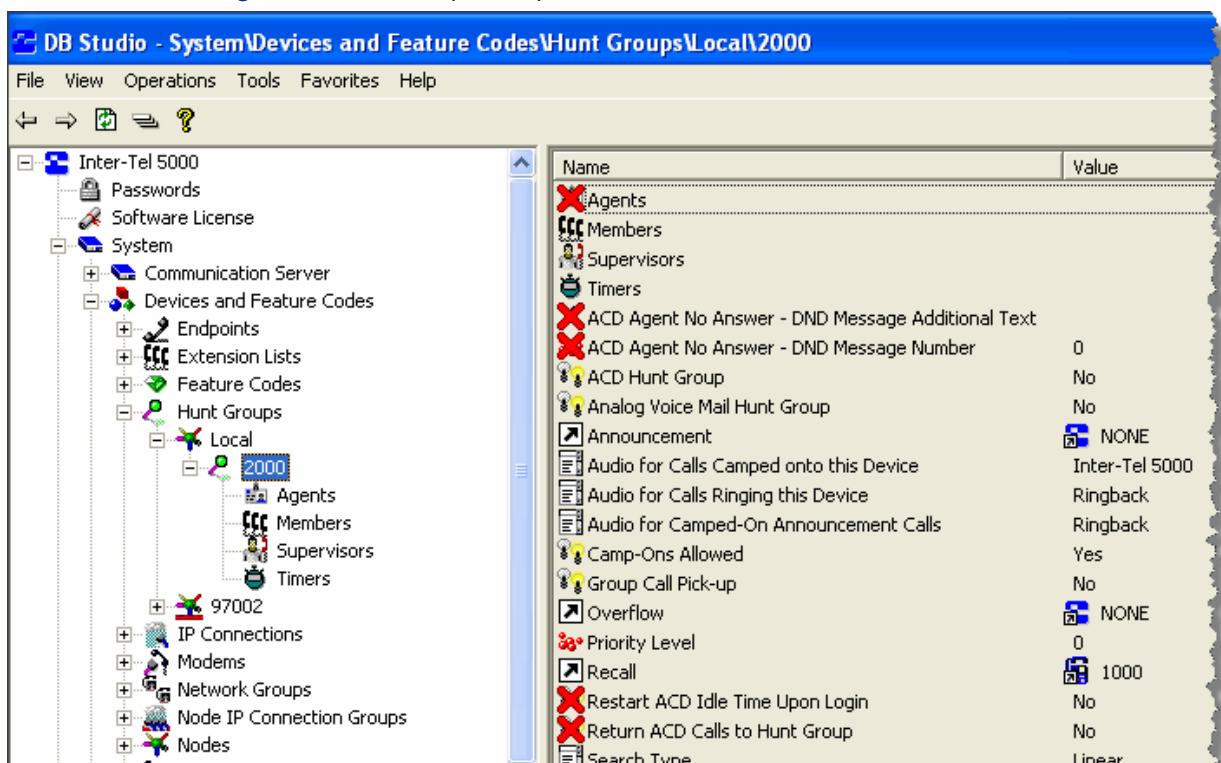
There are two types of hunt groups:

UCD Hunt Groups: Included with the system license. UCD hunt group members are automatically logged in to the hunt group. UCD hunt group members cannot log in or log out of hunt groups.

ACD Hunt Groups: Requires a software license. ACD hunt group members log in to the hunt group to receive calls. See “ACD Hunt Groups” on [page 8-33](#).

The hunt group location in DB Programming is shown in [Figure 8-4](#). For detailed information about system hunt groups, refer to the System Features chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

Figure 8-4. Hunt Group and Options



The Hunt Group feature permits calls to be placed to a group of endpoints and to be automatically transferred to an available endpoint in the group. You can program up to 75 hunt groups (300 on a Mitel CS-5600). Hunt group lists can contain individual endpoints or extension lists (see [page 8-4](#)). Non-ACD hunt group endpoints must reside on the same node; off-node devices must be ACD hunt group members.

The order in which hunt group endpoints receive incoming calls is determined by the search type selected (see [page 8-49](#)). An endpoint or extension list can appear in a single hunt group more than once, and it can appear in multiple hunt group lists, if desired.

Hunt groups have their own extension numbers (defaults to 2000–2074 or 2000–2299). Individual endpoints within the hunt group can be called using their assigned extension numbers.

ACD Hunt Groups

ACD hunt group members are referred to as “agents.” Agents log in to the ACD hunt group to receive calls and log out to halt ACD hunt group calls.

NOTE This feature requires an ACD Hunt Groups software license.

An ACD hunt group can be programmed to circulate calls to agents in the following two ways:

- **Agent IDs:** If the hunt group is programmed to use ACD Agent IDs, each agent is assigned an Agent ID number which the agent enters during the login procedure. The hunt group calls are routed to logged in agents, according to their Agent ID number instead of their endpoint extension. Because the Agent ID is not associated with any endpoint extension, the agent can use any endpoint in the system to log in and does not have to use the same endpoint every time.
- **Members:** If the hunt group *is not* programmed to use Agent IDs, it will have a list of endpoints and will send calls to the endpoints where agents are logged in.

When a call camps on to an ACD hunt group that uses Agent IDs, only the agents currently logged in to the hunt group will receive camp-on indications. ACD hunt group supervisors will receive visual camp-on displays if they are programmed as members of the hunt group and have the ACD Agent Logout feature turned on. ACD Agent IDs can be included in Extension Lists, which allow several ACD Agents to receive a call at once.

Viewing Agent ID Lists

To view an Agent ID list:

Select System – Hunt Group Related Information – **ACD Agent IDs**. ACD Agent IDs are shown in the right pane.

Creating ACD Agent IDs

NOTICE

For optimum system performance, no more than 1000 Agent IDs should exist in any one hunt group, and no more than 2000 Agent ID entries should exist in all hunt groups combined.

To create ACD Agent IDs:

1. Select System – Hunt Group Related Information – **ACD Agent IDs**.
2. Right-click anywhere in the right pane. An option dialog box appears.
3. Click **Create Agent ID**. The Create ACD Agent dialog box appears.
4. In the **Starting Extension** list, select the starting extension number (or lowest extension number, if creating multiple IDs).
5. In the Number of Extensions list, enter the number of IDs you want to create, and then click **OK** to continue. The new ACD Agent IDs appear in the list without a description or username.
6. Program the following options:
 - **Description:** The ACD Agent ID description can be up to 20 characters long. To program the description:
 - a.) Select the current description, then type the new entry in the text box.
 - b.) Press **ENTER** or click out of the field to save the change.
 - **Auto Connect:** When this flag is turned on, and headset mode is enabled, ACD hunt group calls automatically connect following a short ring burst. When the ACD agent logs in, however, the first call rings until the ACD agent answers it. For subsequent calls, the agent hears the ring burst in the headset, and the call is automatically connected. When the ACD agent removes the endpoint from DND, the call may or may not ring until the agent answers it. This is dependent on the **Allow Immediate ACD Auto Connect after DND** flag (under System\Flags). If this flag is turned on, the agent is automatically connected to all calls, including the first one received after exiting DND. If this flag is turned off, the first call rings until the agent answers it, but subsequent calls are automatically connected. The Auto Connect flag overrides the Transfer-To-Connect Allowed endpoint flag (see [page 7-22](#)) and is turned off by default.

To enable the flag:

 - a.) Select the current value, and then select the check box. The field changes to **Yes**. To disable the flag, clear the check box.
 - b.) Press **ENTER** or click out of the field to save your changes.

Deleting ACD Agent IDs

To delete ACD Agent IDs:

1. Select System – Hunt Group Related Information – **ACD Agent IDs**.
2. Select the agent IDs. You can use the SHIFT and CTRL keys to select more than one item.
3. Right-click, and then click **Delete**.

Local Hunt Groups

When you double-click the Local node, a list of the existing local hunt groups, if any, appears. You can create or delete hunt groups and/or enter descriptions and usernames. You can then program the hunt group, as described below.

Creating Hunt Groups

To create a hunt group:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Right-click anywhere in the right pane, and then select **Create Hunt Group**. The Create Hunt Group Extension dialog box appears.
3. In the **Extension** box, select or enter the hunt group extension number.
4. Click **OK** to continue. The new hunt group appears in the list without a description or username.
5. Select the **Description** field, and then type the new information in the text box. Descriptions can contain up to 20 characters and hunt group usernames can contain up to 10 characters. Do not use slash (/), backslash (\), vertical slash (|), or tilde (~) characters in usernames. Do not use Control characters in descriptions or usernames.
6. Press **ENTER** or click out of the field to save the change.

Deleting Hunt Groups

To delete a hunt group:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Right-click, and then click **Delete**. The hunt group is automatically removed from the list.

Changing Hunt Group Extensions Numbers

You can change hunt group extensions, descriptions, and user names.

To change the hunt group extension:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Enter the new number in the text box (or scroll to an available number).

To change several hunt group extension numbers at once:

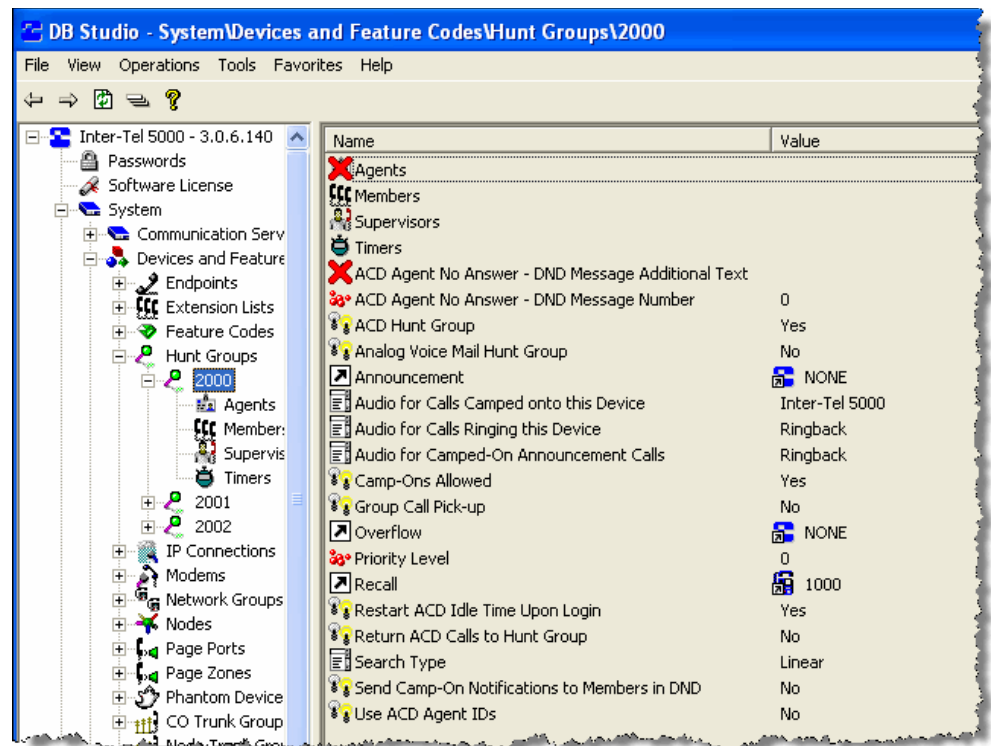
1. Select System Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt groups that you want to change.
3. Right-click, and then select **Batch Extension Change**. The Create Hunt Group Extension dialog box appears.
4. Select the number that you want to assign to the first selected hunt group (the other selected hunt groups will be numbered consecutively after this number).
5. Click **OK**. the hunt groups are automatically renumbered and re-sorted in the list.

Local Hunt Group Options

You can program the following local hunt group options, as shown in:

- “Agents” on [page 8-38](#)
- “Members” on [page 8-40](#)
- “Supervisors” on [page 8-41](#)
- “Timers” on [page 8-42](#)
- “ACD Agent No Answer – DND Message Additional Text” on [page 8-43](#)
- “ACD Agent No Answer – DND Message Number” on [page 8-43](#)
- “ACD Hunt Group” on [page 8-44](#)
- “Analog Voice Mail Hunt Group” on [page 8-44](#)
- “Announcement Endpoints” on [page 8-45](#)
- “Audio for Calls Camped onto this Device” on [page 8-45](#)
- “Audio for Calls Ringing this Device” on [page 8-46](#)
- “Audio for Camped-On Announcement Calls” on [page 8-46](#)
- “Camp-Ons Allowed” on [page 8-47](#)
- “Group Call Pick-Up” on [page 8-47](#)
- “Overflow Endpoints” on [page 8-45](#)
- “Priority Level” on [page 8-47](#)
- “Recall Destination Endpoint” on [page 8-48](#)
- “Restart ACD Idle Time Upon Login” on [page 8-48](#)
- “Return ACD Calls to Hunt Group” on [page 8-49](#)
- “Search Type” on [page 8-49](#)
- “Send Camp On Notifications to Members in DND” on [page 8-50](#)
- “Use ACD Agent IDs” on [page 8-51](#)

Figure 8-5. Local Hunt Group Options



Agents

If the hunt group is programmed to use ACD Agent IDs, each agent enters an assigned Agent ID number during the login procedure. The hunt group calls are routed to logged in agents according to their Agent ID number instead of their endpoint extension. Because the Agent ID is not associated with any endpoint extension, the agent can use any endpoint in the system to log in and does not have to use the same endpoint every time. ACD Agent IDs can be included in Extension Lists (see [page 8-4](#)), which allows several ACD Agents to receive a call at once.

To add Agent IDs to the hunt group:

NOTICE

For optimum system performance, no more than 1000 Agent IDs should exist in any one hunt group, and no more than 2000 Agent ID entries should exist in all hunt groups combined.

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Select **Agents**.
4. Select the extension number.
5. Double-click **Agent IDs** to see the current list of IDs, if any.

NOTE

The Agents List is an ordered list, so you must place the agents in the list in the order you want them to be accessed when the hunt group receives a call.

6. Do one of the following:
 - *To add to the bottom of the list:* Do not select any existing agents, right-click anywhere in the right side of the window, and then select **Add To Agents List**.
 - *To add to the list above an existing agent:* Select the agent, right-click the selected agent, and then select **Add To Agents List**.

A window appears prompting for the device type to include.

7. Select **ACD Agent ID** and/or **ACD Agent ID Extension List** (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
8. Select the appropriate items, then select **Add Items**. When you have added all the Agent IDs, click **Finish**. The selections appear in the list. ACD Agent IDs are programmed in Hunt Group-Related Information. To view programming options, double-click the Agent ID number.

To move an agent to another location in the list:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Select **Agents**.
4. Double-click **Agent IDs** to see the current list of IDs, if any.
5. Drag and drop the agent to the new position. Or, select the agent to move and press **CTRL** + the up/down arrow to move the agent up or down in the list.

To delete Agent IDs:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Select **Agents**.
4. Double-click **Agent IDs** to see the current list of IDs, if any.
5. Select the agent ID(s), and then press **DELETE** on the keyboard, or right-click and select **Remove Selected Items**.

Members

Prepare a list of the endpoints and extension lists to be included in each of the hunt groups. If desired, an endpoint or extension list can appear more than once in a hunt group list or can be in more than one hunt group. If an extension list is included in an ACD hunt group set for Longest Idle or Balanced Call Count distribution, it will treat each endpoint in the extension list as a separate agent; it will not ring all of the endpoints on the list at once. If the hunt group is set for linear or distributed order, a call will ring at all endpoints on an extension list at once when the call reaches that point in the hunt group list. Therefore, to create an “all ring” type of hunt group, you can program the hunt group as either linear or distributed and then assign an extension list as the only hunt group member.

To add hunt group members:

1. Select System Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Double-click **Members** to see the current list.

NOTE

The Agents List is ordered, so you must place the devices in the list in the order you want them to be accessed when the hunt group receives a call.

4. *To add to the bottom of the list:* Do not select any existing members. Right-click anywhere in the right side of the window, and then select **Add To Members List**.

To add to the list above an existing member: Select the member, right-click the selected member, and then select **Add To Members List**.

A window appears prompting for the device type to include.

NOTE

Adding a large extension list can result in slowing down system performance. Adding an Extension List that contains more than 30 members (CS-5200) or 60 members (CS-5400 and CS-5600) may cause a system slowdown because when the list is called, ALL members of the list are called at the same time.

5. Select the device types (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
6. Select the items, and then select **Add Items**. When you have added all the members, click **Finish**. The selections appear in the list. To view programming options, double-click the extension number.

To move a member to another location in the list:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Double-click **Members** to see the current list.
4. Drag and drop the member to the new position. Or, select the member to move and press **CTRL** + the up/down arrow to move the member up or down in the list.

To delete members:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Double-click **Members** to see the current list.
4. Select the members that you want to remove, and then press **DELETE**, or right-click and select **Remove Selected Items**.

Supervisors

(Hunt group supervisors can be off-node devices.) Hunt groups can have one or more endpoints assigned as a hunt group supervisor. An extension list can be included in the list of supervisors. If desired, an endpoint can be assigned as the supervisor for more than one hunt group. If not using Agent IDs, ACD hunt group supervisors with display endpoints receive visual camp-on displays if they are programmed as members of the hunt group and they have the ACD Agent Logout feature enabled. If a Hunt Group is using ACD Agent IDs, the supervisor must be logged on to the group to receive camp-on indications. If not using ACD Agent IDs, you can add the supervisor as a hunt group member, set the Hunt Group flag for the supervisor's station to "Remove," and the supervisor will still receive hunt group camp-on indications.

To add supervisors to the hunt group:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Double-click **Supervisors** to see the current list of supervisors, if any.
4. Right-click anywhere in the right side of the window. An option box appears.
5. Select **Add To Supervisors List**. A window appears prompting for the device type to include.
6. Select the endpoint or extension types (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
7. Select the appropriate items, then select **Add Items**. When you have added all the supervisors, click **Finish**. The selections appear in the list. To view programming options, double-click the extension number.

To delete supervisors:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Double-click **Supervisors** to see the current list of supervisors.
4. Select the supervisor(s) you want to remove and then press **DELETE** on the keyboard, or right-click and select **Remove Selected Items**.

Timers

You can program the following hunt group timers:

- **No Answer Advance:** The amount of time a call will ring at a hunt group endpoint (unanswered) before advancing to the next endpoint on the list. It is started when the call is received at the hunt group. The range is 1–255 seconds; the default value is 18 seconds.
- **Announcement:** *(UCD Hunt Groups Only)* The amount of time a call will remain unanswered before it is picked up by the hunt group announcement endpoint. It is started when the call is received at the hunt group. The range is 1–255 seconds; the default value is 18 seconds.
- **Overflow:** *(UCD Hunt Groups Only)* The amount of time a call will circulate through the hunt group (unanswered) before being picked up by the hunt group overflow endpoint. This timer is started when the Announcement timer expires (or, if there is no announcement endpoint, when the call is received by the hunt group) and it is restarted each time the call leaves the overflow endpoint. The range is 1–255 seconds; the default value is 72 seconds.
- **Recall:** The amount of time a call will circulate through the hunt group (unanswered) before being sent to the hunt group recall destination endpoint. The timer is started when the call is received by the hunt group. The range is 1–65,535 seconds; the default value is 180 seconds (3 minutes).
- **Wrap-Up:** *(ACD Hunt Groups Only)* Each time an agent ends an ACD hunt group call, the ACD Wrap-Up Duration timer starts. Until the timer expires, the agent will not receive another call through any ACD hunt group. However, the agent can receive other non-ACD hunt group calls, direct ring-in calls, and transfers. The range is 1– 65,535 seconds; the default value is 15 seconds.
- **Average Connect Time Per Call:** *(UCD Hunt Groups Only)* An application announcement or overflow endpoint message can be programmed to include the caller's queue position and/or estimated wait time. The estimated wait time is based on the Average Connect Time Per Call multiplied by the number of calls ahead of the caller in the queue, divided by the number of available hunt group members (*average connect time per call x number of waiting calls ÷ available members*). The range is 1–10,000 seconds; the default value is 60 seconds.

To program a hunt group timer:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Double-click **Timers**.
4. Select the timer, and then type the new value in the **Value** column.
5. Press **ENTER** or select another field to save the change.

ACD Agent No Answer – DND Message Additional Text

This option is disabled and displays a red “X” if the ACD Hunt Group option is set to No, or if the ACD Agent No Answer – DND Message Number option is set at 0.

This option enables endpoint users to enter additional DND text when using the DND message chosen for the “DND Message Number” flag (see the following section).

NOTE

To determine if trunk calls will be allowed to go to DND for the selected hunt group, program the “Return ACD Calls to Hunt Group” option (see [page 8-49](#)).

To change the ACD Agent No Answer – DND Additional Text option:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Make sure the **ACD Hunt Group** option is set to **Yes** and that the **ACD Agent No Answer – DND Message Number** has a value other than 0.
4. Enter the text, up to 16 characters, that displays when endpoint users select the ACD Agent No Answer – DND Message Number, or leave the field blank to allow users to enter their own text.
5. Press **Enter** or click outside of the field to save your changes.

ACD Agent No Answer – DND Message Number

This option is disabled and display a red “X” if the “ACD Hunt Group” option is set to No.

if the last agent in a Hunt Group does not answer an incoming call, the agent is automatically placed in DND, and the call returns to the Hunt Group where it is answered or camped on. This flag and the “ACD Agent No Answer - DND Additional Text” flag (see the previous section) allow you to determine which DND message is used (selected by number) and the bottom line of the DND message text. This flag allows OAI applications to function better with the Hunt Groups.

The DND Message Number flag is a link to Endpoint-Related Information\Messages (see [page 7-72](#)) where you can select the language that you want to use and see which DND message you want to use. Endpoint users can select 0 – 20, which corresponds with the DND messages. A value of zero does not allow an agent to go into DND. It is set to zero by default.

NOTE

To determine if trunk calls will be allowed to go to DND for the selected hunt group, program the “Return ACD Calls to Hunt Group” option (see [page 8-49](#)).

To select the ACD Agent No Answer – DND Message Number:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. In the Value column, select the number to be used for the **ACD Agent No Answer – DND Message Number**. You are prompted to view the Messages folder.
4. Do one of the following:
 - Click **Yes** to see the Messages folder and select the appropriate language. Click **DND** to see a list of DND messages from which you can determine the number to select. Then click the **Back** button on the toolbar several times to return to the Hunt Group folder to enter the value.
 - Click **No** to ignore the prompt and use the value you selected.
5. Click the **Value** column for **ACD Agent No Answer - DND Additional Text** to enter any additional text you want to accompany the DND message you chose in step 2.
6. Press **Enter** or click outside of the field to save your changes.

ACD Hunt Group

(This option is not recommended for Analog Voice Mail hunt groups.) This option allows the hunt group to use the ACD features. The ACD Hunt Groups software license, part no. 840.0230, is required to enable this option.

Automatic Call Distribution (ACD) hunt groups can use all of the standard and UCD hunt group features, if enabled, in addition to the following features:

- ACD hunt groups can be programmed to distribute calls to equalize call time or call count among the available members.
- ACD can provide call information records that can be processed by an external device connected to a system serial port.
- ACD hunt groups can use of Agent ID numbers in place of endpoint extensions in the hunt group list. See the Agent ID information on [“ACD Hunt Groups” on page 8-33](#).

To enable ACD hunt group features:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Select **ACD Hunt Group**.
4. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
5. Press **ENTER** or select another field to save the change.

Analog Voice Mail Hunt Group

If the Analog Voice Mail Hunt Groups software license, part no. 840.0229, is installed, the hunt group can be composed of endpoint ports which are connected to an analog voice mail device. Enabling this option has the effect of passing along endpoint identification when a call reaches the hunt group as a result of forwards and transfers. The purpose of this flag is to provide compatibility between the system and analog voice mail units. The optional external voice processing system is a digital system and does not require this flag.

NOTE

When an analog voice mail unit is connected to the system, the voice mail unit should use the Silent Message feature code (367) instead of the Message feature code (365). Mitel recommends *not* using this option with ACD hunt groups

To enable the Analog Voice Mail Hunt Group option:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Select **Analog Voice Mail Hunt Group**.
4. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
5. Press **ENTER** or select another field to save the change.

Announcement and Overflow Endpoints

(Announcement and overflow endpoints can be assigned to off-node endpoints or Voice Processor applications, if they are programmed as off-node devices. See [“Creating Off-Node Devices”](#) on page 7-13.

Hunt groups can have an announcement endpoint and/or an overflow endpoint. If a call to the hunt group is not answered before the Announcement timer expires, the call is picked up by the announcement endpoint. If the call remains unanswered when the hunt group Overflow timer expires, the call is picked up by the overflow endpoint. Announcement and overflow endpoints should be playback device endpoints (these can be Auto Attendant, Voice Mail, or Call Routing Announcement applications). Do not include these endpoints in the hunt group distribution list.

To program an Announcement or Overflow endpoint:

Do one of the following:

Method A

- a. Select System – Devices and Feature Codes – **Hunt Groups**.
- b. Select the hunt group extension number.
- c. Select **Announcement**.
- d. Select the current value, and then enter the new value in the text box.
- e. Press **ENTER**. A screen appears displaying what is associated with the number entered.
- f. Click **OK**. The new number appears in the field.

Method B

- a. Select System Devices and Feature Codes – **Hunt Groups**.
- b. Select the hunt group extension number.
- a. Right-click the existing value for the Announcement or Overflow endpoint, and then click **Change Announcement**. The Change Announcement dialog box appears.
- b. Select the device types (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
- c. Select the device you want as the Announcement or Overflow endpoint, and then click **Finish**. The selection appears in the applicable field.

Audio for Calls Camped onto this Device

The Audio for Calls Camped onto this Device field defines the audio that a caller hears when camped-on to this hunt group.

To program Audio for Calls Camped onto this Device:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Select **Audio for Calls Camped onto this Device**.
4. In the **Value** column, select one of the following options from the list:
 - **Silence**: Callers hear no Music-On-Hold.
 - **Tick Tone**: Callers hear tick tone.
 - **Ringback**: Callers hear ringback.
 - **Inter-Tel 5000**: Callers hear an external music source. This is the default value.
 - **File-Based MOH**: Callers hear the MOH file selected in DB Programming. For more information, see “File-Based Music-On-Hold (MOH)” on [page 10-9](#).
5. Press **ENTER** or click outside the field to save the change.

Audio for Calls Ringing this Device

The Audio for Calls Ringing this Device field defines the audio that a caller hears when ringing this hunt group. By default, the system determines the music source based on the trunk group in which the call resides. However, endpoints (as well as Hunt Groups and Voice Processor Applications) can be programmed to determine the music source a caller hears based on the device for which the caller is ringing.

NOTE

The Audio for Calls Ringing this Device option only works when the call goes through a trunk group and also when used in conjunction with the Use Next Device's Audio Source field. IC calls do not apply to the use of this field when this field is set to a music source. For a hunt group in which the primary purpose is to support IC callers (for example, an internal help desk), you should set all of the "Audio for Calls..." fields to something other than a music source, such as Ringback.

To program Audio for Calls Ringing this Device:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Select **Audio for Calls Camped onto this Device**.
4. In the **Value** column, select one of the following options from the list:
 - **Silence**: Callers hear no Music-On-Hold.
 - **Tick Tone**: Callers hear tick tone.
 - **Ringback**: Callers hear ringback. This is the default value.
 - **Inter-Tel 5000**: Callers hear an external music source.
 - **File-Based MOH**: Callers hear the MOH file selected in DB Programming. For more information, see "File-Based Music-On-Hold (MOH)" on [page 10-9](#)
5. Press **ENTER** or click outside the field to save the change.

Audio for Camped-On Announcement Calls

This flag determines the functionality for camped-on hunt group calls that are listening to an Announcement Endpoint message when they transition from camped-on to ringing. If this flag is set for ringback, the user switches from hearing the Announcement Endpoint to hearing ringback when the call moves from camped-on to ringing. This is the default functionality.

If this flag is set for Announcement Endpoint, the user continues to hear the Announcement Endpoint when the call moves from camped-on to ringing. When the Announcement Endpoint hangs up (for example, the entire message is played), the user starts to hear ringback. If, however, an agent answers the call before the Announcement Endpoint hangs up, the call is connected, and the rest of the message is not played. The user may hear Music-On-Hold instead of ringback depending on how the system is programmed.

To program Audio for Camped-On Announcement Calls:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Select **Audio for Camped-On Announcement Calls**.
4. In the **Value** column, select one of the following options from the list:
 - **Ringback**: Callers hear ringback. This is the default value.
 - **Announcement Station**: Callers continue to hear the Announcement station (endpoint) when the call moves from camped-on to ringing.
5. Press **ENTER** or click outside the field to save the change.

Camp-Ons Allowed

If this flag is enabled, callers are allowed to camp on to the hunt group when all members are busy. If the flag is disabled, the callers hear busy tones when no members are available. In the default state, camp-ons are enabled.

To prevent callers from camping on to the hunt group:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Select **Camp-Ons Allowed**.
4. In the **Value** column, clear the check box. The field changes to **No**. To enable the option, select the check box.
5. Press **ENTER** or select another field to save the change.

Group Call Pick-Up

The Group Call Pick-up feature allows users to reverse transfer a call that is ringing in to a hunt group or one of its endpoints using the hunt group extension number.

- *If enabled*, users can enter the Reverse Transfer feature code (4), and then dial the hunt group extension number to pick up a call that is ringing in to any endpoint extension within that hunt group or to the hunt group extension number.
- If *disabled*, reverse transfers using the hunt group extension number will reverse transfer only calls ringing to the hunt group extension number, not calls ringing at the individual endpoints within the hunt group.

To enable Group Call Pick-Up:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Select **Group Call Pick-Up**.
4. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
5. Press **ENTER** or click out of the field to save the change.

Priority Level

Some endpoints may be members of more than one ACD or UCD hunt group. For this reason, hunt groups are assigned a “priority level.” The priority level determines which hunt group calls should be received first when calls ring in and/or camp on to several hunt groups at once. If an endpoint is a member of multiple hunt groups that have the same priority level, calls received by those hunt groups will be queued in the order they were received by the system.

To set the hunt group priority level:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Select **Priority Level**.
4. In the **Value** column, select or type the priority level for this hunt group. Higher numbers have higher priority. The range is 0–75; the default is 0.
5. Press **ENTER** or click out of the field to save the change.

Recall Destination Endpoint

The recall destination can be assigned to an off-node endpoint or application, if it is programmed as an off-node device. See “Creating Off-Node Devices” on [page 7-13](#). Any hunt group can have a recall destination endpoint, regardless of whether UCD is enabled. If a call remains unanswered when the Recall timer expires, it will be sent to the recall destination endpoint. The recall destination endpoint should be an endpoint or single-line endpoint. Do not include this endpoint in the hunt group distribution list.

To program the Recall Destination Endpoint:

Use one of the following methods:

Method A

- a. Select System – Devices and Feature Codes – **Hunt Groups**.
- b. Select the hunt group extension number.
- c. Select **Recall**.
- d. In the **Value** column, type the new destination endpoint extension number.
- e. Press **ENTER** or click out of the field to save the change. A screen appears showing what is associated with the number entered.
- f. Click **OK**. The new number appears in the field.

Method B

- a. Select System – Devices and Feature Codes – **Hunt Groups**.
- b. Select the hunt group extension number.
- c. Select **Recall**.
- a. Right-click the existing value for the Recall endpoint, and then click **Change Recall**. The Change Recall dialog box appears.
- b. Select the device types (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
- c. Select the device you want as the Recall endpoint, and then click **Finish**. The selection appears in the Recall field.

Restart ACD Idle Time Upon Login

This option determines where an agent is placed in a longest idle queue when the agent logs back in to a hunt group.

- When *enabled*, the agent's idle time is reset to zero whenever the agent logs in (for example, that agent will be least likely to receive the next distributed call).
- When *disabled*, the agent's idle time includes the time the agent was logged out of the hunt group (for example, that agent will be most likely to receive the next distributed call). By default, this flag is *disabled*.

To enable the Restart ACD Idle Time Upon Login option:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Select **Restart ACD Idle Time Upon Login**.
4. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
5. Press **ENTER** or click out of the field to save the change.

Return ACD Calls to Hunt Group

When enabled, this option re-queues a call to the front of the Camp On queue for the hunt group from which the call came. It allows a calling party to immediately return to the front of the hunt group queue, if the assigned agent station is in Do-Not-Disturb (DND) mode. If the option is not enabled, the calling party will continue to ring until the No Answer Advance timer expires or the agent removes DND from the endpoint and answers the call.

To enable the Return ACD Calls to Hunt Group option:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Select **Return ACD Calls to Hunt Group**.
4. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
5. Press **ENTER** or click out of the field to save the change.

Search Type

Available Search Types depend on the type of hunt group being programmed:

- **For Standard and UCD Hunt Groups:** Determine whether the calls are sent to the endpoints in linear or distributed order. Linear order means that the call is sent to the first endpoint or extension list on the list and moves down the list until it reaches an available endpoint. With distributed order, the call is sent to the endpoint that appears on the list after the last endpoint or extension list to receive a call (even if the call was not answered).
- **For ACD Hunt Groups:** ACD Hunt Group calls can circulate in linear or distributed order (as described above) or using one of the ACD distribution methods: Longest Idle or Balance Call Count order. Longest idle means that an incoming call is sent to the endpoint that has not been involved in a call to this hunt group for the longest period of time. Balance Call Count means that, to balance the call load, each incoming call is sent to the endpoint that has received the fewest calls through this hunt group. (It does not count calls that were received through other hunt groups, direct ring-in, or transfer.)

To set the search type:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Select **Search Type**.
4. In the **Value** column, select the search type from the list.
5. Press **ENTER** or click out of the field to save the change.

Send Camp On Notifications to Members in DND

This option indicates whether or not camp-on burst tones are sent to hunt group members that are in DND or that are logged out. When sent to display endpoints, the display shows *N CALLS WAITING FOR <HUNT GROUP>*, where *N* is the number of calls that are currently camped-on to the hunt group. This allows hunt group members to see the hunt group queue in real-time.

When this flag is enabled:

- If the hunt group is a UCD hunt group, members receive one of the following notifications:
 - Logged into hunt group and in DND: Tone -YES
 - Logged into hunt group and not in DND: Tone - YES
 - Logged out of hunt group and in DND: Tone - YES
 - Logged out of hunt group and not in DND: Tone - YES
- If the hunt group in an ACD hunt group but does *not* use Agent IDs, members receive one of the following notifications:
 - Logged into hunt group and in DND: Tone -YES
 - Logged into hunt group and not in DND: Tone - YES
 - Logged out of hunt group and in DND: Tone - YES
 - Logged out of hunt group and not in DND: Tone - YES
- If the hunt group is an ACD hunt group and uses ACD Agent IDs:
 - The user receives Camp On notifications if the Agent ID is **logged in** to the Hunt Group *and* in DND.
 - The user does **not** receive Camp On notifications if the Agent ID is **logged out** of the hunt group.

When this flag is disabled:

- If the hunt group is a UCD hunt group, members receive one of the following notifications:
 - Logged out of hunt group and not in DND: Tone - YES
 - Logged out of hunt group and in DND: Tone - NO
 - Logged into hunt group and not in DND: Tone - YES
 - Logged into hunt group and in DND: Tone - NO
- If the hunt group in an ACD hunt group but does *not* use Agent IDs, members receive one of the following notifications:
 - Logged out of hunt group and not in DND: Tone - YES
 - Logged out of hunt group and in DND: Tone - NO
 - Logged into hunt group and not in DND: Tone - YES
 - Logged into hunt group and in DND: Tone - NO
- If the hunt group is an ACD hunt group and uses ACD Agent IDs:
 - The user does **not** receive Camp On notifications if the Agent ID is **logged in** to the Hunt Group *and* in DND.
 - The user does **not** receive Camp On notifications if the Agent ID is **logged out** of the hunt group.

To enable the Send Camp On Notifications to Members in DND option:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Select **Send Camp On Notifications to Members in DND**.
4. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
5. Press **ENTER** or click out of the field to save the change.

Use ACD Agent IDs

If the ACD Hunt Group Option is enabled, you can choose to route calls according to ACD Agent ID numbers instead of endpoint extensions.

To enable the Use ACD Agent IDs option:

1. Select System – Devices and Feature Codes – **Hunt Groups**.
2. Select the hunt group extension number.
3. Select **Use ACD Agent IDs**.
4. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
5. Press **ENTER** or click out of the field to save the change.

Node-Spanning Hunt Groups

There is a software license called Remote Automatic Call Distribution Hunt Groups. It allows ACD hunt groups to span nodes. Node-spanning ACD hunt groups can have either members or ACD Agent IDs. Agent IDs are considered global throughout all nodes in which the Agent exists. This means that if you create Agent ID 100 on one node, you must also create Agent ID 100 on all other nodes that have an endpoint that may want to login to the hunt group using that ID.

Remote (Off-Node) Hunt Groups

When you double-click a remote node, a list of the existing off-node hunt groups for that node, if any, appears. You can create or delete off-node hunt groups or enter descriptions and user names.

To create an off-node hunt group:

1. Right-click anywhere in the right pane, and then select **Create Off-Node Hunt Group**. The Create Hunt Group dialog box appears.
2. Enter the extension number in the box or scroll to the desired number.
3. Click **OK** to continue. The new hunt group appears in the list without a description or username.
4. Program the **Description** and **Username fields**. All trunk groups should have a description and a username. The description appears in all trunk group lists in the database and can be up to 20 characters long. The username appears on endpoint displays and can have up to 10 characters.

To program the Description and Username fields:

- a. Select the box.
- b. Type the entry.
- c. Press **ENTER** or click out of the field to save your changes.

Network Groups

Network Groups define the IP devices that can communicate through Peer-to-Peer (P2P) audio. When you assign an IP device (including SIP endpoints and MGCP gateways and endpoints) to a circuit, the device is automatically added to the default Network Group (PP029). This Network Group is not programmed for P2P audio and it cannot be configured. To use P2P audio, you must assign the IP devices to a Network Group that is programmed to support the feature. Before you assign IP devices to a Network Group, however, you must make sure the hardware is properly upgraded. You cannot delete the default Network Group. For more information about Network Groups, refer to the System Features chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

Hardware Upgrades

To have IP endpoints use P2P to communicate through SIP/MGCP gateways, place the IP endpoints and SIP/MGCP trunks (gateway and endpoints) in the same Network Group. The P2P option must be set on that Network Group. P2P audio requires upgrading IP endpoints and IP SLAs to the latest firmware version.

NOTICE

Run the Network Qualifier (for at least 24 hours) to determine if the network meets the minimum requirements identified for P2P audio. These requirements are the same as those identified for IP networking and IP private networking. For more information about the Network Qualifier, refer to the *Network Qualifier Reference Manual*, part number 835.2427.

To upgrade the hardware:

Use the Upload Utility or TFTP to upload the latest firmware to all IP devices that use P2P audio. For details about using the Upload Utility to upgrade IP devices, see “Upload Utility” on [page 14-21](#). For information on using TFTP to upgrade IP devices, refer to the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

Network Group Assignments

When you double-click Network Groups, the default Network Group (PP029) and any other programmed groups are displayed.

NOTE

IP softphones that are used as mobile devices cannot be part of a Network Group configured for P2P Audio. If you attempt to add an IP softphone to the Network Group list or change the Use Peer-To-Peer Audio setting of a Network Group to Yes, a warning message appears.

To create a Network Group:

1. Select System – Devices and Feature Codes – Network Groups.
2. Right-click, and then select **Create Network Group**.
3. Select a P7XXX extension and the number of groups to create.
4. Click **OK**. Each Network Group on a node must have a unique extension.
5. Program the description and user name. The description that appears can be up to 20 characters long. The username, that will appear on display endpoints, can have up to eight characters. Do not use slash (/), backslash (\), vertical slash (|), or tilde (~) characters in usernames. Do not use Control characters in descriptions or usernames.
6. In the **Use Peer-To-Peer Audio** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box. If this option is disabled, the devices in the group use the system vocoders for all calls.

Creating Network Group Endpoints and Trunks

After you have created the Network Group, you must assign endpoints and trunks to the group. The endpoints and/or trunks in this group will then use P2P audio or the TDM highway based on the **Use Peer-To-Peer Audio** option (see step 6 on [page 8-52](#)).

Network Group IP Endpoints

IP endpoints include IP endpoints (except the IP SoftPhone), IP SLAs, and multi-protocol (SIP or IP) endpoints. To view a list of IP endpoints that are currently assigned to the Network Group, double-click **Endpoints**.

NOTICE

Model 8602 softphones are not supported for P2P audio and network groups. Model 8602 IP softphone applications may be used as mobile devices, allowing them to move between the LAN containing a Mitel 5000 platform and public network/Internet. However, any Model 8602 used for this purpose must **not** be included in a Network Group using P2P Audio.

To add endpoints to the list:

1. Right-click and select **Move To Endpoints List**.
2. Select IP Endpoint or IP Single-Line Adapter, and then click **Next**.
3. Select the devices to add to the list, then click **Move To List**.
4. Click **Finish** when all devices have been moved.

Network Group Trunks

IP trunks include SIP/MGCP gateways and endpoints. To view a list of IP trunks that are currently assigned to the Network Group, double-click **Trunks**.

To add trunks to the list:

1. Right-click and select **Move To Trunks List**.
2. Select **MGCP Endpoint** or **MGCP Gateway and Endpoint** or **SIP Trunk**, and then click **Next**.
3. Select the devices to add to the list, and then click **Move To List**.
4. Click **Finish** when all devices have been moved.

You can also program Network Groups for P2P audio across nodes, as described below.

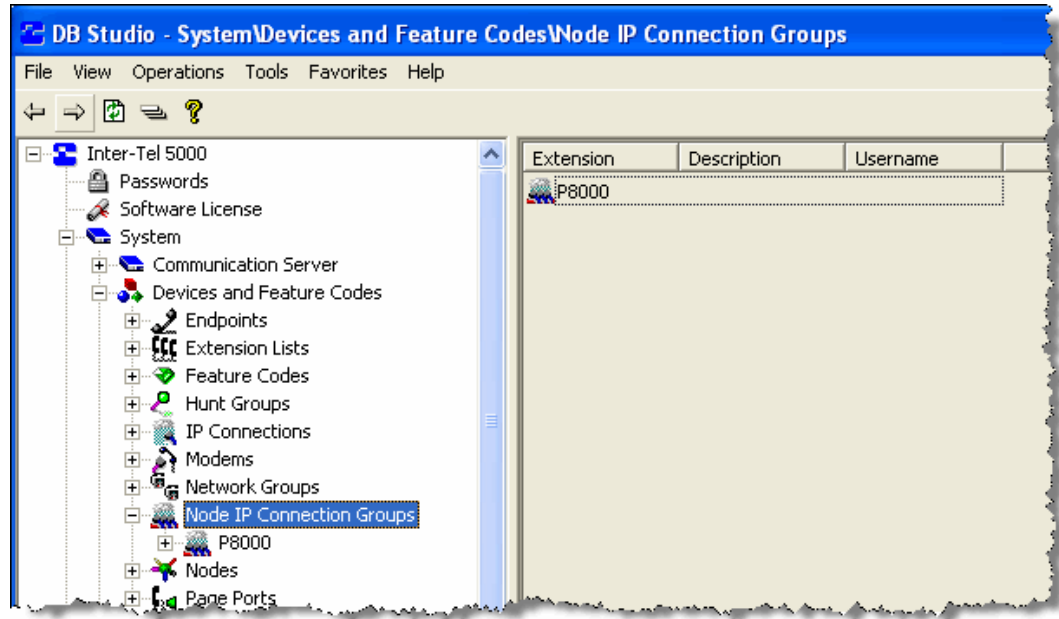
To program Network Groups for P2P audio across nodes:

1. Create a Network Group on each node and assign each group the same extension number. For example, if the devices that will use P2P audio reside on nodes 2 and 3, program a Network Group with the same extension number (for example, P7000) on both nodes.
2. Assign the appropriate endpoints and trunks to the Network Group on each node. For example, to use P2P audio between device 2000 on node 2 and device 3000 on node 3, Network Group P7000 on node 2 must contain device 2000, and Network Group P7000 on node 3 must contain device 3000.
3. Enable the **Use Peer-To-Peer Audio** flag for the Network Group on each node.

Node IP Connection Groups for Remote Nodes

The system automatically creates a node IP connection group for each remote node added, as shown in [Figure 8-6](#).

Figure 8-6. *Node IP Connection Groups*



The node IP connection group, which corresponds to an IP network connection between the remote node and the local node, can then be programmed for each off-node IP connection. Like other devices, DB Programming displays off-node IP connections within a folder corresponding to the node on which the off-node IP connection resides. When you access the IP Connections folder, the right side of the screen displays the extension, description, and username of the IP connection group.

All IP connection groups should have a description and a username. The description that appears in all IP connection group lists in the database can be up to 20 characters long. The username, that will appear on display endpoints, can have up to 10 characters. To program the names, select the desired text box and type the entry. Do not use slash (/), backslash (\), vertical slash (|), or tilde (~) characters in usernames. Do not use Control characters in descriptions or usernames.

You can program the following IP Call Configuration options:

- "Node IP Connection Group IP Call Configurations" on [page 8-55](#)
- "Remote Node IP Connections" on [page 9-21](#)
- "Day/Night Emergency Outgoing Access" on [page 8-56](#)
- "Day or Night Outgoing Access" on [page 8-15](#)
- "Remote Node" on [page 8-57](#)
- "Camp-Ons Allowed" on [page 8-57](#)

Node IP Connection Group IP Call Configurations

Changes to IP Call Configuration settings do not take effect until the next call is placed or received. Changes do not affect existing calls. For descriptions about IP Call configuration options, see “Programming Call Configuration Options” on [page 9-27](#).

To program a Node IP Connection Group IP Call Configuration:

1. Select System – Devices and Feature Codes – Node IP Connection Groups – **<Node Connection Group number>**.
2. Double-click **IP Call Configuration**. IP Call Configuration options are shown in the right pane.

Local Music Source

Available only when you set the Music-On-Hold vocoder to Local Music Source. When set to Local Music Source, the system does not transmit and receive Music-On-Hold between the local node and the remote node. Rather, the local music source field defines the music source the caller on the local node hears when he would otherwise be listening to Music-On-Hold.

To program the Local Music Source:

1. Select System – Devices and Feature Codes – Node IP Connection Groups – **<Node Connection Group number>**.
2. Select the call configuration.
3. Select **Local Music Source**.
4. In the **Value** column, select one of the following options from the list:
 - **Silence**: Callers hear no Music-On-Hold.
 - **Tick Tone**: Callers hear tick tone.
 - **Ringback**: Callers hear ringback.
 - **Inter-Tel 5000**: Callers hear an external music source (this is the default value).
 - **File-Based MOH**: Callers hear the MOH file selected in DB Programming. For more information, see “File-Based Music-On-Hold (MOH)” on [page 10-9](#).
5. Press **ENTER** or click outside the field to save the change.

Music-On-Hold Encoding Setting

Determines whether Music-On-Hold is transmitted across a network connection. You can program this field to either *Use Speech Encoding Setting* or *Use Local Music Source*. If set to *Use Speech Encoding Setting*, the system uses the vocoder specified by the speech encoding setting when transmitting Music-On-Hold across the network connection. If set to *Use Local Music Source*, the system connects the caller to the music source given by the local music field rather than transmitting Music-On-Hold across the network.

To select the Music-On-Hold Encoding Setting:

1. Select System – Devices and Feature Codes – Node IP Connection Groups – **<Node Connection Group number>**.
2. Select the call configuration.
3. Select **Music-On-Hold Encoding Setting**.
4. In the **Value** column, select the option from the list. The default is *Use Local Music Source*.
5. Press **ENTER** or click out of the field to save the change.

Day/Night Emergency Outgoing Access

There are separate lists for endpoints with emergency outgoing access in day and night modes. By default, the automatic endpoint list (*Auto: All Endpoints*) is assigned to Day/Night Emergency Outgoing Access.

To add endpoints having emergency outgoing access for a node trunk group:

1. Select **System – Devices and Feature Codes – Node IP Connection Groups – <Node Connection Group number>**.
2. Select **Emergency Outgoing Access**. The choices are Day Mode or Night Mode.
3. Right-click anywhere in the right side of the window. An option box appears.
4. Select **Add To List**. A window appears prompting for the device type to include.
5. Select the device types (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
6. Select the appropriate items, and then select **Add Items**.
7. When you have added all the desired devices, click **Finish**. The selections appear in the list. To view programming options, double-click the extension number.

Day/Night Outgoing Access

There are separate lists for endpoints with outgoing access in day and night modes. By default, the automatic endpoint list (*Auto: All Endpoints*) is assigned to Day/Night Outgoing Access.

To add endpoints have outgoing access for a node trunk group:

1. Select **System – Devices and Feature Codes – Node IP Connection Groups – <Node Connection Group number>**.
2. Select **Outgoing Access**, and then double-click **Day Mode** or **Night Mode**.
3. Right-click anywhere in the right pane, and then click **Add to Day** (or **Night**) **List**.
4. Select **Add To List**. The Add to Day (or Night) dialog box appears.
5. Select the device types (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
6. Select the appropriate items, and then select **Add Items**.
7. When you have added all the desired devices, click **Finish**. The selections appear in the list. To view programming options, double-click the device.

To remove endpoints that have outgoing access for the node trunk group:

1. Select **System – Devices and Feature Codes – Node IP Connection Groups – <Node Connection Group number>**.
2. Select **Outgoing Access**, and then select **Day Mode** or **Night Mode**.
3. Select the item, right-click, and then select **Remove Selected Items**.

To delete endpoint(s) having emergency outgoing access for a Node IP Connection group:

1. Select System – Devices and Feature Codes – Node IP Connection Groups – **<Node Connection Group number>**.
2. Select **Emergency Outgoing Access**.
3. Select **Day Mode** or **Night Mode**.
4. Select the endpoint(s) you want to remove, right-click, and then select **Remove Selected Items**.

NOTICE

Responsibility for Regulatory Compliance.

It is the responsibility of the organization and person(s) performing the installation and maintenance of Mitel Advanced Communications Platforms to know and comply with all regulations required for ensuring Emergency Outgoing Access at the location of both the main system and any remote communication endpoints. Remote IP and SIP endpoints may require gateway access to nearby emergency responders.

Emergency Call phone numbers include:

- 911, the default for Mitel systems located in the U.S.
- 999, the default for Mitel systems located in the European market and used primarily in the United Kingdom U.K.
- If applicable, 112, an emergency number used widely in Europe outside of the U.K.
- Any emergency number, such as for a police or fire station, that is appropriate for the location of the main system and/or remote endpoints.

Remote Node

The Remote Node field is a link to the node to which the connection group corresponds.

Camp-Ons Allowed

The Camp On feature can be enabled or disabled for each node IP connection group. If disabled, users placing outgoing calls will hear busy signals when all connections in the group are in use or unavailable. If enabled, users will be able to camp on and wait for an available connection.

To enable/disable the Camp On Allowed flag:

1. Select System – Devices and Feature Codes – Node IP Connection Groups – **<Node Connection Group number>**.
2. Select **Camp-Ons Allowed**.
3. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
4. Press **ENTER** or select another field to save the change.

System and Device IP Settings

Introduction	9-3
IP Device Status	9-4
System IP Settings	9-5
General IP Settings	9-6
Mitel 5600 Base Server/Processing Server Connection Settings	9-11
Viewing or Changing Base Server/Processing Server Connection Settings	9-11
Refreshing the PS-1 to Base Server Connection Status	9-11
Editing the PS-1 to Base Server Connection Password	9-12
Web/SSH Settings	9-13
TFTP Settings	9-14
Advanced IP Settings	9-15
NTP Server Configuration	9-16
NTP Server Advanced IP Settings	9-16
NTP Server Troubleshooting	9-16
Local Processor Module and Expansion Card IP Settings	9-17
NAT IP Address	9-18
Audio RTP Type of Service and Data Type of Service	9-18
Audio Stream Receive Port	9-19
IP Terminal TCP Call Control Port	9-19
IP Terminal General Purpose UDP Port	9-19
MGCP Receive Port	9-20
TCP Call Control Port	9-20
Echo Profile	9-20
Remote Node IP Connections	9-21
Viewing Off-Node IP Connections	9-21
Creating Off-Node IP Connections	9-22
Node IP Connection Group	9-22
Remote IP Address	9-22
Remote Audio Receive Port	9-23
Remote Listening Port	9-23
IP Call Configurations	9-24
Adding Call Configurations	9-25
Adding IP Endpoints to the Call Configuration	9-25
Adding Trunks to the Call Configuration	9-25

Adding SIP Voice Mails to the Call Configuration	9-26
Programming Call Configuration Options	9-27
Audio Diagnostics Sampling Period	9-27
Audio Diagnostics Samplings	9-27
Audio Frames/IP Packet	9-28
Average In Time Frame Percentage Threshold and Timer	9-28
Minimum Playback Time	9-29
Transmit DTMF Level	9-30
DTMF Encoding Setting	9-30
Speech Encoding Setting	9-30
Fax Control-Messages Redundancy Count	9-31
Fax Page-Data Redundancy Count	9-31
Fax Detection Sensitivity	9-31
Fax Encoding Setting (Fax Transmission)	9-32
Fax Maximum Connection Speed	9-32
Supports RTP Redirect	9-33
Sockets	9-34
Enabling or Disabling a Socket Connection	9-34
Entering a Socket Password	9-35
Endpoint and Device IP Settings	9-36
Emergency Extensions for IP Devices	9-37
Network Configuration	9-38
Mitel IP Endpoint Configuration Options	9-38
Inter-Tel IP Endpoint Network Configuration Options	9-39
Call Configuration	9-39
Reserve IP Resource for Device	9-40
Network Group	9-40
NAT Address Type	9-40
Programming Inter-Tel IP Endpoints in ITP Mode	9-41
Resource Reservation Tool	9-42
Resource Reservation Constraints	9-42
Configuring Resources	9-43
Reserved By Function Tab	9-44
Reserved By Device Tab	9-47
Advanced Tab	9-48

Introduction

This chapter describes Mitel 5000 Internet Protocol (IP) features and functionality. This includes 5000 system IP settings in the organizational network and endpoint IP settings and features.

System IP devices include the following:

- IP endpoints, including Mitel and Inter-Tel branded IP endpoints
- SIP endpoints
- MGCP endpoints and Gateways
- Session Initiated Protocol (SIP) endpoints and gateways

For more information about system IP networks, refer to the following resources in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000:

- Appendix A: Mitel Private Networking
- Appendix B: Network Topology

This chapter includes the following IP settings and devices information:

- “IP Device Status” on [page 9-4](#)
- “System IP Settings” on [page 9-5](#)
- “Local Processor Module and Expansion Card IP Settings” on [page 9-17](#)
- “Remote Node IP Connections” on [page 9-21](#)
- “IP Call Configurations” on [page 9-24](#)
- “Sockets” on [page 9-34](#)
- “Endpoint and Device IP Settings” on [page 9-36](#)
- “Resource Reservation Tool” on [page 9-42](#)

IP Device Status

When an endpoint comes online, it searches for a valid license. For more information about IP device licensing, refer to the “System Description” chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

Table 9-1. *IP Device Status Dialog Descriptions – License Category*

Entry in Dialog	Entry Description
Unlicensed	The endpoint was unable to retrieve a valid license and is currently unlicensed.
Category A	The endpoint is using a Category A license.
Category B	The endpoint is using Category B license.
Category C	The endpoint is using a Category C license.
Category D	The endpoint is using a Category D license.

You can view the connection status of Mitel IIP devices on the system at any time from the IP Status page. The window displays the following information about each IP device.

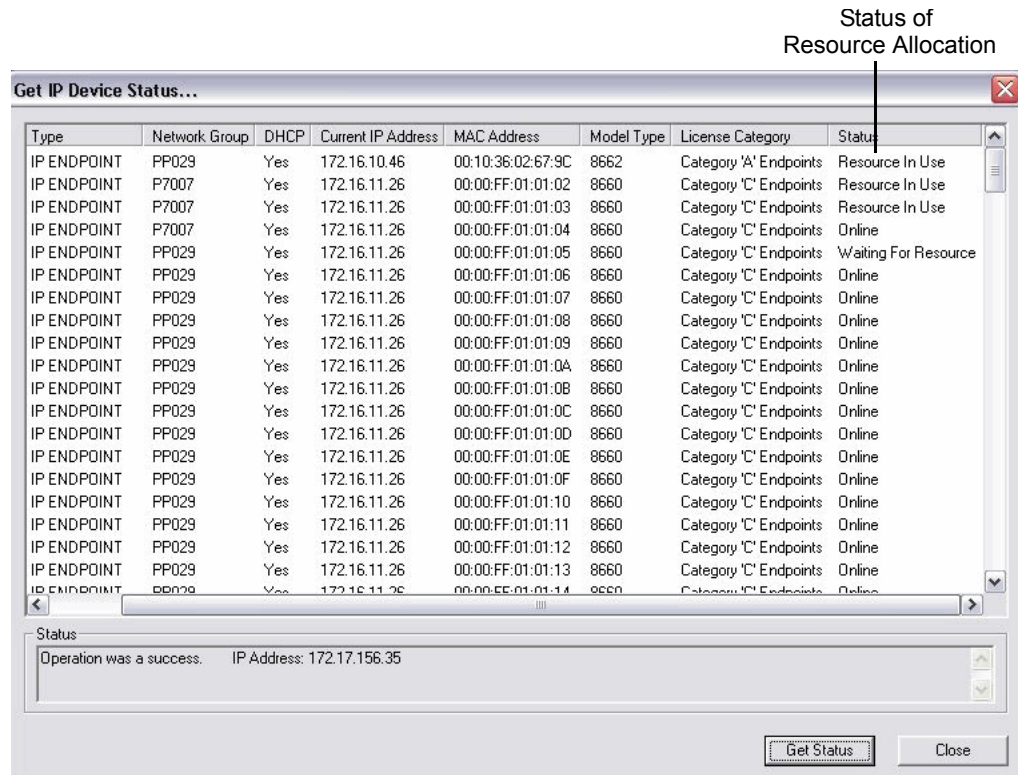
- **Extension:** Indicates the extension number assigned to the IP device.
- **Type:** Displays the device type associated with the extension. Possible options include IP ENDPOINT and IP SLA.
- **Network Group:** Displays the network group that the extension has been assigned. If a network group has not been assigned, the extension will reside in the default PP029.
- **DHCP:** Indicates whether Mitel 5000 DB Programming is configured to DHCP for this device. It does not necessarily mean the device is actually using DHCP, the device could be set to a static IP.
- **Current IP Address:** Displays the IP address currently assigned to the device.
- **MAC Address:** Displays the MAC address assigned to the device.
- **Model Types:** Indicates the type of IP Device. For details, see Figure 6-7 “IP Device Status Dialog Box Model Type and License Category Column” on [page 6-104](#).
- **License Category:** Indicates the type of license associated with the endpoint.

The Status column in the IP Device Status option, as shown in Figure 9-1 on [page 9-5](#), contains the following status indications for IP resource allocation:

- **Online:** Indicates that the device is currently online.
- **Offline :** Indicates that the device is currently offline.
- **No License:** Indicates that there is no license available for the device.
- **Resource In Use:** Indicates that the device has requested and has been allocated an IP resource.
- **Waiting For Resource:** Indicates that the device has requested a resource, but all of the resources were in use. Therefore, the device is camped on to wait for a resource.

For more information about IP Device Status, refer to *Mitel 5000 DB Programming Help*.

Figure 9-1. Get IP Device Status



System IP Settings

Changing IP database settings may drop all calls in progress.

This following sections describes IP settings, which includes the following:

- **General IP Settings Parameters:** General IP options that apply for both the Base Server and the Processing Server. For more information, see [page 9-6](#).
- **Base Server/Processing Server Connection Settings:** Contains settings required for communication between the Base Server and the Processing Server. For more information, see [page 9-11](#).

NOTE

Base Server/Processing Server Connection Settings option apply to Mitel CS-5600 systems only. If your system is a Mitel CS-5200 or CS-5400 system, this option and its settings appear with a red "X."

- **Web/SSH Settings:** Options to configure the SSH server or the Administrative Web Session. For more information, see [page 9-13](#).
- **TFTP Settings:** Options to configure the TFTP server. For more information, see [page 9-14](#).
- **Advanced IP Settings:** Options to configure the WINS and DNS servers. For more information, see [page 9-15](#).
- **NTP Server Configuration Settings:** Options to configure the NTP Server. When the Enable Network Time Protocol (NTP) flag is set to No, these fields are displayed with a red "X." Every time this field is changed, the system attempts an NTP update. For more information, see [page 9-16](#).
- **Remote Configuration Settings:** *This feature is reserved for controlled introduction.* Configures on-demand Remote Configuration options. For more information, see "Remote Configuration" on [page 3-54](#).

General IP Settings

Table 9-2 on [page 9-7](#) shows general IP setting options that apply to *both* the Mitel 5000 Base Server (all Mitel 5000 systems) and the Processing Server (Mitel 5600 systems only). For detailed instructions to apply DB Programming settings in the installation process, refer to the Installation chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

To view or change General IP settings:

Select System – IP Settings. General IP settings are shown in the right pane, as shown in [Figure 9-2](#).

Figure 9-2. General IP Settings

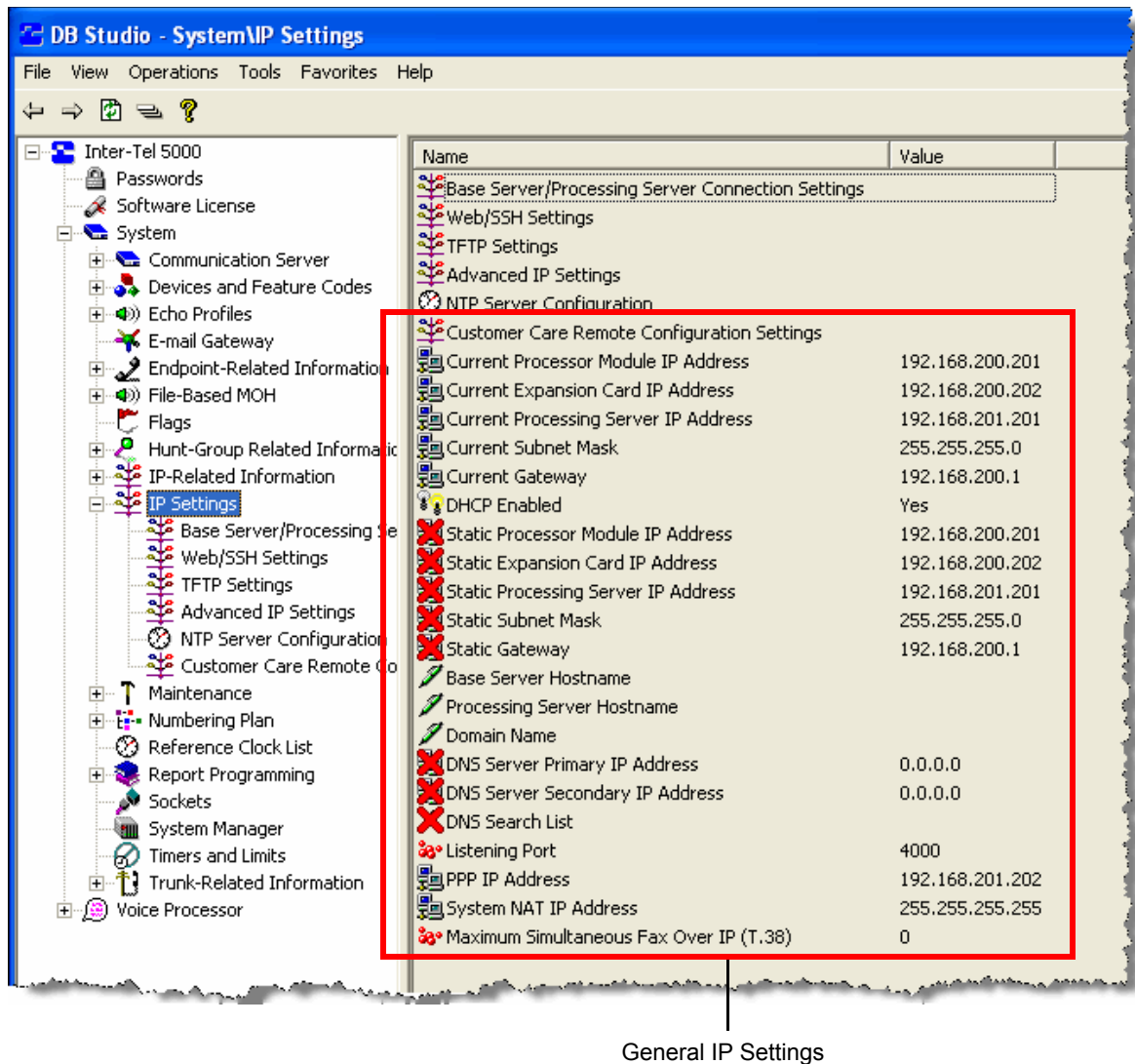


Table 9-2. General IP Settings Fields

Option	Description	Range	Default
Current Processor Module IP Address	<i>Read-only.</i> Indicates the current IP address of the Processor Module on the Base Server. Applies to 5200, 5400, and 5600 systems. This value may change if using a DHCP server to obtain an IP address.	0.0.0.0 – 255.255.255.255	192.168.200.201
Current Expansion Card IP Address	<i>Read-only.</i> Identifies the current IP address of the Expansion Card on the Base Server. It applies for 5400 and 5600 systems (not displayed for 5200 systems).	0.0.0.0 – 255.255.255.255	192.168.200.202
Current Processing Server IP Address	<i>Read-only.</i> Identifies the current IP address of the Processing Server. It only applies for 5600 systems (not displayed for 5200 or 5400 systems). This value may change if using a DHCP server to obtain an IP address.	0.0.0.0 – 255.255.255.255	192.168.201.201
Current Subnet Mask	<i>Read-only.</i> Displays the current subnet mask assigned to the IP port for both the Base Server and Processing Server that are on the same subnet. This value may change if using a DHCP server to obtain an IP address.	0.0.0.0 – 255.255.255.255	255.255.255.0
Current Gateway	<i>Read-only.</i> Identifies the current IP address of the network gateway for both the Base Server and Processing Server that are on the same subnet. This value may change if using a DHCP server to obtain an IP address.	0.0.0.0 – 255.255.255.255	192.168.200.1
DHCP Enabled	Determines whether Dynamic Host Configuration Protocol (DHCP) is used for both Base Server and Processing Server.	Yes/No	Yes
Static Processor Module IP Address	Specifies the static IP Address of the Processor Module on the Base Server. It appears with a red “X” if DHCP is enabled.	0.0.0.0 – 255.255.255.255	192.168.200.201
Static Expansion Card IP Address	Specifies the static IP Address for the Expansion Card. Applies for 5400 and 5600 systems (not shown if a 5200 system). It appears with a red “X” if DHCP is enabled.	0.0.0.0 – 255.255.255.255	192.168.200.202
Static Processing Server IP Address	Specifies the static IP Address of the Processing Server. Applies for 5600 systems only (not shown if a 5200 or 5400 system). It appears with a red “X” if DHCP is enabled.	0.0.0.0 – 255.255.255.255	192.168.200.201
Static Subnet Mask	Specifies the default subnet mask associated with the Base Server/Processing Server IP address. Displays with a red “X” if DHCP is enabled.	0.0.0.0 – 255.255.255.255	255.255.255.0
Static Gateway	Specifies the default IP address of the gateway that is used to access the port. Displays with a red “X” if DHCP is enabled.	0.0.0.0 – 255.255.255.255	192.168.200.1

Table 9-2. General IP Settings Fields (Continued)

Option	Description	Range	Default
Base Server Hostname	<p>Specifies the Base Server hostname provided by the IP network administrator.</p> <p>Allows you to access the system without having to enter the IP address.</p> <p>Also used to identify the system on the network.</p> <p>Because the Basic Voice Mail (BVM) e-mail system requires DNS and a valid hostname, deleting the hostname causes BVM to fail. For more information about BVM, see “Mitel Voice Processing Systems” on page 11-4.</p> <div> <p>NOTE</p> <p>To receive and send e-mail messages using Voice Profile for Internet Mail (VPIM), the Base Server Hostname must be the same as the DNS hostname programmed in the Domain Name field under System – IP Settings. If the hostname does not match the DNS server hostname or if an alias is used for the address, the system cannot resolve the name and its destination, and the VPIM server may reject the message.</p> </div>	<p>String (0–15 characters)</p> <p>Avoid using special characters such as the asterisk (*), tilde (~), etc. in hostnames.</p>	Blank
Processing Server Hostname	<p>Specifies the Processing Server hostname provided by the IP network administrator. Applies for 5600 systems only. Not shown otherwise.</p> <p>Allows you to access the system without having to enter the IP address.</p> <p>Also used to identify the system on the network.</p> <p>Because the Basic Voice Mail (BVM) e-mail system requires DNS and a valid hostname, deleting the hostname causes BVM to fail. For more information about BVM, see “Mitel Voice Processing Systems” on page 11-4.</p> <div> <p>NOTE</p> <p>To receive and send e-mail messages using VPIM, the Processing Server Hostname must be identical to the DNS hostname programmed in the Domain Name field under System – IP Settings. If the hostname does not match the DNS server hostname or an alias is used for the address, the system cannot resolve the name and its destination, and the VPIM server may reject the message.</p> </div>	<p>String (0–15 characters)</p> <p>Avoid using special characters such as the asterisk (*), tilde (~), etc. in hostnames.</p>	Blank

Table 9-2. General IP Settings Fields (Continued)

Option	Description	Range	Default
Domain Name	<p>The domain name that identifies the local system for VPIM. For example, the following VPIM address “Doe, John <1000@LocalDomain.com.” When the system sends a VPIM message, the “From” address contains the VPIM domain. When other VPIM systems sends messages to the local system, the “To” address contains an address with the domain as the VPIM domain of the local system. For more information, see “Voice Profile for Internet Mail (VPIM) Networking” on page 11-9.</p> <div> <p>NOTE</p> <p>To receive and send e-mail messages using VPIM, the Base Server Hostname or Processing Server Hostname must be the same as the DNS hostname programmed in the Domain Name field. If the hostname does not match the DNS server hostname or if an alias is used for the address, the system cannot resolve the name and its destination, and the VPIM server may reject the message.</p> </div>	<p>String (0–15 characters)</p> <p>Avoid using special characters such as the asterisk (*), tilde (~), etc. in hostnames.</p>	Blank
DNS Server Primary IP Address	<p>Specifies the DNS Primary IP address for both the Base and Processing Servers that are on the same subnet. However, if the Processing Server requires a different DNS Primary IP Address, this may be programmed in the Advanced IP Settings subfolder.</p> <p>Displayed with a red “X” if DHCP is enabled.</p>	0.0.0.0 – 255.255.255.255	0.0.0.0
DNS Server Secondary IP Address	<p>Specifies the DNS server secondary IP address for both the Base and Processing Servers that are on the same subnet. However, if the Processing Server requires a different DNS Secondary IP address, this may be programmed in the Advanced IP Settings subfolder (see page 9-15).</p> <p>Displayed with a red “X” if DHCP is enabled.</p>	0.0.0.0 – 255.255.255.255	0.0.0.0
DNS Search List	<p>Specifies the DNS Search List for both the Base and Processing Servers that are on the same subnet. However, if the Processing Server requires a different DNS Search List, this may be programmed in the Advanced IP Settings subfolder (see page 9-15).</p> <p>Displayed with a red “X” if DHCP is enabled.</p>	String, up to 200 characters	Blank
Listening Port	<p>Specifies the port number that the system uses to process incoming socket requests (e.g., for voice mail, OAI, and so on).</p>	none	4000
PPP IP Address	<p>Specifies the PPP IP address of the internal modem in the chassis.</p>	0.0.0.0 – 255.255.255.255	192.168.201.202

Chapter 9: System and Device IP Settings

System IP Settings

Table 9-2. General IP Settings Fields (Continued)

Option	Description	Range	Default
System NAT IP Address	<p>Specifies the NAT, or public, IP address that is used to put a SIP gateway behind a NAT. The NAT IP address is the address the system recognizes on the NAT side of the firewall.</p> <p>To correctly inform the gateway where the SIP messages are originating from, you must also program the SIP Gateway Name field. For programming instructions, see “Placing a SIP Gateway Behind a NAT Device” on page 6-7.</p>	0.0.0.0 – 255.255.255.255	255.255.255.255
Maximum Simultaneous Fax Over IP (T.38)	<p>Specifies how many IP networking resources should be reserved/allocated as T.38 and specifies the maximum Fax Over IP calls that can be placed simultaneously. This flag can also be configured in the Resource Reservation Tool. For details, see page 9-42.</p>	0-6	0

Mitel 5600 Base Server/Processing Server Connection Settings

Base Server/Processing Server Connection Settings options apply to Mitel CS-5600 systems only. If your system is a Mitel CS-5200 or CS-5400, these options are shown with red Xs.

Viewing or Changing Base Server/Processing Server Connection Settings

You can view or change the settings shown in [Table 9-3](#).

Table 9-3. Base Server/Processing Server Connection Settings Fields

Setting	Description	Range	Default
Base Server/Processing Server Connection Address	Specifies the IP address that the PS-1 uses to connect with the Base Server.	0.0.0.0–255.255.255.255	192.168.200.201
Base Server/Processing Server Connection Port	Specifies the port number the PS-1 uses to connect with the Base Server.	1–65535	3400
Base Server/Processing Server Connection Status	For a remote Mitel CS-5600 session only, this field shows the status of the connection between the PS-1 and Base Server. For other system types or a CS-5600 local session, this field displays with a red “X.” The connection status is only retrieved for a CS-5600 remote session of DB Programming when you browse to this folder.	Connected/Disconnected If the connection is set to “Disconnected,” you are warned against changing the settings. The warning only appears once during a session.	Disconnected

To view or change Base Server/Processing Server Connection Settings:

1. Select System – **IP Settings**.
2. Double-click **Base Server/Processing Server Connection Settings**.

Refreshing the PS-1 to Base Server Connection Status

You can refresh the connection status without closing and reopening DB Programming.

To refresh the connection:

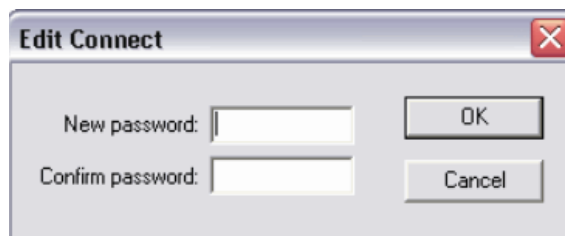
1. Select System – **IP Settings**.
2. Double-click **Base Server/Processing Server Connection Settings**.
3. Right-click **Base Server/Processing Server Connection Status**. The status field is updated.

Editing the PS-1 to Base Server Connection Password

You can specify the password that the PS-1 uses to connect with the Base Server. To enhance security, the password is encrypted and is not displayed as an editable option. Because the password does not correspond to a field in the database, the password cannot be saved or restored in the database. Although a default password is provided so the PS-1 and Base Server can communicate initially, Mitel recommends that you set your own password. The Edit Password option appears only in *remote* mode for a Mitel 5600 system. The password cannot be edited in local mode.

To set the password:

1. Select System – IP Settings – **Base Server/Processing Server Connection Settings**.
2. Double-click **Base Server/Processing Server Connection Settings**.
3. Right-click in the right pane, and then select **Edit Password**. The following dialog box appears.



4. In the **New password** and **Confirm password** boxes, enter the new password, up to 128 characters.
5. Click **OK** to save the change.

Web/SSH Settings

Table 9-4 shows Web/SSH settings.

To view or edit Web/SSH settings:

1. Select System – IP Settings.
2. Double-click **Web/SSH Settings**. Web/SSH settings appear in the right pane.

Table 9-4. Web/SSH Settings Fields

Field Name	Description	Range	Default
SSH (Secure Shell) Server Enabled	Specifies whether or not the SSH Server is enabled to log into OLM (Online Monitor).	Yes/No	Yes
SSH Server Port	Specifies the port number that the SSH Server uses.	1–65535	22
Web Listening Port	Specifies the port number that the Web Server uses. If using the IP port for the Upload Utility, the Web Listening Port number must match the port number assigned in the Upload Utility.	1–65535	80
Web Server Enabled	Specifies whether or not Administrative Web Session (AWS) is enabled.	Yes/No	Yes
Base Server Web Theme	Corresponds to the theme for the AWS. You may set different themes for the Base and Processing Servers to make it easy to tell which AWS you are viewing based on its theme.	Default, Aqua, Desert, Gray Scale, Inter-Tel, Mint, or Rose	Default
Processing Server Web Theme	Corresponds to the theme for the AWS. You may set different themes for the Base and Processing Servers to make it easy to tell which AWS you are viewing based on its theme.	Default, Aqua, Desert, Gray Scale, Inter-Tel, Mint, or Rose	Default
Web/SSH Password	Specifies the password used to log into the Web pages.	characters	itpassw

TFTP Settings

Table 9-5 shows TFTP settings.

NOTE

If you are logged on to both DB Programming and AWS at the same time *and* you use AWS to change TFTP settings, the DB Programming view will not refresh immediately. To see the new TFTP settings, you must restart DB Programming.

To view or edit Web/SSH settings:

1. Select System – **IP Settings**.
2. Double-click **TFTP Settings**. TFTP settings appear in the right pane

Table 9-5. TFTP Settings Fields

Field Name	Description	Range	Default
Base Server Upgrade TFTP IP Address	Specifies the path and name of the directory to where upgrade files will be located on the TFTP server root directory. Applies to the Base Server. You can also use AWS to configure this option.	0.0.0.0 – 255.255.255.255	0.0.0.0
Base Server Upgrade TFTP Pathname	Specifies the path and name of the directory to where upgrade files will be located on the TFTP server root directory. Applies to the Processing Server in a CS-5600 system. This field is not visible for a CS-5200/5400 system. You can also use AWS to configure this option.	String (up to 126 characters)	Intl5000
Base Server Upgrade TFTP Port	If a firewall is between the Mitel 5000 system and the TFTP server, this port needs to be open to the TFTP server from the DMZ. Applies to the Base Server. You can also use AWS to configure this option.	1–65535	69
Processing Server Upgrade TFTP IP Address	Specifies the path and name of the directory to where upgrade files will be located on the TFTP server root directory. Applies to the Base Server. You can also use AWS to configure this option.	0.0.0.0 – 255.255.255.255	0.0.0.0
Processing Server Upgrade TFTP Pathname	Specifies the path and name of the directory to where upgrade files will be located on the TFTP server root directory. Applies to the Processing Server. You can also use AWS to configure this option.	String (up to 126 characters)	Intl5000
Processing Server Upgrade TFTP Port	If a firewall is between the Mitel 5000 system and the TFTP server, this port needs to be open to the TFTP server from the DMZ. Applies to the Processing Server in a 5600 system. This field is not visible for a 5200/5400 system. You can also use AWS to configure this option.	1–65535	69
Enabled On-Board TFTP Server	Enables the TFTP Server running on the 5000 system that is used for endpoint upgrades. It is set to Yes by default.	Yes/No	Yes

Advanced IP Settings

Table 9-6 shows Advanced IP Settings.

To view or edit Advanced IP settings:

1. Select System – IP Settings.
2. Double-click **Advanced IP Settings**. Advanced IP settings appear in the right pane

Table 9-6. Advanced IP Settings Fields

Field Name	Description	Range	Default
Current Base Server WINS	(Read-only.) Displays the current IP address of the WINS Server for the Base Server. The value may change if using a DHCP server to obtain an IP address.	0.0.0.0 – 255.255.255.255	0.0.0.0
Current Processing Server WINS	(Read-only.) Displays the current IP address of the WINS Server for the Processing Server. The value may change if using a DHCP server to obtain an IP address. This field is visible in a 5600 system only.	0.0.0.0 – 255.255.255.255	0.0.0.0
Static Base Server WINS	Specifies the IP connection's WINS IP address provided by the IP network administrator. Applies to the Base Server.	0.0.0.0 – 255.255.255.255	0.0.0.0
Static Processing Server WINS	Specifies the IP connection's WINS IP address provided by the IP network administrator. Applies to the Processing Server.	0.0.0.0 – 255.255.255.255	0.0.0.0
Processing Server DNS Server Primary IP Address	Used for when the Processing Server needs to point to a different DNS than the Base Server. This field is displayed with a red 'X' if DHCP is enabled. Use case—Set the DNS Server Primary IP Address in the System\IP Settings folder for the Base Server (which affects both the Base and Processing Servers and updates this field as well), and then change this field. Likewise for the following two fields, "Processing Server DNS Server Secondary IP Address" and "Processing Server DNS Search List." Only applies for 5600 systems (not shown otherwise).	0.0.0.0 – 255.255.255.255	0.0.0.0
Processing Server DNS Server Secondary IP Address	Used for when the Processing Server needs to point to a different DNS than the Base Server. Only applies for 5600 systems (not shown otherwise). This field is displayed with a red "X" if DHCP is enabled. See Processing Server DNS Server Primary IP Address field on page 9-15 for use case.	0.0.0.0 – 255.255.255.255	0.0.0.0
Processing Server DNS Search List	Used for when the Processing Server needs to point to a different DNS than the Base Server. Only applies for 5600 systems (not shown otherwise). This field is displayed with a red "X" if DHCP is enabled. See Processing Server DNS Server Primary IP Address field on page 9-15 for use case.	0.0.0.0 – 255.255.255.255	0.0.0.0
SIP UDP Listening Port Enable	Enables/disables the external SIP gateway port.	Yes/No	Yes
SIP UDP Listening Port	Specifies the port number that an external SIP gateway uses.	1025–65468	5060

NTP Server Configuration

This folder contains the fields used to configure the NTP Server. When the Enable Network Time Protocol (NTP) flag is set to No, these fields are displayed with a red “X.” Every time this field is changed, the system will attempt an NTP update. The fields can also be programmed in the Configuration Wizard.

Table 9-7. *NTP Server Configuration Fields*

Field Name	Description	Range	Default
NTP Server Hostname	Specifies the hostname for the NTP server that is used.	String	north-america.pool.ntp.org (for U.S. systems) or europe.pool.ntp.org (for European systems)
NTP Server IP Address	Specifies the IP address of the NTP Server.	0.0.0.0 – 255.255.255.255	0.0.0.0

NTP Server Advanced IP Settings

If you are using the NTP server hostname instead of the IP address, you must also configure the following options in “Advanced IP Settings” on [page 9-15](#):

- Processing Server DNS Server Primary IP Address
- Processing Server DNS Server Secondary IP Address
- Processing Server DNS Search List

NTP Server Troubleshooting

If you have problems with NTP:

- Verify DB Programming.
- Check DNS settings using `ipconfig /all` from the DOS command prompt.
- Check Message Print messages for “NTP Synchronization Successful” or “NTP Synchronization Failed” messages.
- Verify settings and logs on Web page.

Local Processor Module and Expansion Card IP Settings

NOTICE

System ports used for IP call control and audio may be reserved for other protocols, such as SIP, which uses port 5060 by default. For security purposes, NAT devices, firewalls, or routers occasionally block these ports. If the ports are blocked, you may experience audio or connection problems. If this occurs, change the port numbers in DB Programming to avoid conflicts.

You can program information about each IP connection in the private network. In the IP Connections folder (see [Figure 9-3](#)), the right pane displays shortcuts for the Processor module (IP resource settings) and Processor Expansion Card (extra IP resources).

To view or edit Processor Module or Expansion Card IP Connection settings:

1. Select System – Devices and Feature Codes – IP Connections – Local – **<extension>**.

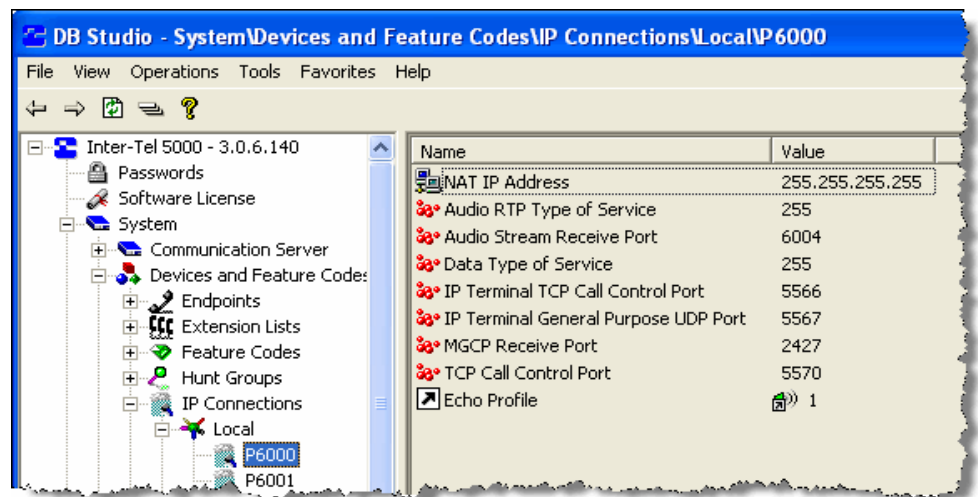
If applicable, type the description and user name for the Processor Module or Expansion Card: The description, which appears in all IP connection lists in the database, can consist of up to 20 characters. The username, which appears on display endpoints, can consist of up to 10 characters. To program the names, select the box and type the entry. Do not use slash (/), backslash (\), vertical slash (|), or tilde (~), in usernames. Do not use Control characters in descriptions or usernames.

2. Double-click either **Processor Module** or **Expansion Card** to view IP settings.

You can program the following IP settings for the local Processor Module and Expansion Card, as shown in [Figure 9-3](#).

- “NAT IP Address” on [page 9-18](#)
- “Audio RTP Type of Service” on [page 9-18](#)
- “Audio Stream Receive Port” on [page 9-19](#)
- “Data Type of Service” on [page 9-18](#)
- “IP Terminal TCP Call Control Port” on [page 9-19](#)
- “IP Terminal General Purpose UDP Port” on [page 9-19](#)
- “MGCP Receive Port” on [page 9-20](#)
- “TCP Call Control Port” on [page 9-20](#)
- “Echo Profile” on [page 9-20](#)

Figure 9-3. Local Processor Module and Expansion Card IP Settings



NAT IP Address

You can program the NAT IP address for the local Processor Module or Expansion Card. A NAT device translates private network IP addresses to one or more public network IP addresses based on NAT translation rules.

NAT devices are installed at the edge of the private network and have internal and external interfaces (and IP addresses). For outgoing IP traffic from the private network to the Internet, NAT translates the source IP address. For incoming IP traffic from the Internet to the private network, NAT translates the destination IP address. NAT devices provide the following advantages:

- Internal IP addresses are hidden from the open Internet and therefore more secure.
- IP addresses are conserved because they are allocated dynamically when needed.

Despite the advantages of NAT devices, they can cause problems for protocols using Peer-to-Peer technologies like multimedia traffic on VoIP networks using SIP.

For more information about NAT, refer to the System Features chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

To program the NAT IP Address:

1. Select System – Devices and Feature Codes – IP Connections – **Local**.
2. Double-click either **Processor Module** or **Expansion Card**.
3. In the **NAT IP Address** option, click the value shown in the **Value** column. The Edit NAT IP Address dialog box appears.
4. Enter the public IP Address that is statically NATed to the private native address. For example, the programmed IP address for the system. The default address is 255.255.255.255.
5. Click **OK**.

Audio RTP Type of Service and Data Type of Service

The Audio RTP and Data Types of Service specify the precedence for audio and data packets. The system inserts the values of these two fields into the Type of Service (ToS) field of each audio and data packet. Network devices can then use the value of the ToS field to establish precedence for IP routing. The default value is 0, meaning the packets have no precedence. A value of 184 indicates “IP Precedence.” All other values may be used by a network device using Differentiated Services (Diffserv) to establish precedence.

To establish precedence for IP routing:

1. Select System – Devices and Feature Codes – IP Connections – **Local**.
2. Double-click either **Processor Module** or **Expansion Card**.
3. Select either **(Audio RTP)** or **(Data) Type of Service**.
4. In the **Value** column, enter the new value in the box.
5. Click out of the field or press **ENTER** to save the change.

Audio Stream Receive Port

The Audio Stream Receive Port defines the first of the (even-numbered) ports that the system uses to receive audio data packets from IP endpoints, IP gateways, and remote nodes. The Audio Stream Receive Port must not conflict with port numbers used by other applications running on the system, such as Call Processing, BVM, and so on.

Although the system allows the Processor Module and Processor Expansion Card port values to overlap, the default database does **not** allow these ports to overlap. [Table 5-17](#) shows the value ranges and default values.

Table 9-8. *Audio Stream Receive Port Ranges and Default Values*

Module	Range	Default Value
Processor Module (PM-1)	1025–64000	6004
Processor Expansion Card (PEC-1)	1025–64000	6604

The system broadcasts changes to an IP connection Audio Stream Receive Port to the other nodes in the private network as a database update. This field corresponds to the remote IP connection Remote Audio Receive Port—see [page 9-23](#).

To change the Remote Audio Receive Port number:

1. Select System – Devices and Feature Codes – IP Connections – **Local**.
2. Double-click either **Processor Module** or **Expansion Card**.
3. Select **Audio Stream Receive Port**.
4. In the **Value** column, type the new number in the box.
5. Click out of the field or press **ENTER** to save the change.

IP Terminal TCP Call Control Port

The IP Terminal TCP Call Control Port defines the port number the IP resource application uses for call control.

To change the IP Terminal TCP Call Control Port number:

1. Select System – Devices and Feature Codes – IP Connections – **Local**.
2. Double-click either **Processor Module** or **Expansion Card**.
3. Select **IP Terminal TCP Call Control Port**.
4. In the **Value** column, type the new number in the box. The range is 1024–65535; the default is 5566.
5. Click out of the field or press **ENTER** to save the change.

IP Terminal General Purpose UDP Port

The IP Terminal General Purpose UDP Port defines the port number the IP resource application uses for general purpose and broadcast messages.

To change the IP Terminal General Purpose UDP Port number:

1. Select System – Devices and Feature Codes – IP Connections – **Local**.
2. Double-click either **Processor Module** or **Expansion Card**.
3. Select **IP Terminal General Purpose UDP Port**.
4. In the **Value** column, type the new number in the box. The range is 1024–65535; the default is 5567.
5. Click out of the field or press **ENTER** to save the change.

MGCP Receive Port

The MGCP Receive Port defines the port number the MGCP gateway and MGCP endpoints use for communication.

To change the MGCP Receive Port number:

1. Select System – Devices and Feature Codes – IP Connections – **Local**.
2. Double-click either **Processor Module** or **Expansion Card**.
3. Select **MGCP Receive Port**.
4. In the **Value** column, type the new number in the box. The range is 1024–65535; the default is 2427.
5. Click out of the field or press **ENTER** to save the change.

TCP Call Control Port

The TCP Call Control Port defines the port number that off-node IP resources use to connect call control with this IP resource. The TCP Call Control Port cannot conflict with other port numbers on the IP connection. The system broadcasts changes to an IP connection TCP Call Control Port to the other nodes in the private network as a database update. The IP connection TCP Call Control Port must be kept in sync throughout the network. This field corresponds to the off-node IP connection Remote Listening Port. For more information, see [“Remote Listening Port” on page 9-23](#).

To change the TCP Call Control Port number:

1. Select System – Devices and Feature Codes – IP Connections – **Local**.
2. Double-click either **Processor Module** or **Expansion Card**.
3. Select **TCP Call Control Port**.
4. In the **Value** column, type the new number in the box. The range of values is 1025–65535. The default is 5570.
5. Click out of the field or press **ENTER** to save the change.

Echo Profile

For information about Echo Profiles, see “Echo Profiles” on [page 10-5](#).

NOTE

If you are using the IP port for the Upload Utility, the Web Listening Port number must match the port number assigned in the Upload Utility. The default setting for both is 80.

To change the Echo Profile:

1. Select System – Devices and Feature Codes – IP Connections – **Local**.
2. Double-click either **Processor Module** or **Expansion Card**.
3. Select **Echo Profiles**.
4. In the **Value** column, type the new number in the box. The range is 1–65535, and the default is 80.
5. Click out of the field or press **ENTER** to save the change.

Remote Node IP Connections

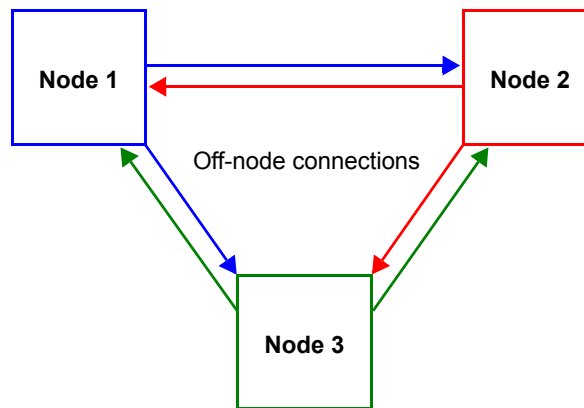
You can create remote node IP connections to represent IP resources on other nodes within the network. For each off-node IP connection, the following fields are displayed:

- “Node IP Connection Group” on [page 9-22](#)
- “Remote IP Address” on [page 9-22](#)
- “Remote Audio Receive Port” on [page 9-23](#)
- “Remote Listening Port” on [page 9-23](#)

NOTE

Each node in an IP network must have an off-node IP connection for all other IP nodes in the network. For example, in a three-node network, node 1 must have an off-node IP connection for nodes 2 and 3; node 2 must have off-node IP connections for nodes 1 and 3; and node 3 must have off-node IP connections for nodes 1 and 2. See the example in [Figure 9-4](#). Nodes that do not have the correct off-node IP connections programmed may not be able to communicate with each other.

Figure 9-4. IP Network Off-Node Connections



Viewing Off-Node IP Connections

You can view off-node IP connections for each remote node.

To view off-node IP connections:

Select System – Devices and Feature Codes – IP Connections – **<remote node>**. Off-node IP connections appear in the right pane.

Creating Off-Node IP Connections

You must create off-node IP connections for each remote IP node in the system network.

NOTE

When you create off-node connections and other IP-related extension numbers, use a numbering plan that associates the extension to the device and the node on which it resides. For example, the first IP resource on node 2 would be P6021 (P6 followed by the node number and then the IP resource number). The second would be P6022, and so on.

To create an off-node IP connection:

1. Select System – Devices and Feature Codes – IP Connections – *<remote node>* – *<extension>*.
2. Right-click in the right pane, and then click **Create Off-Node IP Connection**. The Create Off-Node IP Connection dialog box appears.
3. In the **Starting Extension** list, select an extension that begins with “P6.”
4. In the **Number of Extensions** list, select a unique extension for the IP connection.
5. Click **OK**.

Node IP Connection Group

The Node IP Connection Group option links to the node IP connection group in DB Programming to which the IP connection belongs. For more information, see “Node IP Connection Groups for Remote Nodes” on [page 8-54](#).

To view the node IP Connection Group settings:

1. Select System – Devices and Feature Codes – IP Connections – *<remote node>* – *<extension>*.
2. Double-click **Node IP Connection Group**.

Remote IP Address

The Remote IP Address defines the remote IP connection IP address provided by the network administrator. This corresponds to the static IP address programmed for the connection on the remote node. For more information, see “[System IP Settings](#)” on [page 9-5](#).

To change the Remote IP Address:

1. Select System – Devices and Feature Codes – IP Connections – *<remote node>* – *<extension>* – **Remote IP Address**.
2. In the **Value** column, click the current value. The Edit Remote IP Address dialog box appears.
3. Type the new IP address (do not include the periods). The following IP addresses are not allowed: 0.0.0.0 and 255.255.255.255.
4. Click **OK**.

Remote Audio Receive Port

The Remote Audio Receive Port defines the remote IP connection audio receive port. This should match the corresponding IP connection Audio Stream Receive Port (see [page 9-19](#)) programmed on the local node.

To change the Remote Audio Receive Port setting:

1. Select System – Devices and Feature Codes – IP Connections – *<remote node>* – *<extension>* – **Remote Audio Receive Port**.
2. In the **Value** column, click the current value, and then type the new port number in the box.
3. Click out of the field or press **ENTER** to save the change.

Remote Listening Port

The Remote Listening Port defines the remote IP connection listening port. This should match the corresponding IP connection TPC Call Control Port (see [page 9-20](#)) programmed on the local node.

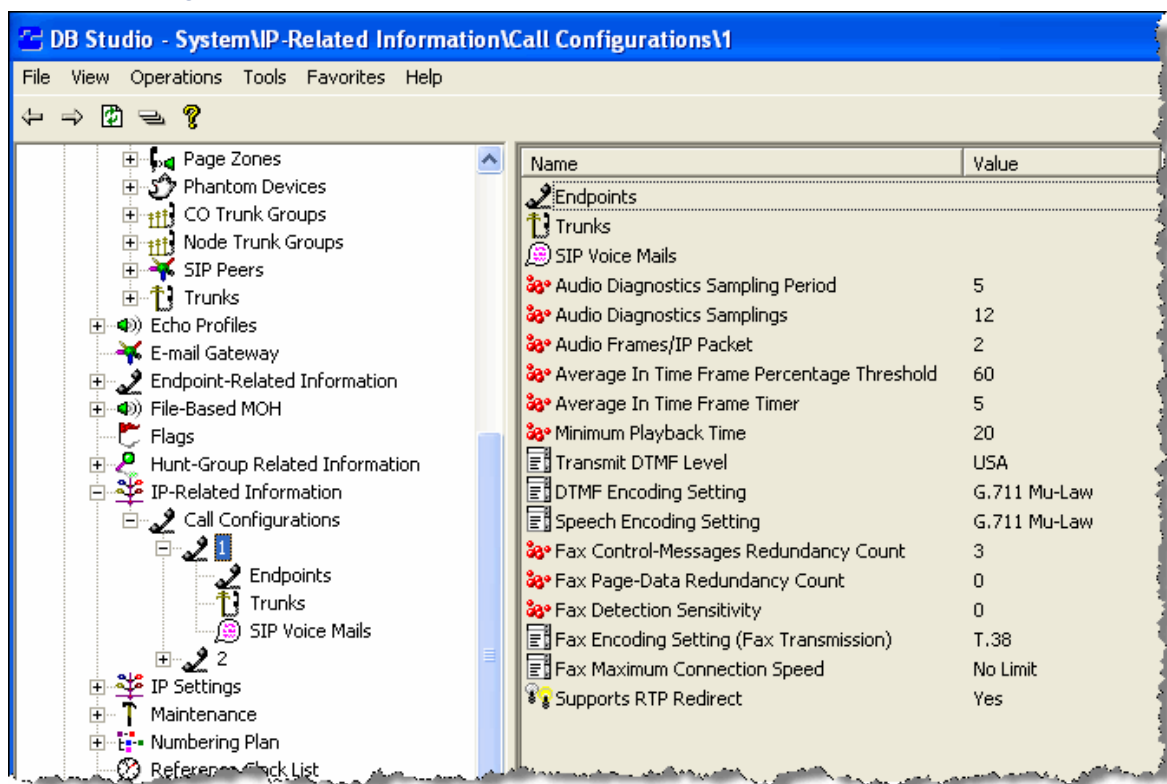
To change the Remote Listening Port setting:

1. Select System – Devices and Feature Codes – IP Connections – *<remote node>* – *<extension>* – **Remote Listening Port**.
2. In the **Value** column, click the current value, and then type the new port number in the box.
3. Click out of the field or press **ENTER** to save the change.

IP Call Configurations

Call configurations, as shown in Figure 9-5, define the settings that IP endpoints and gateways use when connected to calls. You can assign multiple devices to a specific call configuration.

Figure 9-5. Call Configuration Options



By default, all IP devices are placed in Call Configuration 1, which is programmable. You do not need to add SIP endpoints and MGCP endpoints to Call Configurations, because these devices negotiate call configurations before establishing a connection. You can program up to 25 different Call Configurations.

NOTE

IP Devices that use P2P to communicate do not have to share the same Call Configuration. When the system detects that IP devices have different settings, it uses the setting that consumes the least amount of bandwidth.

You cannot delete the default Call Configuration settings.

To view a list of IP endpoints that are currently assigned to the call configuration:

1. Select System – IP Related Information – Call Configurations – **Local** (or **Remote**).
2. Double-click **Endpoints**.

To view IP trunks that are currently assigned to a Call Configuration:

1. Select System – IP Related Information – Call Configurations – **Local** (or **Remote**).
2. Double-click **Trunks**. IP trunks include MGCP gateways and endpoints and SIP trunks.

Adding Call Configurations

If applicable, add any system trunks or before configuring configurations. See “Creating (Adding) Devices” on [page 7-4](#).

To add a Call Configuration:

1. Select System – IP Related Information – **Call Configurations**.
2. Right-click in the right pane, and then click **Add To Call Configurations List**.
3. Enter the starting ID and the number of call configurations that you want to program.
4. Click **OK**. The new call configurations appear in the list.
5. For each call configuration, select the current description, and then type the new entry in the box. The Call Configuration description can contain up to 20 characters.
6. Click out of the field or press **ENTER** to save the change.

You now need to add IP endpoints to the call configuration as described in the following section.

Adding IP Endpoints to the Call Configuration

To add IP endpoints to the list:

1. Select System – IP Related Information – **Call Configurations**.
2. Double-click the call configuration.
3. Double-click **Endpoints**.
4. In the right pane, right-click and then click **Move To Endpoints List**.
5. Select the IP endpoint types, and then click **Next**.
6. Select the devices to add to the list, and then click **Move Items**.
7. Click **Finish**.

Adding Trunks to the Call Configuration

To add trunks to the list:

1. Select System – IP Related Information – **Call Configurations**.
2. Double-click the call configuration.
3. Double-click **Trunks**.
4. Right-click in the right pane, and then click **Move To IP Trunks List**.
5. Select the trunk type, and then click **Next**.
6. Select the devices to add to the list, and then click **Move Items**.
7. Click **Finish**.

Adding SIP Voice Mails to the Call Configuration

For NuPoint Messenger voice processing systems only. For more information about NuPoint Messenger, refer to the *Mitel 5000 and NuPoint Messenger Integration Guide*, part number 580.8008 or *NuPoint Messenger Technical Documentation Help*.

To add SIP Voice Mails to the Call Configuration:

1. Select System – IP Related Information – **Call Configurations**.
2. Double-click the call configuration.
3. Double-click **SIP Voice Mails**.
4. Right-click in the right pane, and then click **Move To SIP Voice Mails List**.
5. Select the SIP Voice Mail type, and then click **Next**.
6. Select the devices to add to the list, and then click **Move Items**.
7. Click **Finish**.

Programming Call Configuration Options

You can program the following call configuration options:

- “Audio Diagnostics Sampling Period” below
- “Audio Diagnostics Samplings” on [page 9-27](#)
- “Audio Frames/IP Packet” on [page 9-28](#)
- “Average In Time Frame Percentage Threshold and Timer” on [page 9-28](#)
- “Minimum Playback Time” on [page 9-29](#)
- “Transmit DTMF Level” on [page 9-30](#)
- “DTMF Encoding Setting” on [page 9-30](#)
- “Speech Encoding Setting” on [page 9-30](#)
- “Fax Control-Messages Redundancy Count” on [page 9-31](#)
- “Fax Page-Data Redundancy Count” on [page 9-31](#)
- “Fax Detection Sensitivity” on [page 9-31](#)
- “Fax Encoding Setting (Fax Transmission)” on [page 9-32](#)
- “Fax Maximum Connection Speed” on [page 9-32](#)
- “Supports RTP Redirect” on [page 9-33](#)

Audio Diagnostics Sampling Period

Mitel IP 5000-series IP endpoints only. The Audio Diagnostics Sampling Period indicates the time, in seconds, of a sampling interval. Mitel IP endpoints report the statistics at the set interval. Setting the period to 0 seconds sets the diagnostics to report after the audio stream is broken down with an interval of the entire audio stream. Increasing the Audio Diagnostic Sampling Period increases the lost-packet tolerance of endpoints using the Call Configuration.

If during an interval of the Audio Diagnostic Sampling Period, the received packets percentage drops below the Average In Time Frame Percentage (see [page 9-28](#)), the system displays an Insufficient Bandwidth for Voice alarm A032 for the Mitel endpoint reporting the bad statistics.

To program the Audio Diagnostics Sampling Period:

1. Select System – IP Related Information – **Call Configurations**.
2. Double-click the call configuration.
3. Select **Audio Diagnostics Sampling Period**.
4. In the **Value** column, select the sampling period (in seconds) from the list. The range is 0–300 seconds; the default value is 5 seconds.
5. Click out of the field or press **ENTER** to save the change.

Audio Diagnostics Samplings

Mitel Model 5000-series IP endpoints only. Indicates the number of network statistics samplings that call processing saves. The samplings occur every Audio Diagnostic Sampling Period.

To program the Audio Diagnostics Samplings:

1. Select System – IP Related Information – **Call Configurations**.
2. Double-click the call configuration.
3. Select **Audio Diagnostics Samplings**.
4. In the **Value** column, select the number of samplings from the list. The range is 1–100; the default value is 12.
5. Click out of the field or press **ENTER** to save the change.

Audio Frames/IP Packet

The Audio Frames/IP Packet option is the number of audio frames that the system inserts into each packet. The system defines an audio frame as 10 ms of audio. Each audio packet consists of the number of frames set in the Audio Frames/IP Packet option. For example, if you set the Audio Frames/IP Packet option to “2,” each audio packet contains two frames (20 ms of audio).

Consider the following when setting this option:

- The lower the value, the lower the latency (delay) in the signal. However, fewer audio frames per packet increases bandwidth consumption (more packets are required), which also increases the chance of jitter and network congestion.
- The higher the value, the higher the latency in the signal. However, more audio frames per packet lowers bandwidth consumption (fewer packets are required), which also decreases the chance of jitter and network congestion.
- Some IP endpoints support a smaller frames/packet range than this option allows. The system usually tries to negotiate a setting that is within range for both endpoints. Depending on the call control protocol, this may not always be possible, in which case you must configure the correct value.

To change the number of frames:

1. Select System – IP Related Information – **Call Configurations**.
2. Double-click the call configuration.
3. Select **Audio Frames/IP Packet**.
4. In the **Value** column, select the number audio frames per packet from the list. The range is 1–8 packets. The default value for local endpoints is 2 packets; the default value for remote endpoints is 3 packets.
5. Click out of the field or press **ENTER** to save the change.

Average In Time Frame Percentage Threshold and Timer

The Average In Time Frame Percentage Threshold / Average In Time Frame Timer settings indicate when network characteristics are inhibiting voice connections.

When the average number of in time frames falls below the Average In Time Frame Percentage Threshold *and* stays below that threshold for the time given by the Average In Time Frame Timer (in seconds), the system displays the INSUFFICIENT BANDWIDTH alarm. For more information about system alarms, refer to the “System Features” chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

NOTE

If the Average In Time Frame Percentage is set to zero (0), the INSUFFICIENT BANDWIDTH alarm is disabled for all endpoints in the selected call configuration.

To change the Average In Time Frame Percentage Threshold:

1. Select System – IP Related Information – **Call Configurations**.
2. Double-click the call configuration.
3. Select **Average In Time Percentage Threshold**.
4. In the **Value** column, select the percentage setting from the list. The range is 0–100%; the default is 60%.
5. Click out of the field or press **ENTER** to save the change.

To change the Average In Time Frame Timer:

1. Select System – IP Related Information – **Call Configurations**.
2. Double-click the call configuration.
3. Select **Average In Time Frame Timer**.
4. In the **Value** column, select the percentage setting from the list. The range is 0–255 seconds; the default is 5 seconds.
5. Click out of the field or press **ENTER** to save the change.

Minimum Playback Time

The Minimum Playback Time is the time, in milliseconds (ms), that packets wait in the receive buffer before the system plays the audio. The higher this number, the more latency in the signal; however, it is less likely that network problems like jitter would cause lost or late audio packets. The lower the minimum playback time, the less latency there is in the signal; however, there is a greater chance of jitter.

To change the Minimum playback Time setting:

1. Select System – IP Related Information – **Call Configurations**.
2. Double-click the call configuration.
3. Select **Minimum Playback Time**.
4. In the **Value** column, select the time (in ms) from the list. The range is 1–320 ms; the default is 20 ms.
5. Click out of the field or press **ENTER** to save the change.

Transmit DTMF Level

Defines the level at which the system injects tone onto the backplane when receiving an out-of-band DTMF tone. The options are U.S., Japan, U.K., or Mexico. By default, this is the country associated with the language selected in the Session Manager.

To change the Transmit DTMF Level country:

1. Select System – IP Related Information – **Call Configurations**.
2. Double-click the call configuration.
3. Select **Transmit DTMF Level**.
4. In the **Value** column, select the country from the list.
5. Click out of the field or press **ENTER** to save the change. The Extended Value and dB columns automatically update to reflect the values associated with the country.

DTMF Encoding Setting

The DTMF Encoding Setting is the vocoder type used to send DTMF. The options are G-711 Mu-Law, G-711 A-Law, G-729, and RFC 2833. For MGCP gateways and endpoints, this value must either match the Speech Encoding Setting field or be set to RFC 2833. By default, this is G.711 Mu-Law [G.711 A-Law in Europe]. If the DTMF Encoding Setting field is set incorrectly, users cannot dial DTMF tones while on a call.

To change the DTMF Encoding Setting:

1. Select System – IP Related Information – **Call Configurations**.
2. Double-click the call configuration.
3. Select **DTMF Encoding Setting**.
4. In the **Value** column, select the vocoder type from the list.
5. Click out of the field or press **ENTER** to save the change.

Speech Encoding Setting

The Speech Encoding Setting is the vocoder that the system uses when transmitting speech data. The options are G.711 Mu-Law, G.711 A-Law, G.729, G.729B (VAD), and BroadVoice 32. For MGCP gateways and endpoints, if the DTMF Encoding Setting is set to RFC 2833, set this value to either G.729 or G.711; if the DTMF Encoding Setting is set to G.729 or G.711, this value must match (for example, set to G.729 or G.711).

To change the Speech Encoding Setting:

1. Select System – IP Related Information – **Call Configurations**.
2. Double-click the call configuration.
3. Select **Speech Encoding Setting**.
4. In the **Value** column, select the vocoder type from the list.
5. Click out of the field or press **ENTER** to save the change.

Fax Control-Messages Redundancy Count

Applies to Session Initiation Protocol (SIP) voice mail only. Controls the redundancy count for the fax control messages. The range is 0–7. It is set to 3 by default. The Control-Data redundancy is set to 3 by default because losing even one control message may cause the fax call to fail. Increasing the Control-Data redundancy does not have an impact on the bandwidth. If a red “X” is displayed in this field, you must change the Fax Detection Sensitivity field to any value other than 0.

To program the Fax Control-Messages Redundancy Count:

1. Select System – IP-Related Information – **Call Configurations**.
2. Select the call configuration.
3. Select **Fax Control-Messages Redundancy Count**.
4. In the **Value** column, select or enter the redundancy setting. The range is 0–7; the default is 3.
5. Click out of the field or press **ENTER** to save the change.

Fax Page-Data Redundancy Count

Applies to SIP voice mail only. Controls the redundancy count for the fax page data. In general, the more redundancy, the more reliable. However, increasing the Page Data redundancy increases the bandwidth. Losing some Page Data may impact the quality of the image. If a red “X” is displayed in this field, you must change the Fax Detection Sensitivity field to any value other than 0.

To program the Fax Page-Data Redundancy Count:

1. Select System – IP-Related Information – **Call Configurations**.
2. Select the call configuration.
3. Select **Fax Page-Data Redundancy Count**.
4. In the **Value** column, enter the redundancy setting. The range is 0–3. The default is 0.
5. Click out of the field or press **ENTER** to save the change.

Fax Detection Sensitivity

Applies to SIP voice mail only. Allows you to make false fax detection more or less likely. The higher this number, the less likely the system is to falsely detect fax transmission, but the more likely the system is to fail to correctly detect fax transmission. The lower the number, the more likely the system is to falsely detect fax transmission, but the less likely the system is to fail to correctly detect fax transmission. When this value is zero (0), all faxing options are disabled (indicated with a red “X” next to the options).

NOTE

If you are sending a fax between two Mitel 5000 systems and the Fax Detection Sensitivity settings on the two servers conflict (one is zero and one is nonzero), faxing will not work.

To program the Fax Page-Data Redundancy Count:

1. Select System – IP-Related Information – **Call Configurations**.
2. Select the call configuration.
3. Select **Fax Page-Data Redundancy Count**.
4. In the **Value** column, select or enter the redundancy setting. The range is 0–100; the default is 0, indicating that faxing is disabled.
5. Click out of the field or press **ENTER** to save the change.

Fax Encoding Setting (Fax Transmission)

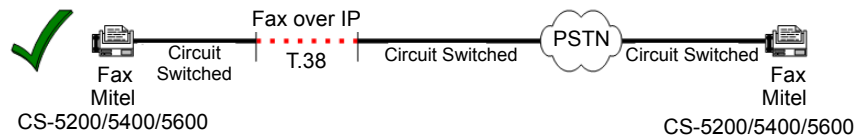
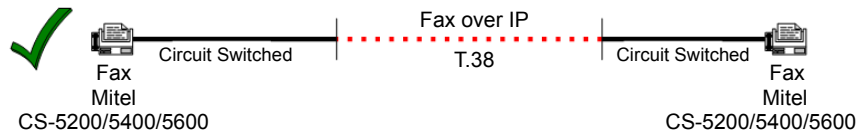
Applies to SIP voice mail only. Defines the vocoder that the system uses when the system believes it is transmitting fax data. If a red “X” is displayed in this field, you must change the Fax Detection Sensitivity field to any value other than 0.

NOTICE

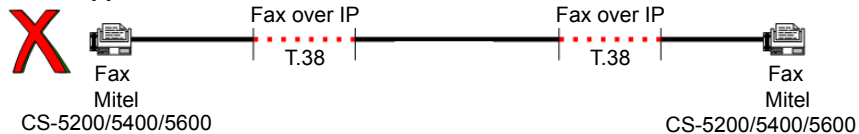
Mitel currently supports T.38 Fax over IP (FoIP) only. If you change any of the fax settings to a value other than the current default setting of T.38, a warning message appears. If you click **OK** when this message is displayed and continue to program the fax settings, you do so at your own risk.

The Mitel 5000 supports only a 1-hop T.38 connection, as illustrated in the examples below.

Supported



NOT Supported



To select the Fax Encoding Setting (Fax Transmission) setting:

1. Select System – IP-Related Information – **Call Configurations**.
2. Select the call configuration.
3. Select **Fax Encoding Setting (Fax Transmission)**.
4. In the **Value** column, select the option from the list. The options are G.711 Mu-Law, G.711 A-Law, and T.38. The default setting is T.38.
5. Click out of the field or press **ENTER** to save the change.

Fax Maximum Connection Speed

Applies to SIP voice mail only. Defines the fax connection speed. The available options are 2400 or 4800 or 7200 or 9600 or 12000 or 14400 or No Limit. It is set to *No Limit* by default. If a red “X” is displayed in this field, you must change the Fax Detection Sensitivity field to any value other than 0.

To select the Fax Maximum Connection Speed:

1. Select System – IP-Related Information – **Call Configurations**.
2. Select the call configuration.
3. Select **Fax Maximum Connection Speed**.
4. In the **Value** column, select the option from the list.
5. Click out of the field or press **ENTER** to save the change.

Supports RTP Redirect

Determines whether the SIP Peer changes the source port of the RTP and whether the VoIP should start sending its RTP to the new port. It is set to No by default.

To change the RTP Redirect setting:

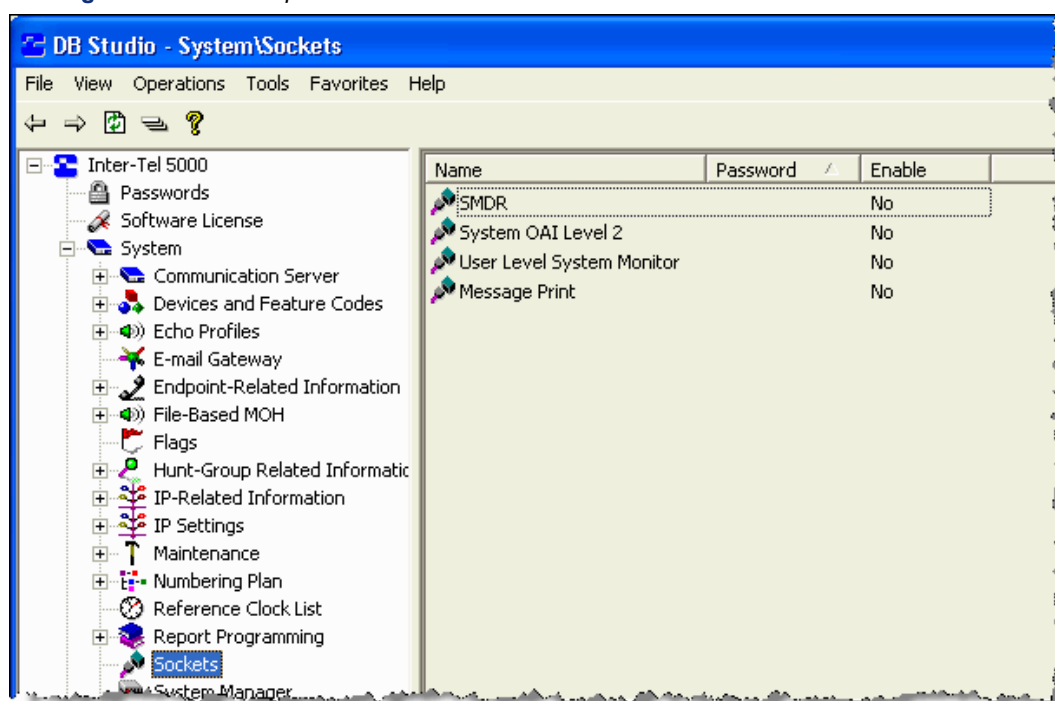
1. Select System – IP-Related Information – **Call Configurations**.
2. Select the call configuration.
3. Select **Supports RTP Redirect**.
4. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
5. Click out of the field or press **ENTER** to save the change.

Sockets

You can set TCP/IP socket connections for the following applications, as shown in [Figure 9-6](#):

- SMDR (for external voice processing systems)
- System Open Architecture Interface (OAI) Level 2
- User Level System Monitor
- Message Print

Figure 9-6. Socket Options



Enabling or Disabling a Socket Connection

You can enable or disable socket connections.

To enable or disable a socket connection:

1. Select System – Sockets – **<socket option>**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Click out of the field or press **ENTER** to save the change.

Entering a Socket Password

Socket passwords prevent unauthorized users from accessing socket applications when using the following diagnostic and OAI tools:

- Diagnostics Monitor (SMDR, User Level System Monitor, and Message Print sockets)
- OAI (System OAI Level 2 socket)

To enter a socket password:

1. Select System – Sockets – **<socket option>**.
2. In the Password column, right-click, and then click **Edit Password**. The Edit Password **<option>** dialog box appears.
3. In the **Old Password** box, type the old password, if applicable.
4. In the **New Password** box, type the new password. Typed characters appear as asterisks (***).
5. In the **Confirm Password** box, retype the new password.
6. Click **OK** to exit and save the password. If the entered passwords match, you return to the Password field. If not, you must re-enter the new password.

Endpoint and Device IP Settings

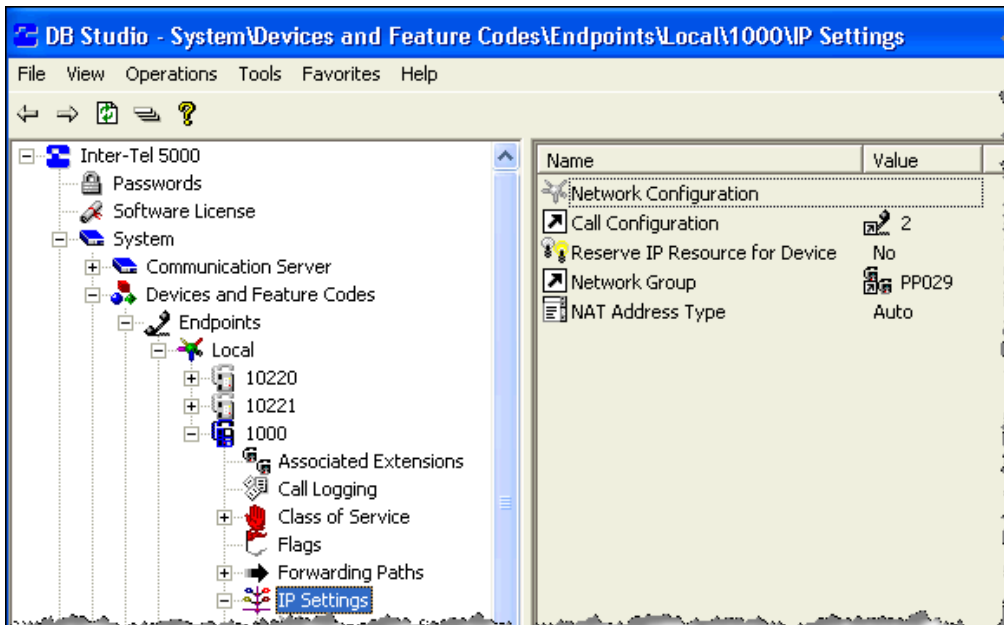
NOTE Changing IP database settings may drop all calls in progress.

System settings serve as a “template” for IP endpoints. However, you can change configuration settings for specific IP endpoints. For example, Dynamic Host Configuration Protocol (DHCP) can be enabled at the system level but disabled for a specific IP endpoint. DHCP would still be enabled for the other IP endpoints that are configured to use it at the system level. For more information about supported IP endpoints, refer to the “Endpoints” chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

The following sections describe endpoint IP settings, as shown in:

- “Emergency Extensions for IP Devices” on [page 9-37](#)
- “Call Configuration” on [page 9-39](#)
- “Reserve IP Resource for Device” on [page 9-40](#)
- “Network Group” on [page 9-40](#)
- “NAT Address Type” on [page 9-40](#)

Figure 9-7. Endpoint IP Settings



Emergency Extensions for IP Devices

The following procedure is recommended programming for a system that has remote loop termination with the need for emergency access for the remote IP endpoints.

WARNING

Possible Delay in Local Emergency Response to Remote Sites.

You should alert IP and SIP endpoint users to the following hazardous situations:

- If an Emergency Call phone number is dialed from an IP or SIP endpoint located at a remote site that is **not** equipped with a correctly configured gateway, the call will be placed from the location where system chassis is installed rather than from the location where the emergency call is made.

In this situation, emergency responders may be dispatched to the wrong location. To minimize the risk of remote site users misdirecting emergency responders, Mitel recommends regular testing of MGCP/SIP gateway trunk(s) for dial tone.

- If uninterruptible power supply (UPS) protection has not been installed as part of the Mitel 5000 system, IP and SIP endpoints will **not** operate when electrical power fails either at remote sites or at the main system location.

To place calls during a power failure in this situation, IP and SIP endpoint users can only use a single line endpoint connected to one of the power failure bypass circuits built into the system chassis. If an endpoint connected to a power failure bypass circuit is not available, users should make emergency calls **from a local phone not connected to the system**. For details about the Power Failure Bypass feature, refer to the "Installation" chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

Responsibility for Regulatory Compliance:

It is the responsibility of the organization and person(s) performing the installation and maintenance of Mitel Advanced Communications Platforms to know and comply with all regulations required for ensuring Emergency Outgoing Access at the location of both the main system and any remote communication endpoints. Remote IP and SIP endpoints may require gateway access to nearby emergency responders.

Emergency Call phone numbers include:

- 911, the default for Mitel systems located in the U.S.
- 999, the default for Mitel systems located in the European market and used primarily in the U.K.
- If applicable, 112, an emergency number used widely in Europe outside of the U.K.
- Any emergency number, such as for a police or fire station, that is appropriate for the location of the main system and/or remote endpoints.

Equipment Damage Hazard. Use only a single appropriate power adapter. Do **not** connect a U.S. power supply and a universal power supply (UPS) to the same device.

Also, when using the UPS with a barrel connector, no devices (for example, hubs) should be inserted between the KS/SLA jack on the adapter and the LAN jack on the endpoint because power is supplied through the cable.

NOTE

If an installation needs Emergency Outgoing Access across nodes, make sure the Local Trunk Group is the first member in the facility group. This allows cross-node emergency calls to use the Local Trunk Group first and **not** the Remote IP Trunk Group.

The following procedure provides information on how to program an emergency extension for IP devices. Refer to the following books for more information:

- *AudioCodes MGCP Gateway Installation Guide*, part number 835.2741
- *AudioCodes MP-114 SIP Gateway Installation Manual*, part number 835.3202
- *Quintum SIP Gateway Installation Manual*, part number 835.3123

To program an emergency extension for an IP device:

1. Create a Trunk Group that contains the MGCP gateway or SIP trunk(s).
2. Program the Trunk Group as the Emergency Extension for the remote IP endpoints.
3. Program the Emergency Outgoing Access for the Trunk Group MGCP gateway or SIP trunk(s), give the remote IP endpoints outgoing access, but remove all other endpoints and extension lists.
4. Program the Local Trunk Group as the Emergency Extension for local endpoints.
5. Program the Emergency Outgoing Access for the Local Trunk Group, include all local endpoints, but **not** the remote IP endpoints.
6. Create a facility group that contains the Local Trunk Group first, followed by the Trunk Group for the IP endpoints.
7. Program this facility group in Route Group 1.
8. Program the Emergency Outgoing Access for all node trunk groups to include no devices. Each node should have local trunk termination because emergency outgoing access across nodes is not warranted.

Network Configuration

The following sections describe network configuration options for Mitel and Inter-Tel IP endpoints.

Mitel IP Endpoint Configuration Options

Network Configuration options for Mitel IP endpoints include the following:

- **MAC Address:** The MAC address that was programmed when the device was assigned a circuit. The system reads the MAC address, but it does not set this on the endpoint.
- **Audio Stream Receive Port:** The Mitel IP Endpoint Audio Stream Receive Port has a range of 50098–50508 with a default of 50100, which differs from the other IP endpoints. This field programs the base receive port number for all channels on this device. Because this device only has one channel, the first audio channel uses base+2 for RTP and base+3 for RTCP, if used.
- **Call Control Timeout:** The number of seconds that the system waits between heartbeats before it determines that the device is offline.

To view or change Mitel IP Endpoint Network options:

1. Select System – Devices and Feature Codes – Endpoints – Local – **<extension>**.
2. Double-click **IP Settings**.
3. Double-click **Network Configuration**.
4. Program the desired options, and then click out of each area or press **ENTER** to save your changes.

Inter-Tel IP Endpoint Network Configuration Options

For descriptions about Inter-Tel IP options, refer to *Mitel 5000 Database Programming Help*. You can program the following network settings for IP endpoints:

- MAC Address *
- Hostname *
- Static IP Address *
- Static Gateway *
- Static Subnet Mask *
- Static WINS Server *
- IP Address Assignment: BOOTP *
- DHCP Enabled *
- Remote Server IP Address *
- Overwrite Self Programming *
- Telnet Server *
- Web Server *
- Audio RTP Type of Service
- Audio Stream Receive Port
- Password
- Call Control Timeout
- IP Terminal TCP Call Control Port
- IP Terminal General Purpose UDP Port

* The system does not set this information for the Models 8662, 8622, 8620, and 8600 endpoints, even though the fields exist in DB Programming. These endpoints use configuration files over TFTP for configuration or manual programming using Administrative Web Session (AWS).

Call Configuration

The call configuration assigned to the endpoint. For more information, see “IP Call Configurations” on [page 9-24](#).

To view or change the IP Endpoint Call Configuration:

1. Select System – Devices and Feature Codes – Endpoints – Local – **<extension>**.
2. Double-click **IP Settings**.
3. Select **Call Configuration**.
4. In the **Value** column, type the new Call Configuration number in the box.
5. Click out of each area or press **ENTER** to save your change.

Reserve IP Resource for Device

Enables or disable the Reserve IP Resource feature for the endpoint. For more information, see “Resource Reservation Tool” on [page 9-42](#).

To enable or disable Reserve IP Resource for Device:

1. Select System – Devices and Feature Codes – Endpoints – Local – **<extension>**.
2. Double-click **IP Settings**.
3. Select **Reserve IP Resource for Device**.
4. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
5. Click out of the field or press **ENTER** to save the change.

Network Group

Displays the Network Group to which the device belongs. For more information, see “Network Groups” on [page 8-52](#).

To change the Network Group:

1. Select System – Devices and Feature Codes – Endpoints – Local – **<extension>**.
2. Double-click **IP Settings**.
3. Select **Network Group**.
4. In the **Value** column, type the new Network Group in the box.
5. Click out of the field or press **ENTER** to save the change.

NAT Address Type

Specifies the NAT address type as follows:

- **Native**: Used for internal IP endpoints (those that do not pass through near-end NAT).
- **NAT**: Used for external IP endpoints (those that do pass through near-end NAT).
- **Auto**: Allows the IP endpoints to be moved inside or outside the firewall (NAT) without programming intervention. For more information, see “Understanding NAT Challenges for SIP Devices” on [page 6-6](#).

NOTE

The “Auto” option is not applicable to SIP Trunks, MGCP Gateways, MGCP endpoints, and Mitel endpoints. You must manually select the NAT Type setting (Native or NAT). IP endpoints retain the NAT Address Type settings after an upgrade. Any database converted to v2.0 or later with the “Auto” option set has this field changed to “Native.”

For more information about IP endpoint NAT settings, refer to the “Endpoints” chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

To change the NAT Address Type:

1. Select System – Devices and Feature Codes – Endpoints – Local – **<extension>**.
2. Double-click **IP Settings**.
3. Select **NAT Address Type**.
4. In the **Value** column, select the option from the list.
5. Click out of the field or press **ENTER** to save the change.

Programming Inter-Tel IP Endpoints in ITP Mode

When the IP endpoint is in ITP mode, the system sends down configuration information when the IP endpoint powers up. However, the only fields that the system can update are as follows:

- MAC Address
- Telnet Server
- Password (changes the password on the IPR side, *not* the endpoint side).
- Audio RTP Type of Service
- Audio Stream Receive Port
- Call Control Timeout
- IP Terminal TCP Call Control Port
- IP Terminal General Purpose UDP Port

These options are located under System – Devices and Feature Codes– Endpoints – *<IP endpoint>* – IP Settings – Network Configuration. The remaining fields must come from the areas that are programmed in a higher priority configuration source, such as the internal database, self-programming mode, configuration files, and so on.

Resource Reservation Tool

NOTICE

Reservations Reduce Available Shared Resources. Avoid unnecessarily reserving IP resources. Reserving IP resources reduces the number of resources available for sharing in an oversubscribed system. The more reservations you make, the smaller the pool of shared resources becomes, which increases the potential for delay due to camping on for resources. Reserved resources are used only while the identified function or endpoint is active. The rest the time, reserved resources cannot be used for other purposes.

You can use the Resource Reservation Tool to reserve IP resources for specific IP endpoints or system functions. For example, if you reserve two resources for Basic Voice Mail (BVM), the two resources are removed from the shared pool of resources that is dynamically allocated by the system. The first two simultaneous calls to BVM use the reserved resources. Additional calls to BVM have resources allocated from the shared pool.

The following two messages related to reserving resources may appear on display IP endpoints:

- For calls to BVM, if both reserved BVM resources and shared resources are unavailable, the calling party endpoint displays the BVM EXT IS BUSY message.
- For calls to an endpoint, if resources are not available the call is placed in a Camp On state, and the WAITING FOR RESOURCES message displays until resources become available.

Resource Reservation Constraints

Keep the following constraints in mind when reserving resources for specific endpoints or functions:

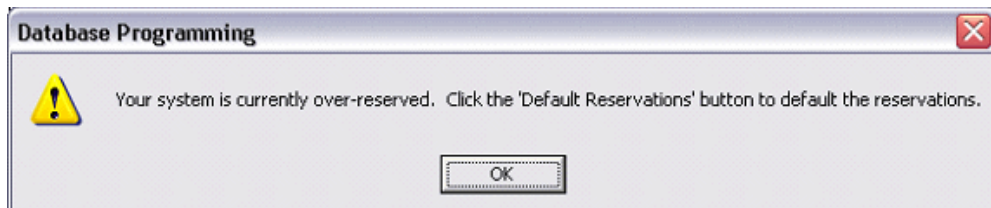
- You should **not** configure reservations unless IP resources are oversubscribed.
- If the system is primarily digital, the demand for IP resources should be minimal. Therefore, IP resources are unlikely to be oversubscribed so reservations should **not** be used.
- Mitel recommends that you reserve IP resources for attendants and other high-traffic users such as call center agents. However, excessive use of reservations degrades the effectiveness of oversubscription by reducing the amount of resources that can be shared. In most cases, only a fraction of the users are likely to be on calls at any given time, which minimizes the likelihood of needing to camp on for IP resources.
- Reserving IP resources for a specific device guarantees that the device can communicate to the system, as long as the IP resources are available when the resource is dedicated. If the IP resources are not available when requested, the endpoint camps on until they become available. Reserving IP resources does not guarantee that a call can be completed. For example, if no trunks are available a call could not be completed even if adequate IP resources were available.
- A call to an All-Ring Hunt Group is essentially a call to each hunt group member. The system will consume an IP resource for every IP endpoint in the All-Ring Hunt Group. Therefore, a single call can consume a great deal of IP resources. Mitel recommends that you minimize the use of All-Ring Hunt Groups in a system that uses oversubscription. If All-Ring Hunt Groups span multiple nodes, the consumption of resources can be even greater.

- A call to a page zone is essentially a call to each member of the page zone. The system consumes an IP resource for every IP endpoint in the page zone. Therefore, a single call can consume a great deal of IP resources. Mitel recommends that you carefully consider the use of all page zones containing IP endpoints in a system that uses oversubscription.
- An endpoint with Background Music enabled is essentially the same as a call to the endpoint. This is effectively the same as reserving an IP resource for the endpoint. Therefore, enabling Background Music for a large number of IP endpoints can consume a great deal of IP resources. Mitel recommends that you minimize the use of background music on IP endpoints on a system that uses oversubscription. You can also change the feature code for Background Music to restrict use.

Configuring Resources

To configure resources:

1. Make sure you have configured all IP devices (see [page 9-36](#)), IP Networking (see [page 9-37](#)), BVM ports (see [page 11-54](#)), and Call Configurations (see [page 9-24](#)).
2. From the DB Studio Tools menu, select **Resource Reservation Tool**. When the Resource Reservation Tool starts, if the current reservations in the database cause the system to be over-reserved, the following warning appears. To default the reservations, click **OK**, and then click **Save**.



3. Select the **Reserved By Function** tab to reserve resources based on the following three functions. For more information about the Reserved By Function tab, see [page 9-44](#).
 - Emergency/911 resources
 - Basic Voice Mail port resources
 - Maximum simultaneous Fax over IP (T.38)
4. Select the **Reserved By Device** tab to reserve resources for individual IP devices. All configured IP devices are listed on this tab. For more detailed information about the Reserved by Device tab, see [page 9-47](#).
5. Select the **Advanced** tab to view reservations based on vocoder types for IP Endpoints, Trunks, or Networking, as well as reservations for Caller ID Transmitters and Caller ID Receivers. Changing the values appearing on this tab is not permitted; the information is displayed for reference only. For more detailed information about the Advanced tab, see [page 9-47](#).

At any time while programming through this tool, you can click one of the following buttons:

- **Help:** Opens the online Help.
- **Default Reservations:** Defaults all the reservations in each tab of the tool to their default values. The default values are not committed to the database until you click the **Save** or **Save and Close** button.
- **Save:** Saves the current reservations of all tabs to the database.
- **Save And Close:** Saves all the current reservations from all tabs and closes the Resource Reservation Tool dialog.
- **Close:** Closes the Resource Reservation Tool without making any changes to the database.

NOTE

If more resources have been reserved than a system can support, the DB Test utility reports an error and defaults the reserved resources fields to 0.

Reserved By Function Tab

The Reserved By Function tab allows you to reserve resources based on functions. The available functions are summarized in Table 9-9 on [page 9-45](#).

Figure 9-8. *Reserved By Function Tab*

The screenshot shows the 'Resource Reservations' dialog box with the 'Reserved By Function' tab selected. It includes a note about configuration, guidelines for reserving resources, and a table with three columns: Function, Reserved, and Range. The table lists three functions: Emergency/911 Resources Reserved (Reserved: 1, Range: 1 - 123), Basic Voice Mail Port Resources Reserved (Reserved: 0, Range: 0 - 4), and Maximum Simultaneous Fax Over IP (T.38) (Reserved: 0, Range: 0 - 6). The 'Reserved' column has input fields for each function. At the bottom are buttons for Help, Default Reservations, Save, Save and Close, and Close.

Resource Reservations

Note: All IP devices, BVM ports, IP Networking, and Call Configurations should be configured prior to adjusting resource reservations. Use the fields in the 'Reserved' columns to adjust the resource reservations.

Reserved By Function | Reserved By Device | Advanced

Guidelines: It is recommended that you reserve resources for functions that cannot tolerate any delays in getting resources like Emergency/911. To utilize Fax Over IP, you must enter reservations for the maximum Fax Over IP calls you expect to occur simultaneously. Note that, in general, reserving resources is less efficient than sharing resources.

Function	Reserved	Range
Emergency/911 Resources Reserved	1	1 - 123
Basic Voice Mail Port Resources Reserved	0	0 - 4
Maximum Simultaneous Fax Over IP (T.38)	0	0 - 6

Help | Default Reservations | Save | Save and Close | Close

Table 9-9. *Reserved By Function Fields*

Function Title	Description	Guidelines	Default Value and Range ¹
Emergency/911 Resources Reserved	<p>For each Emergency/911 reservation, the system reserves a G.729 resource. This way, even if all the remaining resources are currently in use, if a user tries to place an emergency call, the call will receive this emergency/911 resource and be able to go through without having to camp on. If more than one emergency call is placed, but only one resource is reserved for emergency, the first call will receive the reserved resource and the other call will have to have a resource allocated from the shared pool. If all shared resources are currently in use, the second call will camp on.</p> <p>Reserving IP resources for a 911 call guarantees that 911 calls can communicate with the Mitel 5000 system. It does <i>not</i> guarantee that a call can always be completed (for example, if no trunks are available).</p>	<p>Mitel recommends that the emergency resource reservation count be set at 1 with the understanding that on heavily loaded systems only the first emergency call is guaranteed to have IP resources available. Note that heavily loaded systems will likely have IP resources reserved for specific endpoints, and that the 911 reservations apply only to the IP endpoints that do not have IP resources reserved.</p> <p>Mitel also recommends that IP resources be reserved as emergency reservations for IP Gateway trunks used for emergency access. In other words, if IP Gateway Trunks are used for emergency access, the Emergency/911 resource reservation setting should be twice the number of concurrent 911 calls to be supported. For example, if the system uses IP trunks (MGCP or SIP gateway trunks) and uses IP endpoints, set the Emergency/911 resource reservation value to at least 2: 1 for an IP endpoint and 1 for the IP trunk.</p>	<p>Default: 1</p> <p>Range: 1–75 (CS-5200) 1–175 (CS-5400) 1–250 (CS-5600)</p>
Basic Voice Mail Port Resources Reserved	<p>BVM requires an IP resource for each voice mail port. For the CS-5200 or CS-5400, the G.729A codec and the G.726-32 codec are used for BVM. For the CS-5600, G.711 vocoders are used for BVM. Systems using external voice mail (for example, Enterprise Messaging) do not use BVM ports. For more information, refer to <i>Mitel 5000 DB Programming Help</i>.</p>	<p>Mitel recommends reserving IP resources for BVM ports. This action allows digital endpoints and Auto Attendant functions to avoid delays.</p>	<p>Default: 0</p> <p>Range: 0–16</p> <p>Note: The maximum BVM reservations are further limited by the Voice Processor\Timers And Limits\Number of Voice Channels field. This field is limited in remote mode by the number of ports licensed for BVM.</p>

Table 9-9. Reserved By Function Fields (Continued)

Function Title	Description	Guidelines	Default Value and Range ¹
Maximum Simultaneous Fax over IP (T.38)	This reservation type is slightly different than the others. It does <i>not</i> reserve IP resources from the shared pool. Instead, it reserves T.38 vocoder types for any IP networking call placed. To place a Fax over IP (FoIP) call, a networking resource is allocated (either from the shared pool or from the reservations if any are available). This networking resource must be allocated as a T.38 vocoder, which has a higher “cost” associated with it than the G.711 or G.729. To compensate for the higher cost, each networking reservation utilizes a T.38 resource up to the number specified in this field. Therefore, the maximum number of FoIP calls that can be placed simultaneously will equal the number of reservations made in this field. Because an FoIP call cannot be placed unless there is at least one reservation made, this field also appears in the IP Settings folder. See “System IP Settings” on page 9-5 .	Mitel recommends that the number of concurrent T.38 calls be set to a reasonable maximum. T.38 calls are costly in terms of IP resources, and setting this value higher than necessary needlessly takes IP resources away from the shared pool.	Default: 0 Range: 0–6

1. The upper limit of the range for each individual reservation can be further limited by the other reservations currently configured

As you change the different reservations, you will see the ranges changing dynamically. A progress bar is displayed as the ranges are calculated along with the message “Updating Ranges.” For each given reservation type, you will always know how many additional reservations you can make. Note that the progress bar is just an approximate visual indicator.

To make a reservation:

Click in the Reserved column of the desired reservation type and enter the desired reservation.

Reserved By Device Tab

The Reserved By Device tab, as shown in [Table 9-9](#), allows you to reserve resources for individual IP endpoints and IP trunks. All IP devices that are currently configured on the system are automatically displayed when you click the Resource Reservation Tool.

Figure 9-9. Reserved By Device Tab

Resource Reservations

Note: All IP devices, BVM ports, IP Networking, and Call Configurations should be configured prior to adjusting resource reservations. Use the fields in the 'Reserved' columns to adjust the resource reservations.

Reserved By Function | **Reserved By Device** | Advanced

Guidelines: It is recommended that you reserve resources for individual devices that cannot tolerate any delays in getting resources. Some common examples include attendants, call center agents, VIPs, etc.
Note that, in general, reserving resources is less efficient than sharing resources.

Extension	Description	Username	Type	Call Configuration	Reserved
1000			IP Endpoint	1	Yes <input checked="" type="checkbox"/>
1004			IP Endpoint	1	No
1005			IP Endpoint	1	No
1002			IP Single Line Adapter	1	No
1003			IP Softphone	1	No

Help | Default Reservations | Save | Save and Close | Close

The only configurable option in this screen is the Reserved column. The other options are just provided for reference and may be configured outside of this tool. If desired, click the column headings to sort the list by the entries in that column. To sort the list in reverse alphabetical order, click the column heading once more.

The Reserved column is the same as the Reserve IP Resource for Device flag (see [page 9-40](#)). If this flag is enabled, once the reserved device comes online, the system tries to allocate an IP resource for the device. The IP resource comes either from the shared IP resource pool or from the reservations made for the devices by vocoder type in the Advanced tab. If the allocation is successful, the device keeps the resource reserved for itself the whole time it is online, whether it is idle or in use. Note that reserving IP resources for a specific device guarantees only that the device can communicate with the Mitel 5000 system. It does **not** guarantee that a call can be completed, as would occur if no trunks were available.

NOTES

Mitel recommends that you reserve IP resources for attendants and other high-traffic users such as call center agents. However, excessive use of reservations degrades the effectiveness of oversubscription by reducing the amount of resources available to be shared.

One of the important uses of IP gateway trunks is to gain access to Emergency/ 911 services from remote locations. IP gateway trunks should have IP resources reserved for Emergency/911 access. For details, see [Table 9-9, "Reserved By Function Fields," on page 9-45](#).

To reserve or unreserve an IP resource for a particular device:

1. Click the row of the desired device and click the Reserved column. A check box appears.
2. Select **Yes** to reserve a resource for this device or select **No** to unreserve the resource.
3. Click **Save**.

Advanced Tab

Figure 9-10 shows an example of IP resource reservations that are not commonly used. Resources appearing on the Advanced tab include reservations by vocoder type for IP Endpoints, IP Trunks, or IP Networking and by Caller ID Transmitter or Receiver.

Figure 9-10. Resource Reservations Advanced Tab

Type	Reserved	Range	Configured	Reserved By Device	Shared
G.711 Endpoints	0	0 - 222	1	0	1
G.711 Trunks	0	0 - 222	0	0	0
G.711 IP Voice Mail	0	0 - 222	N/A	N/A	N/A
G.711 Networking	0	0 - 220	N/A	N/A	N/A
G.729 Endpoints	0	0 - 108	0	0	0
G.729 Trunks	0	0 - 108	0	0	0
G.729 IP Voice Mail	0	0 - 108	N/A	N/A	N/A
G.729 Networking	0	0 - 108	N/A	N/A	N/A

Each column of the Advanced tab identifies the following information about resource reservations:

- **Type:** Indicates the type of reservation. See Table 9-10, “Resource Types,” on [page 9-49](#).
- **Reserved:** Indicates the current reservations for each type.
- **Range:** Indicates the range of reservations that may be made for each type.

NOTE

The values for G.711 and G.729 resources in the Range column do not reflect the resources that are reserved in the Reserved By Device tab. For example, you have a system with 5 VoIP resources and 5 IP endpoints all running G.729. Although you reserved all of the resources for these devices in the Reserved By Device tab, the range for G.729 in the Advanced tab still shows 0–5. This indicates that you can still reserve up to 5 VoIPs, even though there are no resources available. DB Programming does not always know if the endpoint is on-line or not (that is, local mode). When enabling the “Reserved” flag for an IP device, the system allocates the necessary resource when the IP device goes on-line (using the same algorithm as if the IP device makes a call and does not use “reserved by device”). The system does not deallocate the resource until the IP device goes off-line.

- **Configured:** Indicates the number of each type currently configured on the system.
For example, for the G.711 Endpoints type, the Configured column shows the number of IP Endpoints currently configured on the system under a Call Configuration with G.711 as the speech encoding type.

IP Endpoints configured for a Call Configuration with a speech encoding of G.729 are totaled under the Configured column of the G.729 Endpoints. The same method is used to display the configured entries of the G.711 Trunks and G.729 Trunks reservation types.

The Configured column for Caller ID Transmitters shows **N/A** (Not Applicable) because Caller ID Transmitters cannot be configured on the system.

The Configured column for Networking also shows **N/A** because networking can be configured on the system in terms of nodes, but the volume of IP Networking calls cannot be configured on the system.

- **Reserved By Device:** Indicates how many devices from the Configured column have reservations currently associated with them, as indicated from the Reserved By Device tab.
For example, once all of the currently configured G.711 endpoints are determined, this column further investigates which of these devices has the Reserved column set to **Yes** in the Reserved By Device tab. This summary provides a quick reference as to how many IP devices already have reservations made for them.
- **Shared:** Indicates how many IP devices are sharing resources by oversubscription. The number displayed in this column equals the number of Configured devices of this type minus the number of resource reservations indicated in the Reserved column for the type. The number of shared IP devices equals the number of unreserved devices on the system.

Shared Resource Summary Bar: The Shared Resource Summary: bar displays the potential for Camp On. All of the IP devices sharing resources must compete for resources that have *not* been reserved. The potential for Camp On is determined by assuming all of the IP devices sharing resources are in use simultaneously. If the shared pool of resources cannot support the resource requests of all active IP devices, some of the devices camp on until more resources become available. The likelihood of any of these unreserved devices experiencing Camp On is shown in the Shared Resource Summary: bar.

Table 5-3 summarizes available resource types.

Table 9-10. Resource Types¹

Resource Type	Description	Guidelines	Default Value and Range ²
G.711 Endpoints G.711 Trunks G.711 Networking G.729 Endpoints G.729 Trunks G.729 Networking	Specifies how many G.711 and G.729 IP resources to reserve for IP Endpoints, IP Trunks, or IP Networking. G.711 is used for all locally connected IP endpoints (LAN), and G.729 is used for remotely connected IP endpoints (WAN or Internet).	Mitel recommends <i>not</i> reserving IP resources by device type and vocoder because it reduces the overall efficiency of oversubscription.	Default: 0 Range: 0–75 (Mitel CS-5200) 0–175 (Mitel CS-5400) 0–250 (Mitel CS-5600)
Caller ID Transmitter Caller ID Receiver	The system uses IP Resources to generate Caller ID information for single line endpoints. These resources are needed for a very brief time for each call, but Caller ID transmitting or receiving cannot tolerate Camp On delays. Lack of available resources causes Caller ID transmitting or receiving to fail.	Because Caller ID transmitting or receiving is very transient, Caller ID transmitters and receivers are ideal for oversubscription. Mitel recommends that you <i>not</i> reserve Caller ID transmitter and receiver resources.	Default: 0 Range: 0–75 (Mitel CS-5200) 0–175 (Mitel CS-5400) 0–250 (Mitel CS-5600)

Table 9-10. Resource Types¹ (Continued)

Resource Type	Description	Guidelines	Default Value and Range ²
G.711 IP Voice Mail	Specifies the allocation of Voice over Internet Protocols (VoIPs) in terms of calls to an IP voice mail. These resources are used for calls made to/from a SIP peer voice mail. Note that T.38 is currently not supported for the IP voice mail VoIP allocation.	You should rarely use VoIP reservations because the use of VoIP reservations defeats the sharing model of VoIPs. An example of using VoIP reservations would be an extreme case where the call traffic heavily uses VoIPs. Due to this call traffic, incoming calls to an IP voice mail (for example, NuPoint Messenger) must camp-on waiting for a VoIP. Configuring the IP Voice Mail reservation allows the voice mail system to take precedence in the allocation of VoIPs, thus inflicting the camp-on situations to the other IP devices.	Default: 0 Range: 0-75 (Mitel CS-5200) 0-175 (Mitel CS-5400) 0-222 (Mitel CS-5600)
G.729 IP Voice Mail			Default: 0 Range: 0-31 (Mitel CS-5200) 0-108 (Mitel CS-5400) 0-108 (Mitel CS-5600)

1. To sort the list by the entries in a column, click the column heading. To sort the list in reverse alphabetical order, click the column heading once more.
2. The upper limit of the range for each individual reservation can be further limited by the other reservations currently configured.

System Settings

Introduction	10-2
System-Wide Parameters	10-2
Setting the System Date	10-2
Setting the System Time	10-2
Selecting the System Time Zone	10-3
Programming Primary and Secondary Languages	10-3
Programming Daylight Saving Time [British Summer Time]	10-3
Echo Profiles	10-5
Programming Echo Profiles for Trunks	10-5
Programming Echo Profiles for Endpoints	10-6
Voice Over Internet Protocol (VoIP) Echo Canceller	10-8
File-Based Music-On-Hold (MOH)	10-9
Creating File-Based MOH Profiles	10-11
Using a File-Based MOH Source	10-13
Page Zones	10-15
Viewing Page Zones	10-15
Deleting Page Zones	10-15
Planning a Page Zone	10-16
Programming Local Page Zones	10-16
Creating Local Page Zones	10-16
Assigning Items to Local Page Zones	10-17
Creating Remote Page Zones	10-17
Deleting Page Zones	10-17
Deleting Items from a Page Zone	10-17
Creating Off-Node Page Ports	10-18
Deleting Off-Node Page Ports	10-18
System Flags	10-19
Timers and Limits	10-24
Feature Codes	10-33
Trunk Access Codes	10-33
Endpoint Feature Codes	10-34
SIP and ITP Default Feature Codes	10-39
Show IP Feature Code	10-39
SIP Mode Endpoint Feature Codes	10-39
ITP Mode Feature Codes	10-40
Administrator Feature Codes	10-41
Diagnostics Mode Feature Codes	10-42

Introduction

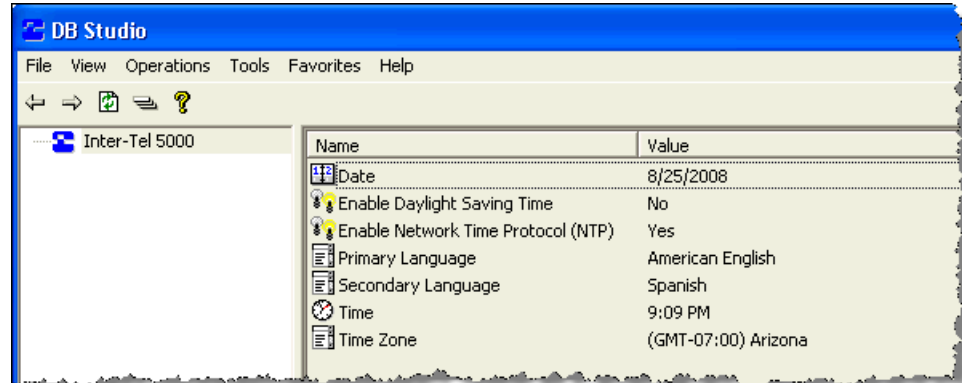
You can use the following features to customize your system settings:

- “System-Wide Parameters” below
- “Echo Profiles” on [page 10-5](#)
- “File-Based Music-On-Hold (MOH)” on [page 10-9](#)
- “Page Zones” on [page 10-15](#)
- “System Flags” on [page 10-19](#)
- “Timers and Limits” on [page 10-24](#)
- “Feature Codes” on [page 10-33](#)

System-Wide Parameters

You can program system-wide parameters, which include date, time, and language options, as shown in [Figure 10-1](#).

Figure 10-1. System-Wide Parameters



Setting the System Date

NOTE

If the Enable Network Time Protocol (NTP) option is enabled, the system date is controlled by the NTP server and the Date field is read-only.

To program the system date:

1. Select **Date**.
2. In the **Value** column, type the date or select the date from the calendar.
3. Click out of the field or press **ENTER** to save your change.

Setting the System Time

NOTE

If the Enable Network Time Protocol (NTP) option is enabled, the system time is controlled by the NTP server and the Time field is read-only.

To change the time:

1. Select **Time**.
2. In the **Value** column, type the time or select the time from the list.
3. Click out of the field or press **ENTER** to save your change.

Selecting the System Time Zone

You can select the time zone for your system.

To change the time zone:

1. Select **Time Zone**.
2. In the **Value** column, select the time zone from the list.
3. Click out of the field or press **ENTER** to save your change.

Programming Primary and Secondary Languages

The System provides a choice between American English, British English, Spanish, and Japanese prompts and displays. The system selects the language to use for each call, as determined by the trunk, endpoint, and voice processor programming.

NOTES

Japanese prompts can be viewed only on endpoints with an LCD display (excluding the Model 8690).

The Japanese language is not supported on Mitel 5000-series IP endpoints.

If you are using a Basic Voice Mail (BVM) or Enterprise® Messaging (EM) voice processing system, make sure that the appropriate prompts have been loaded into the voice processor. Otherwise, if users try to access the prompts, they hear the default American or British English prompts. For more information about loading voice processor prompts, refer to the Installation chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

To select the primary and secondary languages:

1. Select **Primary** (or **Secondary**) **Language**.
2. In the **Value** column, select the language from the list.
3. Click out of the field or press **ENTER** to save your change.

Programming Daylight Saving Time [British Summer Time]

NOTE

Do *not* schedule automatic functions, such as backups and resets, to occur at 2:00 AM [1:00 AM or 2:00 AM in Europe]. If you do, the system may not perform the function when the time changes.

This option determines whether the system automatically adjusts the time when daylight-saving time [British summer time] occurs. If enabled, standard time changes on the days specified. If disabled, the system does not recognize daylight-saving time [British summer time]. The default setting is off.

NOTICE

Station Message Detail Recording (SMDR) generates call costs based on the difference between the start and stop times of a call. System time changes *will* affect this calculation. If Daylight Saving Time is enabled for the system, and the time changes while SMDR is tracking a call, the call cost will be inaccurate. For example, if a call starts at 1:30 AM and ends at 2:30 AM on the night that Daylight Saving Time goes into effect, the call cost will be for 2 hours (1:30 to 3:30) instead of 1 hour (1:30 to 2:30).

To turn the Daylight Saving Time flag on:

1. Select **Enable Daylight Saving Time**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Click out of the field or press **ENTER** to save your change.

Echo Profiles

All system devices are associated with an echo profile. Besides voice mail and conferencing, echo profiles also apply to physical devices of the system, including:

- Endpoints/Connections
- Trunks
- Span Echo Profiles - Dual T1/E1/PRI Devices

You can program Echo Profiles for trunks (see the following section) or individual endpoints (see [page 7-67](#)).

Programming Echo Profiles for Trunks

The following are default Echo Profile options for trunks:

- No Echo (Disabled)
- Low Echo - no NLP (Low Aggressiveness, no Non-Linear Processing)
- Low Echo (Low Aggressiveness)
- Medium Echo (Medium Aggressiveness), and
- High Echo (High Aggressiveness).

Devices programmed for the system are automatically assigned a particular default configuration according to their type (see [page 10-7](#) for the default echo profiles for devices).

Table 10-1. *Trunk Echo Profiles*

Device Type	Default Echo Profile	Default Span Echo Profile - Dual T1/E1/PRI Devices
Loop Start Trunks (analog)	MEDIUM ECHO	N/A
IP Trunks (SIP, MGCP)	NO ECHO	N/A
Single T1/E1/PRI CO Trunks (Loop Starts, Ground Starts, DIDs, E&Ms, B-Channels on a port NOT programmed for private networking)	LOW ECHO	N/A
Single T1/E1/PRI B-Channel Trunks programmed on a port using private networking	MEDIUM ECHO	N/A
Dual T1/E1/PRI CO Trunks (Loop Starts, Ground Starts, DIDs, E&Ms, B-Channels on a port NOT programmed for private networking) ¹	NO ECHO	LOW ECHO
Dual T1/E1/PRI B-Channel Trunks programmed on a port using private networking	NO ECHO	MEDIUM ECHO
DID Trunk (on a DEM-16)	LOW ECHO	N/A
Basic Rate Trunk	LOW ECHO	N/A

1. A B-Channel trunk programmed for private networking is automatically moved into the correct echo profile by the system, so their echo profiles are read-only in DB Programming.

The following two fields set an echo profile for two main system functions:

- Voice Processor Echo Profile (the default is set to **No Echo**)
- Conferencing Echo Profile (the default is set to **Medium Echo**)

These fields apply their associated echo profile settings to any of their functions for the whole system.

To change the echo profile for a trunk:

1. Select System – Trunks – **Echo Profiles**.
2. In the **Value** column, right-click, and then select **Change Echo Profile**. A wizard appears allowing you to select any of the echo profiles for this field.

To move a particular device from one echo profile to another:

Do one of the following:

- Select the device from the current profile and drag/drop it onto the desired configuration in the tree view.
- Use the context menu option of the desired profile's folder to move the desired devices. To the right is an example of the move options of the Endpoints/Connections folder's context menu.

Programming Echo Profiles for Endpoints

The following devices are associated with an Echo Profile by default: all digital endpoints, single lines, IP Endpoints, IP Softphones, IPSLAs, Modems, IP Connections, and trunks. For more information about programming Echo Profiles for system trunks, see [page 10-5](#). Below is an example of the Echo Profile fields for an endpoint. For more information about echo profiles, refer to the “System Features” chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

Each echo profile has the following three subfolders:

- Endpoints/Connections
- Trunks
- Span Echo Profiles - Dual T1/E1/PRI Devices: Span echo profile has the following subfolders:
 - Endpoints
 - Trunks

The devices in the first two subfolders use their associated echo profile for echo generated by the Mitel 5000. The span-side devices cancel echo generated outside the system that comes in through one of the ports on the Dual T1/E1/PRI Module. Therefore, while all physical devices on the system have an echo profile, only devices programmed on a port of a Dual T1/E1/PRI Module have a span-side echo profile.

To add a device to the list:

1. Select System – Devices and Feature Codes – **Endpoints**.
2. Double-click **Echo Profiles**.
3. Double-click the echo profile type.
4. Right-click the right pane, and then select **Move To List**. A wizard appears allowing you to select any of the devices for this field.
5. Click **Next**.
6. Select the devices, and then click **Move Items**.
7. Click **Finish**.

To move a particular device from one echo profile to another:

Do one of the following:

- Select the device from the current profile and drag/drop it onto the desired configuration in the tree view.
- Use the context menu option of the desired profile's folder to move the desired devices.

The default echo profile for each device appears in [Table 10-2](#).

Table 10-2. Default Echo Profiles for Devices

DB Programming Field	Device Type	Default Echo Profile	Default Span Echo Profile - Dual T1/E1/PRI Devices
System\Devices and Feature Codes\Endpoints	Digital Endpoints	LOW ECHO	N/A
	IP Endpoints (IPSLA, IP Softphone, IP Endpoint)	NO ECHO	N/A
	Single Lines	LOW ECHO	N/A
	OPXs programmed on a single T1/E1/PRI Module	LOW ECHO	N/A
	OPXs programmed on a Dual T1/E1/PRI Module	NO ECHO	LOW ECHO
System\Devices and Feature Codes\IP Connections	IP Connections (IP Networking)	NO ECHO	N/A
System\Devices and Feature Codes\Modems	Modems	NO ECHO	N/A

For each device, the associated echo profile is displayed. Double-clicking on the echo profile field changes the view to the folder of that echo profile.

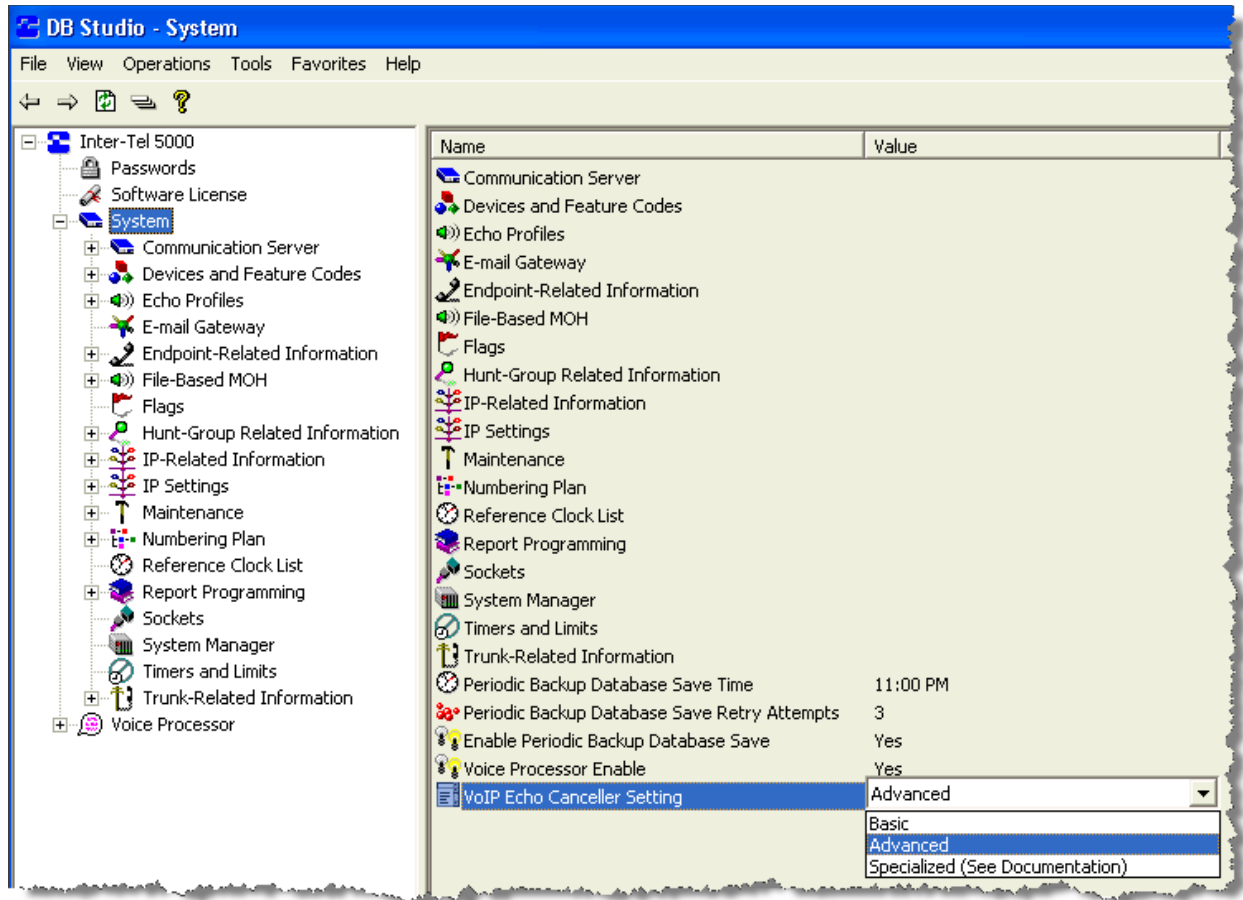
To change the echo profile for a device:

1. Right-click on the device and select **Change Echo Profile**. A wizard appears allowing you to select any of the echo profiles for this field.
2. Click **Next**.
3. Select the echo profile, and then click **Finish** to save the change.

Voice Over Internet Protocol (VoIP) Echo Cancellor

You can use the (improved) VoIP Echo Cancellor, as shown in [Figure 10-2](#), to select the system-wide echo cancellation settings based on the amount of echo that your system is experiencing. Systems upgrading to version 3.0 maintain the “Basic” level of echo cancellation. New system installs default to the “Advanced” level. For VoIP Echo Cancellor troubleshooting, see [page 17-87](#).

Figure 10-2. VoIP Echo Cancellor Setting



The following are VoIP Echo Cancellor settings:

- **Basic:** Provides less echo cancellation, but allows more concurrent IP calls. This is the default setting for Mitel 5000 systems that are *upgrading* to v3.0 and later.
- **Advanced:** Provides the best echo cancellation for most customers but allows fewer concurrent IP calls than the Basic setting. This is the default setting for *new* Mitel 5000 v3.0 installations.
- **Specialized:** *Do not use this option unless you are instructed to do so by Mitel Technical Support. This option is only for sites that are experiencing extreme amounts of echo.* Allows the fewest amount of concurrent IP calls.

To program the VoIP Echo Cancellor:

NOTE You must restart the system to activate VoIP Echo Cancellor changes.

1. Select System – **VoIP Echo Cancellor Setting**.
2. From the **Value** column, select one of the options previously described.
3. Click out of the field or press **ENTER** to save the change.

File-Based Music-On-Hold (MOH)

The File-Based Music-On-Hold (MOH) feature expands the existing MOH source beyond the built-in audio port located on the back of the Mitel 5000 chassis. You are no longer restricted to connecting to an external music source. This feature uses the compact flash-type memory card to store MOH audio files. This feature requires a software license (see “System Software Licenses” on [page 3-6](#)).

Although a device may connect to a music source for a length of time longer than the length in time of the audio file associated with the music source, the file-based music source continuously loops the audio playback so that there is always audio output from the source. A default audio file (it5k_default_moh.n64u) is provided on the Mitel 5000 compact flash-type memory card. You can use this as a sample file to associate a music source after you configure it in DB Programming, v3.0. The sample file plays this message:

“Mitel 5000 Network Communications Solutions enable organizations to blend their voice system into their data network, creating a cost-effective, efficient communications environment for small to medium businesses.”

This feature supports the non-proprietary G.711 (.n64u) file format. You can use the new MOH Converter Utility to convert audio files into the proper format (see “MOH Converter Utility” on [page 14-3](#).) The MOH Converter Utility uses the Sound eXchange (SoX) audio processing utility to convert the audio files to the desired format. When you install the MOH Converter Utility with DB Programming, a new folder called MOH Converter is installed in the same location. This folder contains various SoX text (.txt) and Portable Document Format (.pdf) files. Refer to the SoX .txt and .pdf files for additional information. You may also go to <http://sox.sourceforge.net> for more information. Supported audio file formats are listed in [Table 10-3](#).

Table 10-3. MOH Audio File Formats for Conversion

Audio File Format and Extension	
Apple (*.aif, *.aifc, *.aiff, *.aiffc)	Psion Record (*.prc)
Amiga 8SVX (*.8svx)	Psion (*.wve)
AU Format Sound (*.au, *.snd)	Sample Vision (*.smp)
Audio Visual Research (*.avr)	Sound Blaster (*.voc)
Compact Disc Digital Audio (*.cdda, *.cdr)	SoundTool (*.sndt)
CVSD Modulation (*.cvs, *.cvsd)	SPHERE (*.nist, *.sph)
IRCAM SDIF (*.ircam, *.sf)	VMS (*.dvms, *.vms)
MAUD File (*.maud)	Wave Sound (*.wav)
Maxis XA (*.xa)	Yamaha TX-16W Sampler (*.txw)

Table 10-4 lists other file formats that are used by the MOH Converter Utility. Some of these formats may need additional configuration to use (that is .gsm) or that only a subset of that file type works (that is .m3u, .hcom, .dat).

Table 10-4. *Other File Formats in the MOH Converter Utility*

Other File Formats and Extensions	
GSM File (*.gsm)	This file requires an external library.
M3U File (*.m3u)	This file is a playlist format, not an audio file format.
Macintosh HCOM (*.hcom)	These files may not convert properly. Convert the files to another common format, such as .aiff or .wav.
Text Data File (*.dat)	This file is a SoX-specific text-file representation of an audio file meant for importing into other analysis tools.

Use the MOH Converter Utility (see [page 14-3](#)) locally to convert the files to the proper format, and then upload the MOH files to the Mitel 5000 using Administrative Web Session (AWS). Refer to AWS Help for more information. After a file is converted to the .n64u format, you cannot run that file format through the converter again. The MOH files are stored on the compact flash-type memory card, but they are not included in the Database Save or Voice Processor Save. When you create your MOH files, make sure you save local copies of both the original music file as well as the converted file.

To program a File-Based MOH source:

1. Use the MOH Converter Utility locally to convert the files to the proper format. See [page 14-3](#).
2. Upload the MOH files to the Mitel 5000 using the Administrative Web Session (AWS). Refer to AWS Help for more information (System Management/MOH Files). The MOH files are stored on the compact flash-type memory card, but they are not included in the Database Save or Voice Processor Save. When you create your MOH files, make sure you create a backup of your local files.
3. Use DB Programming to select the audio file to use for MOH (see the applicable audio settings section). You can program a file-based MOH source wherever you are able to program the existing MOH port. Generally, you can program a file-based MOH source in the following fields in DB Programming (refer to the Mitel 5000 DB Programming Help for details):
 - Audio for Calls Camped onto this Device
 - Audio for Calls Ringing this Device
 - Audio for Calls Holding for this Device
 - Audio on Hold for Transfer Announcement
 - Music-On-Hold
 - Local Music Source

After a file-based MOH source is created and assigned a filename and when a VoIP resource is available, the audio begins to play immediately and continues until it is unequipped. The VoIP associated with the source is always in use by that MOH source. If the system is oversubscribed and a VoIP resource is not available, the MOH audio file camps on until a VoIP resource becomes available. Any device that attempts to listen to the MOH audio source hears silence. Each file-based MOH source consumes a VoIP resource and a software license, up to 5 audio files. If you unequip a file-based MOH source while a device is playing the file, silence is heard.

The MOH source licensing works differently than IP endpoint licensing, where an IP endpoint can obtain a license from a formerly equipped endpoint and a MOH source cannot. For example, you have 3 file-based MOH sources licensed and programmed, but then you upload a new license with only 2 MOH licenses. When you upload the new license, the system resets and only the first 2 MOH sources will come online. If you unequip one of the MOH sources with a license, the one without a license will not obtain the newly available license. You must reset the system to reallocate the licenses.

Creating File-Based MOH Profiles

“File-Based MOH” is the new value available in DB Programming wherever you can change the MOH value. Existing MOH values include Silence, Tick Tone, Ringback, Inter-Tel 5000, and Use Next Device’s Audio Source (for CO Trunk groups only). When you select “File-Based MOH” for the MOH value, you also must specify the MOH profile as the Extended Value. The Extended Value is the MOH profile that you set to specify which file-based source number to use. The Extended Value is created in the File-Based MOH folder in the System folder.

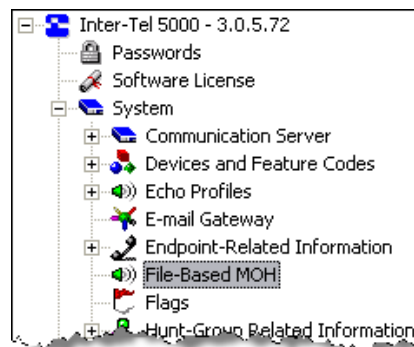
NOTE

The power of all signal energy other than live voice cannot exceed -9dBm when averaged over a 3 second interval. With our default loss plan, worst case, this means that the File-Based MOH file cannot exceed -12 dBm0 when averaged over a 3 second interval. If any gain on the system (for example, the transmit gain on a loop start trunk) is increased, this maximum level must be decreased by the same amount.

The File-Based MOH folder was added to the System folder to set MOH profiles for the system. By default, you can create up to five MOH profiles. If there is a MOH profile that is assigned to a file-based MOH source that no longer exists on the system, a warning message appears when you connect to DB Programming.

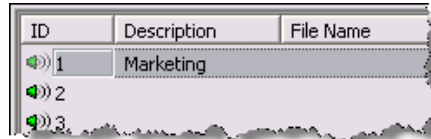
To create a MOH profile and assign a MOH source to the profile:

1. Select System – **File-Based MOH**.



2. Right-click anywhere in the right pane, and then select **Add to File-Based MOH List**. The Get ID dialog box appears.
3. Select the starting ID and the number of IDs to create. By default you can create up to five entries or the number of File-Based MOH licenses the system has.
4. Click **OK**. The items are added to the list with default values.

- Click the **Description** column to open an edit box, and then type a description. Click in another area of DB Programming to save your changes.



ID	Description	File Name
1	Marketing	
2		
3		

- Right-click in the File Name column, and then select **Assign File**. The Assign File-Based Music-On-Hold dialog box appears. This dialog box shows the existing MOH files that reside on the compact flash-type memory card.
- Select the audio file, and then click **Assign**. The MOH profile is configured.



ID	Description	File Name
1	MOH	Swb.n64u

To unassign a file-based MOH source from a profile:

Right-click the File Name, and then select **Unassign**.

To delete a MOH profile:

Right-click the File Name, and then select **Remove Selected Items**.

Using a File-Based MOH Source

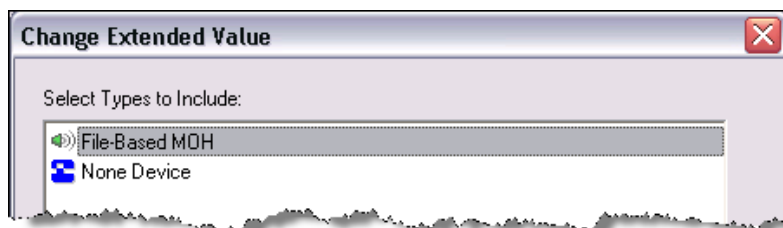
The option to choose the file-based MOH appears anywhere in DB Programming where a music source is currently programmable. The File-Based MOH source is included with the following existing music sources: Silence, Tick Tone, Ringback, Inter-Tel 5000, and Use Next Device's Audio Source (for CO Trunk Groups only). When you select File-Based MOH for the Value, you must also specify the MOH profile for the Extended Value. [Table 10-5](#) shows File-Based MOH options:

Table 10-5. File-Based MOH Option Fields

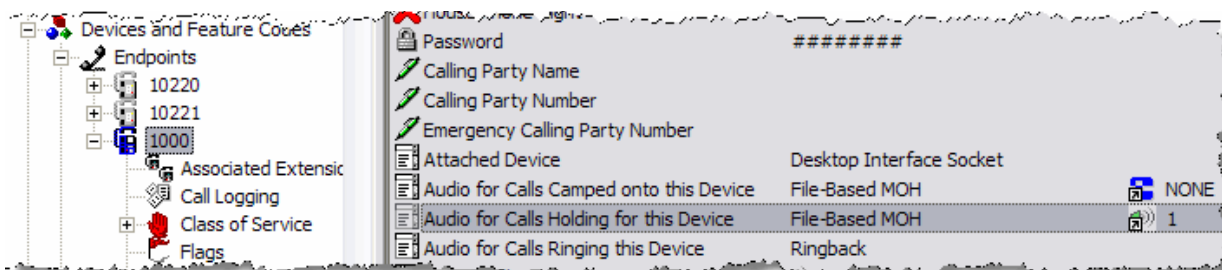
Field	Location
Audio for Calls Camped onto this Device	<ul style="list-style-type: none"> System\Devices and Feature Codes\Nodes\<node> System\Devices and Feature Codes\Hunt Groups\Local\<hunt group> System\Devices and Feature Codes\CO Trunk Groups\<CO trunk group> System\Devices and Feature Codes\Endpoints\Local\<endpoint> System\Devices and Feature Codes\Phantom Devices\Phantom Devices\<phantom device>.
Audio for Calls Ringing this Device	<ul style="list-style-type: none"> System\Devices and Feature Codes\Hunt Groups\Local\<hunt group> System\Devices and Feature Codes\Phantom Devices\<phantom device> System\Trunk-Related Information\Music-On-Hold Profiles
Audio for Calls Holding for this Device	<ul style="list-style-type: none"> System\Devices and Feature Codes\Endpoints\Local\<endpoint> System\Devices and Feature Codes\Phantom Devices\Phantom Devices\<phantom device> System\Trunk-Related Information\Music-On-Hold Profiles.
Audio on Transfer to Ring	<ul style="list-style-type: none"> System\Devices and Feature Codes\CO Trunk Groups\<CO trunk group>
Audio on Transfer to Hold	<ul style="list-style-type: none"> System\Devices and Feature Codes\CO Trunk Groups\<CO trunk group>
Audio on Hold for Transfer Announcement	<ul style="list-style-type: none"> System\Devices and Feature Codes\CO Trunk Groups and Node Trunk Groups. System\Trunk-Related Information\Music-On-Hold Profiles.
Music-On-Hold	<ul style="list-style-type: none"> System\Devices and Feature Codes\CO Trunk Groups\<CO trunk group>
Local Music Source	<ul style="list-style-type: none"> System\Devices and Feature Codes\Node IP Connection Groups\<IP connection group>\IP Call Configuration
Trunk Group Music-On-Hold	<ul style="list-style-type: none"> System\Devices and Feature Codes\CO Trunk Groups and Node Trunk Groups. System\Trunk-Related Information\Music-On-Hold Profiles.

To associate a MOH profile to a file-based MOH source:

1. Click the **Value** column for the specific music source field you are programming, and then select **File-Based MOH**.
2. Right-click the **Extended Value** column, and then select **Change Extended Value**. The following dialog box opens.



3. Select **File-Based MOH**, and then click **Next**.
4. Click the MOH profile, and then click **Finish**. The extended value is populated with the MOH profile number.

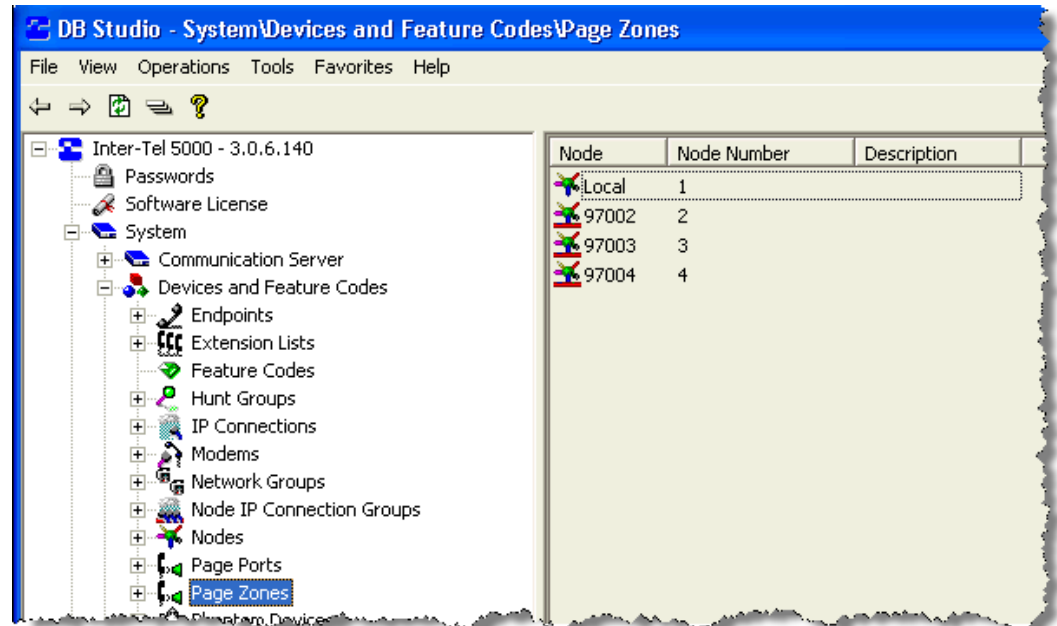


Page Zones

Page zones determine the devices that receive system pages. All endpoints and trunks within a page zone must reside on the same node as the page zone. However, a page zone can contain external *page ports* that are located on other nodes (see [page 10-18](#)), if they are programmed as off-node devices on the local node (see [page 7-13](#)).

[Figure 10-3](#) shows the DB Programming Page Zone location.

Figure 10-3. Local and Remote Page Zones



Viewing Page Zones

You can view page zones for local or remote nodes.

To view a page zone:

Select System – Devices and Feature Codes – Page Zones – **<node>**. Available page zone nodes appear in the right pane.

Deleting Page Zones

To delete a page zone:

Right-click the page zone, and then click **Delete**.

Planning a Page Zone

Page zone programming differs for Local Page Zones and Remote Node Page Zone. For more information, see “[Programming Local Page Zones](#)” below and “Creating Remote Page Zones” on [page 10-17](#).

NOTICE

Placing a large number of endpoints in a paging zone may affect system performance. If system operation is affected when a page is placed to a particular page zone, remove some endpoints from that zone or change to external paging for the area served by that page zone. A significant number of pages between IP endpoints also increases bandwidth usage and impact system performance.

To prepare for page zone programming:

Make a list of the endpoints, trunks, and/or the external paging port(s) included in local paging zones. Devices can be in more than one page zone. In the default state, all endpoints are assigned to page zone 1.

Programming Local Page Zones

Along with the page zone, program the endpoints, trunks, and page ports that are included in the page zone.

Creating Local Page Zones

To create a local page zone:

1. Select System – Devices and Feature Codes – Page Zones – **<node>**.
2. In the right pane, right-click on the node, and then click **Create Page Zone**. The Create Page Zone Extension dialog box appears.
3. Enter the starting extension number and the number of extensions.
4. Click **OK**. The page zone is added to the list.
5. Double-click the page zone extension number.
6. Enter the following information for the page zone:
 - **Number:** Type the page zone number that system users enter on their endpoints when placing pages.
 - **Description and Username:** Descriptions can have up to 20 characters; usernames can have up to 10 characters. Do not use slash (/), backslash (\), vertical slash (|), tilde (~), or Control characters.
7. Add the page zone items. Continue to “Assigning Items to Local Page Zones” on [page 10-17](#).

To change several page zone extension numbers at once:

1. Select the zones you want to change.
2. Right-click, and then select **Batch Extension Change**. The Get Extension screen appears.
3. Select the number you want to assign to the first selected zone (the other selected zones will be numbered consecutively after this number). You can use the SHIFT or CTRL keys to select more than one number.
4. Click **OK**. The page zones are automatically renumbered and re-sorted in the list.

Assigning Items to Local Page Zones

After creating the page zone, you must add the items that receive the paging messages. You must create Page Ports before you can add them to the Page Zone. See the following section, “Creating Off-Node Page Ports” on [page 10-18](#).

To assign endpoints, trunks, or paging ports:

1. Select System – Devices and Feature Codes – Page Zones – **<node>**.
2. Double-click the page zone that you want to program.
3. Double-click **IP/Digital Endpoints, Trunks, or Page Ports and Off-Node Page Zones** to add the devices to the page zone.
4. Right-click anywhere in the right pane. An option box appears.
5. Select **Add To List**. A window appears prompting for the device type to include.
6. Select the device types (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
7. Click **Add Items**, and then click **Finish**.

Creating Remote Page Zones

Off-node page zones allow paging access to paging zones located on other nodes. When you view remote node options, a list of its existing off-node page zones appears.

To create Off-Node Page Zones:

1. Select System – Devices and Feature Codes – Page Zones – **<node>**.
2. Right-click anywhere in the right pane, and then click **Create Off-Node Page Zone**. The Create Page Zone Off-Node dialog box appears.
3. Enter the starting extension number and the number of extensions.
4. Click **OK**. The page zone is added to the list.
5. Double-click the page zone extension number.
6. Enter the following information for the page zone:
 - **Number:** Type the page zone number that system users enter on their endpoints when placing pages.
 - **Description and Username:** Descriptions can have up to 20 characters; usernames can have up to 10 characters. Do not use slash (/), backslash (\), vertical slash (|), tilde (~), or Control characters.

Deleting Page Zones

To delete Off-Node Page Zones:

1. Select the page zone(s).
2. Right-click, and then select **Delete**. The page zone is automatically removed from the list.

Deleting Items from a Page Zone

To delete an item from one of the lists:

Select the list item(s), right-click and select **Remove Selected Items**.

Creating Off-Node Page Ports

You must add Off-Node Page Ports for each off-node page zone.

To create an off-node page port:

1. Select System – Devices and Feature Codes – Page Ports – *<remote node>*.
2. Right-click in the right pane, and then click **Create Off-Node Page Port**.
3. Enter the description and user name for the page port. Descriptions can have up to 20 characters; usernames can have up to 10 characters. Do not use slash (/), backslash (\), vertical slash (|), tilde (~), or Control characters.

Deleting Off-Node Page Ports

To delete Off-Node Page Ports:

1. Select the page port(s).
2. Right-click and select **Delete**. The page port is automatically removed from the list.

System Flags

This section describes system-wide flags. Endpoint flags are described on [page 7-22](#).

To program System Flags:

1. Select System – **Flags** to view a list of all system-wide flags.
2. Select the flag.
3. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box. Some flags require you to choose between two settings (such as 12- or 24-Hour Time Display Format). For those flags, select the current Value and use the scroll box to select the desired value.
4. Click out of the field or press **ENTER** to save your change.

[Table 10-6](#) shows system flags in the order they appear in DB Programming:

Table 10-6. *System Flags*

Flag	Description
Agent Help Display	Determines whether endpoint users will see the Agent Help displays during an Agent Help call. In the default state, this flag is set to Yes.
Agent Help Tone	Determines whether the parties on a call will hear a tone when a supervisor joins or monitors a call using the Agent Help feature. The frequency of the tones are determined by the Agent Help Tone Interval timer, described on page 10-30 . In the default state, this is set to Yes.
Allow Green LEDs	<i>Green LEDs to not apply to multi-protocol endpoints.</i> Gives the installer the option of having all red/green endpoints and red-only endpoints operate the same, or allowing the red/green endpoints to use the green LEDs. If this flag is enabled, the dual-color endpoints will use both the red and green LEDs. If it is disabled, the endpoints will operate in red-only mode, like the endpoints without green LEDs. In the default state, this is set to No. See also “Use Green LEDs for Direct Rings,” which follows in this list of flag descriptions.
Allow Immediate ACD Auto Connect After DND	Allows calls to autoconnect to the ACD agent endpoint immediately after the agent removes the endpoint from DND. If this flag is disabled, the first call received after DND is disabled rings until the agent answers the endpoint. By default, this flag is disabled
Alternate IP/Digital Endpoint Menu Display	Determines the display that Executive Display, Professional Display, and Model 8560 endpoint users see during an outside call. In the default state, the main menu display includes the TRANSFER-TO-HOLD option. If alternate displays are enabled, the FLASH option appears in its place. In the default state, this flag is set to No.
Audible Message Indication for SL Sets	If enabled, single line endpoints will receive message waiting indications (six tones before dial tone) when a message is waiting. In the default state, this is Yes.
Audio Diagnostics Alarm Suppression	Gives you the option of suppressing Alarm 128 (see “Alarms” on page 16-33), which is generated when the Audio Diagnostics feature (see page 16-19) is used. By default, this flag is set to No, which means that the alarm is generated and displayed on the administrator’s endpoint when a user access the Audio Diagnostics feature. If this flag is set to Yes, the alarm is suppressed

Table 10-6. System Flags (Continued)

Flag	Description
Automatic Board Equip	<p>If this flag is set to Yes, all modules inserted into unequipped bays are automatically detected and the bay is equipped to reflect the inserted module when the system is powered up and a new programming session is started. (All ports on inserted modules are unequipped.) This simplifies initial configuration, because all modules can be installed into the equipment chassis and they will appear in DB Programming automatically, reflecting the actual configuration of the system. In the default state, this flag is set to Yes.</p> <p>The Auto Board Detect feature can only function when a DB Programming session is not active.</p> <p>The Auto Board Detect function applies only to unequipped bays. Changes of bay type are not automatically detected and previous programming of modules and ports is left intact when module types are changed in previously used bays. Therefore, use local programming mode and delete any modules that exist in bays you want automatically detected before beginning the direct or remote programming session.</p>
Barge-In Notification Display	<p>Controls whether the agent sees the BARGE-IN PROGRESS or BARGE-IN TERMINATED display whenever a supervisor barges-in or hangs up after barging-in. The default setting is Yes. To turn on Barge-In Notification Display, set this flag to Yes. To turn off the Barge-In displays, set this flag to No.</p> <p>If the supervisor attempts to steal the other party away from the agent, the steal fails. The other party may be another endpoint or a trunk on a different node. The supervisor's endpoint displays VERSION MISMATCH STEAL REJECTED.</p>
Barge-In Notification Tone	<p>When this flag is turned on (set to Yes), each of the barged-in parties (not including the supervisor) can hear a tone on every barged-in call. The tone repeats at the frequency set by the Barge-In Notification Tone Frequency Timer (below). In the default state, this flag is set to No.</p>
Broadcast Alarms To All Administrators	<p>Determine whether system alarms will display on all administrator endpoints (set to "yes"). If not, they will display only at the primary attendant's endpoint (set to "no"). In the default state, this is set to Yes.</p>
Broadcast Station Off-Hook Alarms	<p>Determine whether off-hook alarms will be displayed on all administrator endpoints and the primary attendant's endpoint (set to "Yes"). In the default state, this is set to Yes.</p>
Companding Type	<p>Determine whether the system uses Mu-Law or A-Law companding.</p>
Date Display Format	<p>Determines the order the Day-Month-Year appear in the system. This includes SMDR Header, Keyset Date Programming, and Message Print. In the default state, it is set to Month-Day-Year.</p>
DISA Transfer Tone	<p>Select the ring or music option. If ring tones are enabled, callers will hear ringing instead of music when using DISA to call an endpoint. In the default state, this is set to Ring.</p>
Disable Confirmation Tone to Trunks	<p>Normally, a confirmation tone is played on a CO trunk call transferred to a Call Routing Announcement (CRA). This flag disables the confirmation tone for this type of transfer. It is set to No by default.</p>

Table 10-6. System Flags (Continued)

Flag	Description
Display Caller ID Name and Number	Adjusts the incoming CO call display to always show caller ID name and number on the LCD display instead of the call timer. For example, when a user is on a call, the user's endpoint displays a timer that counts the duration of the call. Setting this flag to Yes removes the timer and instead, shows the caller ID (name and number) of the caller. It is set to No by default.
Drop Incomplete Outgoing Calls	Occasionally, an endpoint user seizes a trunk at the exact time a call is coming in on that trunk and the user connects to the incoming call instead of dial tone. This phenomenon is called "glare." If the Drop Incomplete Outgoing Calls option is turned on (set to Yes), the resulting call on that trunk is dropped, as it would be if the user did not dial a valid number. If the option is turned off (set to No), the call remains connected regardless of the number of digits dialed, if any. In the default state, this flag is set to Yes.
Enable Shutdown On Low Battery	This flag allows the system to initiate a system shutdown if the UPS monitor detects a low battery event. It is set to Yes by default. For details about the UPS Monitoring feature, refer to the "System Features" chapter in the <i>Mitel 5000 Reference Manual</i> , part number 580.8007.
Handsfree Announce On System Forward Transfer	When an endpoint user transfers a call to the principal endpoint of a forwarding path, this option determines what the caller will hear. If turned on (set to yes), the caller will place a handsfree call to the principal endpoint and can announce the transfer (the call does not enter the forwarding path). If the option is disabled, the transferring endpoint user will hear ringing and can announce the call only if it is answered by the principal endpoint or one of the forwarding points. In the default state, this flag is set to No.
House Phone Mode	<i>This flag affects single line House Phones only. Other endpoint users can dial while on-hook and are not affected by this flag.</i> The flag determines whether a single line House Phone returns dial tone or does not return dial tone after the called party disconnects. At the System level of programming, all House Phones may be set in either Normal mode or Restricted mode. At the individual Endpoint level of programming, a House Phone must be programmed to dial specific digits as soon as the handset is taken off-hook. The programmed digits may ring a specific endpoint or a Hunt Group that rings multiple endpoints. Normal mode allows the user to enter a feature code or place a call after the automatically called number hangs up. Restricted mode prevents the user from performing any operation other than placing a House Phone call. The System default state is Normal.
Insufficient Bandwidth Alarm	Indicates whether the administrator endpoint displays a message when alarm 032 is generated. Alarm 032 is generated when the IP network does not have enough bandwidth to support the IP call that is currently connected to the device. If enabled (set to Yes), SYS ALARM #32 X<ext> INSUF BAND, where <ext> is the extension number of the affected device, displays on the administrator endpoint. If disabled (set to No), the endpoint does not display any information when the alarm is generated. In the default state, this flag is set to Yes.

Table 10-6. System Flags (Continued)

Flag	Description
Music On Hold For IC Calls	Determines whether a user hears music when placed on hold by another endpoint or when camped onto a resource. If set to No, IC callers never hear music, although they may hear other tones such as tick tone and ringback. In the default state, this flag is set to Yes.
OHVA Enable	Determines whether the Off-Hook Voice Announce (OHVA) feature will be enabled system-wide. In the default state, this flag is set to Yes. OHVA is not supported on IP endpoints.
Play Pre-Record-A-Call Display	Enables the Voice Processor to play a message before the Record-A-Call message. In the default state, this flag is set to No.
Receive Network Alarms	Determines whether the node will receive and display network-wide alarms sent by other nodes in the network. In the default state, it is set to No.
Record-A-Call Display	Determines whether endpoint users will see the Record-A-Call displays when the feature is used. In the default state, this flag is set to Yes.
Record-A-Call Tone	Determines whether the parties on a call will hear a tone when the Record-A-Call feature is in use. The timing of the tones are determined by the Record-A-Call Tone Interval timer, described on page 10-30 . In the default state, this is set to Yes.
Ring Flash On DSS Lamps	When turn on, this option allows Mini-DSS and DSS/BLF buttons to indicate a ringing call to an endpoint by showing the ring flash on the associated button. If turned off, the button will show that the endpoint is busy (solid lamp). In the default state, this flag is set to Yes.
Send Network Alarms	Determines whether a node will broadcast alarms that occur on that node to the rest of the network. In the default state, this flag is set to No.
Single Idle Time for All Hunt Groups	Invokes an Automatic Call Distribution (ACD) algorithm that sends an incoming call to the agent station with the longest idle time in all the hunt group queues to which that station belongs. For agent stations belonging to multiple HGs, this feature allows calls to be distributed to other stations having the longest idle time, regardless of the station idle time status in an individual hunt group. The default is set to No.
SLC Ring Zones	In some installations, where more than one single line device is connected in series to an SLM circuit, zoned ringing may be necessary. The system can support devices with 3 Ringer Equivalence (REN) units per circuit. However, the system can ring only eight RENs at once. Therefore, if there are more than eight RENs on any Single Line Module, the system-wide flag must be turned on to allow the single line devices to ring in smaller groups (zones). In the default state this flag is turned off.
SPCL Key Required For Feature Code Entry	Depending on the setting of this flag, users can either enter feature codes immediately after lifting the handset or while on hook, or they must press the SPCL button before entering the feature code. If this flag is turned on, endpoint users must always press the SPCL button before entering a feature code. In the default state, this flag is turned off (set to No).

Table 10-6. System Flags (Continued)

Flag	Description
System Speed Dial Override Toll Restriction	If this option is turned on, System Speed Dial numbers can be speed-dialed at any endpoint regardless of toll restrictions. If the flag is turned off, all System Speed Dial numbers are subject to toll restriction. In the default state, this flag is turned off (set to No).
Time Display Format	Determines whether endpoint displays will show the time in 24-hour or 12-hour (AM/PM) format. In the default state, it is set to <i>12 hour</i> .
UCD/ACD Station Monitor Indications	<p>Determines whether endpoint monitoring tones are sent to a UCD or ACD hunt group member when the hunt group supervisor is monitoring the call. In the default state, this flag is turned ON. The frequency of the tone is determined by the UCD/ACD Station Monitor Indication Frequency timer.</p> <div> <p>NOTICE</p> <p>Call monitoring may be illegal in some areas. The end user is ultimately responsible for ensuring that use of this feature is in compliance with applicable laws</p> </div>
Use Green LEDs for Direct Rings	Determines whether direct ring-in calls illuminate a red LED lamp or a green one. If the flag is turned on, direct ring-in calls to the endpoint illuminate a green LED. If turned off, all direct ring-in calls illuminate red. In the default state, this flag is turned on. The Allow Green LEDs flag must also be turned on for this feature to work
Validate Voice Mailbox Numbers	When this flag is enabled, the system checks that a dialed mailbox number matches a programmed extension number when the Record-A-Call or transfer-to-voice mail features are used. In the default state, this flag is set to Yes.
Wrap-Up Mode For Holding ACD Calls	If turned on, this flag prevents an agent from receiving additional ACD hunt group calls while a call the ACD agent placed on hold is holding and the agent's endpoint is idle. The endpoint can still receive non-ACD calls, as usual. If the flag is turned off, the agent will be available to receive additional ACD calls as soon as an ACD call is placed on hold. In the default state, this flag is turned off (set to No).

Timers and Limits

You can program the timers and limits that control various system functions. The default values have been carefully selected to ensure proper system operation under most circumstances. Occasionally, you may need to adjust one or more of the timers.

To change the value of a system timer:

1. Select its current Value and then type the new value in the text box.
2. Press **ENTER** or select another field to save the change.

The timer definitions are shown in [Table 5-30](#) and on the following pages. A “DID [DDI]” in the timer names indicates that the timer applies to DID [DDI] trunks only. “Digital/IP” refers to endpoints only and “SL” applies to single line endpoints only. “E&M” timers apply only to E&M trunks (except E&M Disconnect Flash Duration). “LS” indicates a loop start trunk timer, “GS” refers to ground start trunks, and “LS/GS” applies to both types. The “UCD” timer applies only to UCD hunt groups.

Table 10-7. System Timers

Timer	Default Value U.S. [Europe]	Range	Purpose
Abandoned Call	10	1–255 min	After a call has recalled to the last possible endpoint, it recalls until this timer expires. If it remains unanswered, the system disconnects the call. This timer starts when the call begins recalling the first recall endpoint.
Agent Help Tone Interval	0	0–1000 sec	The system can be programmed to send a tone to the call parties when a supervisor joins or monitors a call using the Agent Help feature. This timer determines how often the tone will be heard. If you set this timer to 0, there will be a single tone when the supervisor joins the call, if tones are enabled, but there will not be periodic tones through out the call.
Background Keypad Update Date and Time	360	60–360 min	Determines how often date and time displays are updated.
Barge-In Notification Tone Frequency Timer	0	0–255	Controls whether the agent sees the BARGE-IN PROGRESS or BARGE-IN TERMINATED display whenever a supervisor barges-in or hangs up after barging-in.
Camp-On	3	1–255 sec	Amount of time a caller hears busy tone before camping on.
Camp-On Tone	15	5–255 sec	Amount of time between Camp On tones.
CO Reseize	3	1–15 sec	When a user reseizes a trunk, this timer determines the length of time the system will hold the trunk open.
Dial Initiation	15	5–30 sec	Limits the amount of time an endpoint can remain off hook without dialing before the system sends reorder tones.
DID Disconnect Recognition	150	2–500 ms (.002–.5 sec)	The minimum amount of time the circuit must be on hook for the system to recognize that the call has been disconnected.
DID Inpulse-dial Inter-digit Pause Recognition	240	2–500 msec (.002–.5 sec)	The minimum pause allowed between in-coming pulse-dial signals sent from the remote circuit. It allows the system to recognize the separation between digits.

Table 10-7. System Timers (Continued)

Timer	Default Value U.S. [Europe]	Range	Purpose
DID Off-hook Debounce	10	2–500 msec (.002–.5 sec)	The minimum amount of time the circuit must be off hook before the system will recognize another on-hook/off-hook transition.
DID On-hook Debounce	12	2–500 msec (.002–.5 sec)	The minimum amount of time the circuit must be on hook before the system will recognize another on-hook/off-hook transition.
DID Post-Seize Delay	64	2–500 msec (.002–.5 sec)	The minimum time allowed between the recognition of a seizure and the beginning of digit validation. Used only for Immediate-Dial circuits.
DID Post-Signal Delay	30	2–500 msec (.002–.5 sec)	The minimum time allowed between the end of a handshake and the beginning of digit validation. Used only for Wink-Start and Dial-Delay circuits.
DID Pre-Signal Delay	100	2–500 msec (.002–.5 sec)	The amount of time that must elapse between the recognition of a trunk seizure and the handshake.
DID Ready Timeout	4000	2–65,000 msec (.002–65 sec)	Used only for Wink-Start and Dial-Delay circuits. This is the maximum time the T1 or T1/E1/PRI Module or SLA will wait for the “Digit Register Ready” command. If the timer expires, the SLA or module will automatically initiate a handshake. Used only for Wink-Start and Dial-Delay circuits.
DID Seizure Recognition	30	2–500 msec (.002–.5 sec)	The minimum amount of time the circuit must be on hook for the system to recognize that the trunk has been seized.
DID Signal Hold	200	2–500 msec (.002–.5 sec)	The maximum duration of a wink-start handshake or the minimum duration of a dial-delay handshake. Used only for Wink-Start and Dial-Delay circuits.
Digital/IP Alternate Transient Display Timer	10	1–255 tenths (.1–25.5 sec)	The amount of time transient displays appear on endpoints with the “Alternate Transient Display Timer” endpoint flag enabled.
Digital/IP Secondary Extension Key Altering Tone	6	1–1000 sec	This timer is in effect only if the endpoint has a number greater than 1 in the “Ring When <i>n</i> Calls At Extension” field. It determines how often the endpoint with the secondary extension button will hear an alerting tone while the primary endpoint has “ <i>n</i> ” number of calls present.
DISA Invalid Extension Failure Limit	3	0–9	Determines how many times a caller will be allowed to enter an incorrect DISA security code without being dropped. To program the failure limit, enter the desired number in the text box. Entering 0 allows unlimited attempts.
DISA Security Code Failure Limit	3	0–9	Determines how many times a DISA caller will be allowed to dial an invalid extension number before being sent to the primary attendant. To program the limit, enter the desired number in the text box. Entering 0 allows unlimited attempts.
Disconnect Wait After Dialing	20	1–60 sec	Length of time the system waits after dialing an outside number before checking the trunk for disconnect.

Table 10-7. System Timers (Continued)

Timer	Default Value U.S. [Europe]	Range	Purpose
DTMF Digit Duration/ Pause	60	30–255 msec (.03–.255 sec)	Adjusts the duration of and pause between digits of DTMF tones sent by the system. Both the tone and the pause will use the assigned duration (for example, a 6/100 second tone has a 6/100 second pause between digits). NOTE If using private IP networking, set this value to 100 msec or greater. If this value is less than 100 msec, the DTMF tones may not be detected.
E&M Answer Recognition	4500	2–20,000 msec (.002–20 sec)	(U.S. Only) Determines the minimum amount of time the receiving PBX must be off-hook, when an endpoint user places an outgoing call on an E&M trunk. This allows the system to recognize that the call has been answered.
E&M Dial Delay	70	2–500 msec (.002–.5 sec)	(U.S. Only) The maximum amount of time the E&M circuit will wait before transmitting digits following a handshake. This timer goes in effect after the handshake on a Wink-Start or Dial-Delay circuit or after seizure on an Immediate-Dial circuit.
E&M Dial Delay Hold	140	2–500 msec (.002–.5 sec)	(U.S. Only) The minimum length for a Dial-Delay handshake. Used only for Dial-Delay circuits.
E&M Dialing Wait After Hookflash	3000	2–20,000 millisecond. (.002–20 sec.)	(U.S. Only) Determines how long the E&M circuit will wait when transmitting a hookflash (recall) before dialing additional digits or checking for disconnection.
E&M Disconnect Flash Duration	15,000	2–40,000 msec (.002–40 sec)	(U.S. Only) The minimum amount of time a T1 E&M or DID circuit remains on-hook to cause a disconnection from the remote circuit.
E&M Disconnect Recognition	1500	2–10,000 msec (.002–10 sec)	(U.S. Only) The amount of time a circuit must be on-hook before the E&M circuit recognizes a disconnection.
E&M False Signal Debounce	50	2–500 msec (.002–.5 sec)	(U.S. Only) Determines the minimum length of a valid handshake signal received from a remote circuit. Used only on Wink-Start and Dial-Delay circuits.
E&M Handshake Timeout	5000	2–20,000 msec (.002–20 sec)	(U.S. Only) Determines the maximum length of a valid handshake signal. Used only on Wink-Start and Dial-Delay circuits.
E&M Hookflash Duration	600	2–10,000 msec (.002–10 sec)	(U.S. Only) Determines the length of hookflashes [recalls] sent to the remote circuits.
E&M Hookflash Recognition	300	2–10,000 msec (.002–10 sec)	(U.S. Only) Determines the minimum length of recognizable hookflashes [recalls] from the remote circuit.
E&M Inpulse-Dial Inter-digit Pause Recognition	300	2–10,000 msec	(U.S. Only) The minimum pause allowed between incoming pulse-dial signals sent from the remote circuit. It allows the system to recognize the separation between digits.

Table 10-7. System Timers (Continued)

Timer	Default Value U.S. [Europe]	Range	Purpose
E&M Off-Hook Debounce	10	2–500 msec (.002–.5 sec)	(U.S. Only) The minimum amount of time the remote circuit must be off hook before the E&M circuit recognizes another on-hook/off-hook transition.
E&M On-Hook Debounce	10	2–500 msec (.002–.5 sec)	(U.S. Only) The minimum amount of time the remote circuit must be on hook before the E&M circuit will recognize another off-hook/on-hook transition.
E&M Outpulse-Dial Inter-digit Pause	700	2–10,000 msec (.002–10 sec)	(U.S. Only) The minimum amount of time the E&M circuit will pause between pulse-dial digits when dialing.
E&M Outpulse-Dial Inter-pulse Pause	40	2–500 msec (.002–.5 sec)	(U.S. Only) The amount of time the E&M circuit pauses between pulse-dial digits when dialing.
E&M Post-Seize Delay	65	2–500 msec (.002–.5 sec)	(U.S. Only) The minimum allowed time between the recognition of a seizure and the beginning of digit validation. Used only for Immediate-Dial circuits.
E&M Post-Signal Delay	30	2–500 msec (.002–.5 sec)	(U.S. Only) The minimum allowed time between the end of a handshake and the beginning of digit validation. Used only for Wink-Start and Dial-Delay circuits.
E&M Pulse Hold	60	2–500 msec (.002–.5 sec)	(U.S. Only) This is the maximum length of a pulse-dial signal that is dialed by the E&M circuit.
E&M Ready Timeout	4000	2–20,000 msec (.002–20 sec)	(U.S. Only) On a Wink-Start circuit: The maximum time the E&M circuit waits for a “Digit Register Ready” command before initiating the Wink-Start handshake. On a Dial-Delay circuit: The maximum time the E&M circuit waits for a “Digit Register Ready” command before the Dial-Delay signal is terminated.
E&M Receive Handshake Delay	20	2–500 msec (.002–.5 sec)	(U.S. Only) The minimum time required, after seizure, before an incoming handshake signal can be recognized. Used only for Wink-Start and Dial-Delay circuits. If a Wink or Dial Delay signal is detected within this time, the outgoing call is blocked.
E&M Seizure Debounce	2	2–500 msec (.002–.5 sec)	(U.S. Only) Determines the minimum amount of time the remote circuit must remain off hook before the E&M circuit validates the incoming call.
E&M Transmit Handshake Delay	100	2–500 msec (.002–.5 sec)	(U.S. Only) The minimum delay time between the recognition of a seizure and the beginning of a handshake signal. Used only for Wink-Start and Dial-Delay circuits.
E&M Wait for Dial Tone	1000	2–20,000 msec (.002–20 sec)	(U.S. Only) The amount of time the E&M circuit waits for dial tone before dialing digits on an outgoing call. Used only on Immediate-Dial circuits with the Dial Tone Wait option enabled.
E&M Wink Hold	214	2–500 msec (.002–.5 sec)	(U.S. Only) Determines the duration of a Wink-Start handshake.

Table 10-7. System Timers (Continued)

Timer	Default Value U.S. [Europe]	Range	Purpose
E&M Wink Timeout	350	2–500 msec (.002–.5 sec)	(U.S. Only) Determines the maximum allowed duration of wink signals that are received from the remote circuit. If the time limit is exceeded, the call is blocked and the attempt terminated. Used only for Wink-Start circuits.
Forward No Answer	15	3–255 sec	Amount of time a call waits at an unavailable endpoint before being forwarded. Applies to manual call forwarding only, not system forwarding.
GS Dialing Wait After Connect	30	1–50 tenths (.1–5 sec)	(U.S. Only) The amount of time the system waits after a ground start trunk has been seized, to place an outgoing call, before dialing digits. This timer is not used if the Loop Current Dialtone Detection option is selected.
GS Tip-Ground Debounce	50	10–500 msec (.001–.5 sec)	(U.S. Only) The amount of time the system ignores subsequent attempts to seize a ground start trunk once it has been seized. The database contains an endpoint option that can be set to prevent users from reseizing a trunk. If selected, the endpoint user cannot reseize a trunk until it is disconnected by replacing the handset, pressing the SPKR button (if off-hook), or pressing another trunk button.
GS Transition Delay	10	10–500 msec (.001–.5 sec)	(U.S. Only) The amount of time that must elapse after a disconnection before another call can ring in on that trunk.
Hold	60	0–255 sec	Limits the time a call remains on hold before recalling the endpoint. If set to 0, the call will not recall.
Hold – Alternate	180	0–1000 sec	If the endpoint has the Alternate Hold Timer flag enabled, this limits time a call remains on hold before recalling the endpoint. If set to 0, the call will not recall.
Inactivity Alarm	60	10–255 sec	Limits the time an endpoint can remain off hook and inactive (after first receiving reorder tones) before registering a system alarm.
Interdigit – Long Interdigit – Short	15 4	2–255 sec 2–30 sec	Used in determining end of dialing. Short timer is used after a valid number has been dialed. Long timer is used until digits form a valid number.
Loopback Timeout	600	10–10,000 sec	The maximum allowed duration of a remote loopback test. If the timer expires, the test is automatically terminated.
LS Dialing Wait After Connect	15	1–50 tenths (.1–5.0 sec)	The amount of time the system waits for outside dial tone before dialing or checking the trunk for a disconnect.
LS/GS Caller ID Relay Hold	3747	2–4000 msec. (.002–4.0 sec)	The amount of time the system looks for Caller ID [CLID] information when a call is received.

Table 10-7. System Timers (Continued)

Timer	Default Value U.S. [Europe]	Range	Purpose
LS/GS Caller ID Ring Idle	128	128–1920 msec (.128–1.1920 sec)	This sets the time between the end of first ring and the time at which the system begins to check for Caller ID [CLID] information. The Caller ID [CLID] timer values combined must be shorter than the period of silence between rings from the CO [local branch].
LS/GS CO Hookflash	60	2–1000 hundredths (.02–10.0 sec)	Adjusts the duration of the timed hookflash (recall) that is sent over the trunk by the system when the Hookflash [Recall] feature code is used.
LS/GS CO-CO Disconnect	35	2–1000 hundredths (.02–10.0 sec)	A call is disconnected by the system if it detects loss of loop current lasting longer than this timer during trunk-to-trunk calls.
LS/GS Dialing Disconnect	120	2–1000 hundredths (.02–10.0 sec)	The connection is dropped if the system detects loss of loop current lasting longer than this timer during dialing.
LS/GS Dialing Wait After Hookflash	30	2–199 tenths (.2–19.9 sec)	Delays dialing after a hookflash [recall] to allow the system and central office hardware to recover.
LS/GS IC-CO Disconnect	60	2–1000 hundredths (.02–10.0 sec.)	During endpoint-to-trunk calls, the system disconnects a call when it detects loss of loop current lasting longer than this timer setting.
LS/GS Inter-ring Silence	60	1–250 tenths (.1–25.0 sec.)	Indicates the duration of the silence between rings on an incoming call to determine if the trunk has stopped ringing prior to being seized. In most areas, trunk ring pattern is 2 seconds on/ 4 seconds off. Check with the local service provider for the ring pattern in your area. NOTE This timer must always be set higher than the central offices ring off time.
LS/GS Loop Current Debounce	100	2–500 msec (.002–.5 sec)	The minimum amount of time the system must detect loop current for it to recognize that a trunk is present when it is seized.
LS/GS Outpulse-dial Inter-digit Pause	700	2–1500 msec (.002–1.5 sec)	The idle time between pulse-dial digits sent by the system.
LS/GS Outpulse-dial Inter-pulse Pause	40	2–500 msec (.002–.5 sec)	The amount of time between pulses when pulse-dial digits are sent by the system.
LS/GS Outpulse-dial Pulse Hold Duration	60	2–500 msec (.002–.5 sec)	The duration of a single pulse-dial digit sent by the system.
LS/GS Ring Frequency – High Boundary	100	1000 Hz maximum	These parameters determine the valid range of ring frequencies that will be recognized by the system.
LS/GS Ring Frequency – Low Boundary	15	4 Hz minimum	Any ring signal outside of this range is ignored. The ranges for the Ring Frequency timers are interdependent. The minimum value for the high boundary is the current Value of the low boundary. The maximum for the low boundary is the current Value for the high boundary.

Table 10-7. System Timers (Continued)

Timer	Default Value U.S. [Europe]	Range	Purpose
LS/GS Trunk Ring Detection	150 [150]	100–1024 msec (.1–2.5 sec)	A low-level timer that specifies the duration that continuous ring voltage must be detected on a trunk for the system to recognize a new incoming call. If this timer is too low, then false rings could be detected. If the timer is too high, then new incoming calls may not be detected at all. Common ring durations sent by central offices [local exchanges] are 1-second and 2-second.
Message Wait	5	1–255 sec	Amount of time a caller waits after pressing the MSG button before being connected to the called party's message center.
Off-Hook Voice Announce Screening	5	1–255 sec	After the Camp On timer expires, length of time before an OHVA call can be completed. OHVA is not functional on IP endpoints.
Page	15	0–255 sec	Limits duration of page. If set to 0, pages are unlimited in length.
Pause Dialing Digit Length	3	1–15 sec	Duration of timed pauses used in System and Station Speed Dial numbers and in ARS dial rules.
Queue Callback	15	10–255 sec	Time allowed for an endpoint to respond to a queue callback before the queue is canceled.
Recall	60	10–255 sec	Amount of time a Hold or Transfer recall rings at an endpoint before recalling that endpoint's recall destination. If the endpoint receiving the recall has no recall destination, the call remains at the endpoint until the Abandoned Call timer expires.
Record-A-Call Tone Interval	0	0–255 seconds	The system can be programmed to send periodic tones when the Record-A-Call feature is used. This timer determines how often the tone will be sent. If you set this timer to 0, there will be a single tone when the Record-A-Call feature begins, if tones are enabled, but there will not be periodic tones through out the call.
Remote Programming Invalid Extension Failure Limit	3	0–9 failures	Determines how many times a caller will be allowed to enter an incorrect extension number while attempting remote programming, without being dropped. To program the failure limit, enter the desired number in the text box. Entering 0 will allow unlimited attempts.
Remote Programming Password Failed Limit	3	0–9 failures	Determines how many times a caller is allowed to dial an invalid extension password while attempting remote programming, before being disconnected. To program the limit, enter the desired number in the text box. Entering 0 allows unlimited attempts.

Table 10-7. System Timers (Continued)

Timer	Default Value U.S. [Europe]	Range	Purpose
SL Disconnect Flash Duration	15	1–250 tenths (.1–25.0 sec)	When a single line endpoint is involved in a call that is dropped by the other party, and the single line endpoint remains off-hook, the system turns off tip and ring battery for the duration of this timer. If peripheral equipment is connected to the single line circuit (such as a voice mail unit, page amplifier, or other system) then this loss of battery signals a call disconnect and usually causes the equipment to disconnect.
SL Hookflash Maximum	12 [15]	2–20 tenths (.2–2.0 sec)	The maximum amount of time a single line endpoint user can press the hookswitch before the system disconnects calls.
SL Hookflash Minimum	2 [7]	1–10 tenths (.1–1.0 sec)	The minimum length of time a single line endpoint user must press the hookswitch for the system to recognize a hookflash [recall].
SL Inpulse-dial Inter-digit Pause	300	2–1500 msec (.002–1.5 sec)	The minimum pause allowed between incoming pulse-dial signals sent from the remote circuit. It allows the single line device to recognize the separation between digits.
SL Wait For Disconnect	2	1–60 seconds	When a single line endpoint is involved in a call that is disconnected by the other party, and the single line endpoint remains off hook, this timer specifies the length of time between the disconnection and when the disconnect flash (which is set by the Disconnect Flash Duration timer) is transmitted to the single line circuit. During this time, the endpoint receives no audible signal.
System Forward Advance	15	2–255 seconds	Determines how long a call will ring (unanswered) at each forwarding point in a system forwarding path.
System Forward Initiate	15	2–255 seconds	Determines how long a call will ring (unanswered) at the principal endpoint before advancing to the first forwarding point in a system forwarding path.
Transfer – Attendant	30	10–255 seconds	When an attendant transfers a call, this timer limits the time a transferred call rings unanswered before it recalls the attendant.
Transfer – Available	20	10–255 seconds	Limits time a transferred call rings unanswered before it recalls the transferring endpoint. (Does not apply to calls transferred by attendant endpoints or the Voice Processor or calls transferred to a busy endpoint.)
Transfer – Busy	24	10–255 seconds	Limits time a transferred call waits at a busy endpoint before recalling the transferring endpoint. Does not apply to calls transferred by attendant endpoints or Voice Processor or to calls transferred to an idle endpoint.
Transfer – Voice Processor	20	10–255 seconds	Limits time a transferred call waits at a Voice Processor destination before recalling the programmed recall destination.

Table 10-7. System Timers (Continued)

Timer	Default Value U.S. [Europe]	Range	Purpose
Trunk Key Debounce	3	1–30 seconds	<p>The amount of time the system ignores subsequent attempts to press a trunk button once it has been pressed. This timer prevents a user from accidentally disconnecting a call by reselecting the trunk button if the button is pressed twice while answering a call.</p> <div> NOTE <p>The database contains a CO/IC Reseize endpoint flag that can be set to prevent users from reseizing a trunk. If selected, the endpoint user cannot reseize a trunk until it is disconnected by replacing the handset, pressing the SPKR button, or pressing another trunk button.</p> </div>
UCD/ACD Station-Monitor Indication Frequency	15	1–255 seconds	The duration of the pause between hunt group endpoint monitoring tones.
Unsupervised CO	5	1–255 minutes	Limits duration of outside calls transferred or forwarded to outside numbers before recalling the primary attendant.
Valid Call	15	1–60 seconds	Minimum duration of an outgoing call before it is recorded in SMDR. Calls placed on hold or transferred are not subject to this timer.
Voice Mail Dial Delay	5	1–250 tenths (.1–2.5 sec)	(Used for Analog Voice Mail Hunt Groups Only) When a call is answered by the voice mail unit, this indicates the amount of time the system waits before sending digits to the voice mail unit after it answers the call.

Feature Codes

System feature codes are preset to carefully selected default values. Changing the codes can erase existing assignments. For example, if 300, 305, and 306 are assigned as feature codes and you attempt to assign 30 as another feature code, you would receive a warning message, because 30 makes up part of existing codes. The warning message allows you to change the existing numbers (300, 305, and 306) individually or to leave the existing numbers unchanged by selecting Cancel.

Feature code tables begin on [page 10-33](#).

Remember the following when changing feature codes:

- If you change feature codes, they are not automatically updated in the feature code directory used by Desktop Interfaces (system devices). You must manually update the directory. However, any devices installed after the change will have the new feature code information.
- Desktop Interface functionality requires the Desktop Interface software license.

To change a feature code number:

1. Select System – Devices and Feature Codes – **Feature Codes**.
2. Select the current Feature Code.
3. Select or enter the new code in the box. Feature code descriptions cannot be changed.

To change several feature code numbers at the same time:

1. Select System – Devices and Feature Codes – **Feature Codes**.
2. Select the codes you want to change.
3. Right-click and select **Batch Extension Change**.
4. When the Get Extension screen appears, select the number you want to assign to the first selected feature code. The other selected codes will be numbered consecutively after this number.
5. Click **OK**. The feature codes are automatically renumbered and resorted in the list. To select a series of items, hold down SHIFT while selecting the first and last item in the range. To select two or more items that are not consecutive, hold down CTRL while selecting the desired items. You may need to continue to hold SHIFT or CTRL while right-clicking to display the option without changing the selected items.

Trunk Access Codes

[Table 10-8](#) lists trunk access codes used to select trunks when placing outgoing calls.

Table 10-8. *Trunk Access Codes*

Feature Name	Code U.S. (Eur.)	Definition
Automatic Route Selection (ARS)	92000	Allows the system to select the route wanted for placing a call, as programmed in the database.
Trunk Group Access 1–208	92001–92208	Selects an available trunk from a programmed group of trunks for placing an outside call.
Emergency Call	911 (999/112 or as applicable)	Entering this feature code selects an outgoing trunk and automatically dials the programmed Emergency Call number, which is routed by default out Trunk Group 1.
Outgoing Call	8	Selects an outgoing trunk according to the programmed outgoing access mode for that endpoint..

Endpoint Feature Codes

Table 10-9 lists the default endpoint system feature codes.

Table 10-9. *Endpoint Feature Codes*

Feature Name	Code	Definition
Account Code – All Calls Following	391	Allows the endpoint user to enter a forced or optional account code that will apply to all calls following the entry of this feature code and will appear in the SMDR. To disable the All Calls Following feature, the feature code is entered again without an account code.
Account Code – Optional	390	Allows the endpoint user to enter an optional account code for SMDR reports during an outside call.
ACD Agent Login ACD Agent Logout ACD Agent Login/Logout Toggle	326 327 328	These feature codes allow an ACD hunt group member (agent) to log into and out of the ACD hunt group(s). The agent will only receive calls through the ACD hunt group(s) while logged in.
ACD Agent Wrap-Up Terminate	329	When an ACD agent completes a call, no other ACD hunt group call will ring at the endpoint until the ACD Wrap-Up Timer expires or the agent enters this feature code to terminate the wrap-up session.
Agent Help	375	The Agent Help feature allows an endpoint user to request help from a designated “Agent Help Extension” during a two- or three-party call.
Agent Help Reject	376	When a request-for-help call rings, the Agent Help Extension can choose to join the call or enter this feature code to reject the request.
Answer (Ringing Call)	351	Answers the call that has been ringing or holding the longest at that endpoint.
Audio Diagnostics	320	When initiated, users are prompted to answer questions about the audio problems by pressing specific keypad buttons.
Automatic CO Access On/Off	360	<i>(Not used on single line endpoints)</i> Allows the endpoint user to determine how ringing outside calls will be answered: simply by lifting the handset or pressing the Speaker button (automatic answer), or by lifting the handset or pressing the Speaker button and pressing a Call button, individual trunk button or the ANSWER button.
Automatic IC Access On/Off	361	<i>(Not used on single line endpoints)</i> Allows the endpoint user to determine how ringing intercom calls will be answered: simply by lifting the handset (automatic answer), or by lifting the handset and pressing the IC button (or a Call button, if there is no IC button).
Automatic Trunk Answer	350	Using this feature code, endpoint users with allowed answer can pick up trunks that are ringing into the system, but that are not actually ringing at their endpoints. This feature does not pick up transferred calls or recalls that are ringing at the endpoint.
Background Music On/Off	313	<i>(Not used on single line endpoints)</i> Turns on and off background music heard through the endpoint speaker.
Barge-In	386	Allows the supervisor to barge-in on a call to help the hunt group member/agent.
Call Forward All Calls	355	Immediately forwards all calls to another endpoint or to an outside endpoint number.

Table 10-9. Endpoint Feature Codes (Continued)

Feature Name	Code	Definition
Call Forward If Busy	357	Immediately forwards all calls to another endpoint or to an outside endpoint number when the endpoint is in use.
Call Forward If No Answer	356	Forwards all calls to another endpoint or to an outside endpoint number if not answered within a predetermined time.
Call Forward If No Answer/Busy	358	Forwards all calls to another endpoint or to an outside endpoint number if not answered within a predetermined amount of time, or immediately if the endpoint is in use.
Call Logging	333	Allows users of display endpoints to view missed, received, and dialed calls.
Change Language	301	An endpoint user can change the assigned language for the endpoint by entering the Change Language feature code while the endpoint is idle.
CO Hookflash	330	Sends a timed hookflash over the trunk while on an outside call (includes conference calls).
Conference	5	Connects from three to four parties in a conference. A conference consists of any combination of inside and outside parties.
Data	340	Allows operation of a data device attached to a digital endpoint. Requires a modem-equipped data device. Supported on Mitel 5000 systems equipped with appropriate digital interface equipment.
Default Endpoint	394	This single feature code cancels account codes for all calls following, Do-Not-Disturb, manual call forwarding, background music, ring intercom always, and queue requests; restores handsfree mode, pages, hunt group calls, and system forwarding; and returns endpoint volumes to default values.
Directory	307	<i>(Display endpoints Only)</i> Allows display endpoint users to search for extension numbers or System Speed Dial numbers. The number can then be dialed, if appropriate.
Display Outside Party Name On/Off	379	<i>(Display endpoints Only)</i> When the endpoint user enters this feature code, while connected to a CO call that has outside party name information, the display will toggle between the caller's name and number. If there is no outside party name or the Expanded CO Call Information On Displays flag is disabled, the user will hear a burst of reorder tone and see the CANNOT ACCESS FEATURE display. If the Display Outside Party Name On/Off feature code is programmed in a user programmable button with a lamp, the lamp will be lit when the outside party name is enabled and off when the outside party number is enabled.
Display Time/Date (ITP) Show IP (SIP)	300	<i>(Display endpoints Only)</i> Temporarily displays the system date and time, user name, and extension number during a call or when other displays are shown. Feature code 300 displays the IP Address of an endpoint if it is in SIP mode.
Do-Not-Disturb Do-Not-Disturb Cancel Do-Not-Disturb On/Off	370 371 372	The Do-Not-Disturb feature code halts all intercom calls, transferred calls, and pages to the endpoint. The Cancel code returns the endpoint to normal operation. The on/off code can be used to turn Do-Not-Disturb on or off.

Table 10-9. Endpoint Feature Codes (Continued)

Feature Name	Code	Definition
Do-Not-Disturb Override	373	<i>(Not used on single line endpoints)</i> If enabled in the database, allows the endpoint user to break through another endpoint's Do-Not-Disturb mode when placing an intercom call.
Enhanced Speakerphone Enable	310	<i>(Digital endpoints only)</i> When entered at a digital endpoint, this feature code enables the enhanced speakerphone as described in "Display and Nondisplay Digital Endpoints" on page 4-98 . Digital endpoints can also use the Special button + Speaker buttons.
Feature Key Default	395	<i>(Not used on single line endpoints)</i> Endpoints have user-programmable feature buttons that can be set to enter feature codes. This code returns the user-programmable buttons to the database default values.
Group Listen	312	<i>(Not used on single line endpoints)</i> Allows a user to transmit a conversation over the endpoint speaker while in handset or headset mode.
Handsfree On/Off	319	<i>(Not used on single line endpoints)</i> Disables/enables the endpoint's handsfree intercom answering. Incoming intercom calls ring as private calls if handsfree answering is disabled.
Headset Enable Headset Disable Headset On/Off	315 316 317	<i>(Not used on single line endpoints)</i> The enable code signals the system that a headset has been connected to the endpoint. The disable code returns the endpoint to normal operation. The on/off feature code can be used to toggle the feature on or off.
Hold – Individual	336	Places a call on hold so that it can be picked up directly at that endpoint or through a reverse transfer from any other endpoint.
Hold – System	335	Places an outside call on system hold. It can be picked up directly at any endpoint that has an individual trunk button and has allowed-answer and/or outgoing access for that trunk, or by the endpoint that placed it on hold. (If used on conference or intercom calls, the system places the call on individual hold.)
Hunt Group Remove Hunt Group Replace Hunt Group Remove/Replace	322 323 324	Removes the endpoint from its assigned hunt group(s) or places it in again. Does not affect non-hunt group calls. The remove/replace feature code can be used to toggle the feature.
LCD Contrast Adjustment	303	Adjusts the LCD contrast on the display. The endpoint must be idle to use this feature.
Message	365	This feature code is used for leaving and retrieving a message waiting indication at a called endpoint or the called endpoint's message center. Depending on how the message was left, the called endpoint user either retrieves the message from his/her message center or from the endpoint that left the message.
Message – Cancel	366	Allows the endpoint user to cancel a message waiting indication that he or she left at another endpoint.
Message – Cancel Current	368	Cancels a message waiting indication that is waiting at the endpoint without requiring the user to respond to it. (Or, press the asterisk [*] button while viewing the message.)
Message – Silent	367	Leaves a Message Waiting indication at an endpoint without first placing an intercom call.
Mute On/Off	314	<i>(Not used on single line endpoints)</i> Turns the microphone on or off during a call. If muted, the endpoint user can hear the other party, but the party cannot hear the endpoint user.

Table 10-9. Endpoint Feature Codes (Continued)

Feature Name	Code	Definition
Page	7	When followed by a paging zone code (0–9 or 0–49), it allows announcements to be made through endpoint speakers and any external paging speakers in the page zone.
Page On/Off	325	<i>(Not used on single line endpoints)</i> Halts pages through the endpoint speaker or allows them to be received again.
Program Bit Rate	393	<i>Reserved for controlled introduction.</i> This allows a digital endpoint user to change the bit per second (bps) rate of an attached PCDDPM serial port.
Program Buttons	397	<i>(Not used on single line endpoints)</i> User-programmable feature buttons and Station Speed Dial buttons can be programmed using this feature code.
Program Endpoint Password	392	The endpoint password is used for the Remote Programming feature. The password can be changed by entering the Program Endpoint Password feature code at the endpoint or when using the Remote Programming feature.
Queue Request	6	Requests (or cancels) an automatic callback when a busy trunk or endpoint becomes available.
Record-A-Call	385	If the system is programmed with a Record-A-Call application, the endpoints can be programmed to use the Record-A-Call feature. It allows users to enter a feature code whenever they want to record an ongoing call in their designated Record-A-Call mailbox. Users can retrieve the recorded messages later, just as they would any other mailbox messages.
Redial	380	Redials the last outside phone number dialed or saved at the endpoint (up to 48 digits). Also used to save numbers at endpoints programmed for last number saved. (Inter-Tel endpoints use the REDIAL button.)
Redirect Call	331	Allows the endpoint user to route ringing outside, intercom, and camped on calls to another endpoint, hunt group, or outside number. Routing of the redirected call is still subject to trunk and toll restrictions. This feature provides these options in addition to the currently available options which allow the endpoint user to redirect calls to Voice Mail or Do-Not-Disturb. The Redirect Ringing Call feature does not require a software license.
Reminder Message Reminder Message Cancel	305 306	<i>(Not used on single line endpoints)</i> The endpoint user can set reminder messages that signal the endpoint at specific times. Or, the user can cancel all reminder messages for the endpoint.
Remote Configuration – Disable	343	<i>Reserved for controlled introduction.</i> Disables the Remote Configuration feature. The VPN connection from the Remote Proxy Server to the Mitel 5000 system is terminated.
Remote Configuration – Display HW Serial Number	347	<i>Reserved for controlled introduction.</i> Displays the hardware serial number for the Mitel 5000 system.
Remote Configuration – Enable	342	<i>Reserved for controlled introduction.</i> Enables a Remote Configuration session. The Virtual Private Network (VPN) connection from the Mitel 5000 system to the Remote Proxy Server is initiated.
Remote Configuration – Reset	344	<i>Reserved for controlled introduction.</i> Resets a Remote Configuration session. The VPN connection from the Mitel 5000 system to the Remote Proxy Server is reset.

Table 10-9. Endpoint Feature Codes (Continued)

Feature Name	Code	Definition
Remote Programming	359	Allows a user to place an endpoint in DND mode, forward the endpoint's calls, or change the password; either from another endpoint or through DISA.
Reverse Transfer (Call Pick-Up)	4	Picks up a call ringing or holding at an endpoint or hunt group
Review Keys	396	<i>(Not used on single line endpoints)</i> User-programmable feature buttons and Station Speed Dial buttons can be viewed using this feature code.
Ring Intercom Always On/Off	377	Enables/disables the feature that allows the endpoint to always place private (non-handsfree) intercom calls.
Ring Tone Selection	398	<i>(Not used on single line endpoints)</i> Selects the type of ringing alert tone that will be heard from the endpoint.
Routing Off	304	Disables System OAI Offering Control for third-party applications. This feature requires you to enter a password. Once you disable routing, you cannot enable it again (i.e., only the third-party application can enable routing).
Station Monitor	321	<i>(Hunt Group supervisors only)</i> Allows a designated hunt group supervisor to monitor a call of anyone in the associated hunt group.
Station Speed Dial Station Speed Dial Programming	382 383	Dials/programs one of the 10 Station Speed Dial numbers when followed by a location code (0–9). Inter-Tel endpoints use the Station Speed Dial button plus a location code for programming and dialing, or they can program Speed Dial buttons for one-button dialing.
Steal	387	Allows the supervisor to take away a call from the hunt group member/agent.
Switch Keymap	399	<i>(Not used on single line endpoints)</i> Allows an endpoint user to switch between standard and alternate keymaps.
System Forward Enable System Forward Disable System Forward On/Off	352 353 354	Enables or disables the database-programmed System Forwarding feature for this endpoint. The on/off feature code can be used to toggle the feature on or off.
System Speed Dial	381	Dials one of the 1000 System Speed Dial phone numbers when followed by a location code (000–999). Also used for reviewing System Speed Dial numbers.
Transfer to Hold	346	Transfers a call to another endpoint and places it on individual hold so that it does not ring or send call waiting signals until it recalls.
Transfer to Ring	345	Transfers a call to another endpoint or to an outside phone number.

SIP and ITP Default Feature Codes

The following tables show default feature codes for SIP and ITP Mode endpoints. For more information about these features, refer to the applicable endpoint user guide.

Show IP Feature Code

The Show IP feature code displays different information in SIP and ITP modes.

Table 10-10. *SIP and ITP Mode Functions for Show IP Feature*

Feature	Default Code	SIP Mode	ITP Mode
Show IP (or Display Time/Date)	300	Displays the IP address of the endpoint.	Displays the system date and time, extension number, and status for IP and digital endpoints. The IP address is <i>not</i> displayed in IP mode.

SIP Mode Endpoint Feature Codes

Table 10-11 shows default feature codes when operating in SIP mode.

Table 10-11. *SIP Default Feature Codes*

Feature	Code	Feature	Code
Answer (Ringing Call)	351	Hold – Individual	336
Call Forward All Calls	355	LCD Contrast	303
Conference	5	Message	365
Do-Not-Disturb	370	Microphone Mute On/Off	314
Do-Not-Disturb Cancel	371	Redial	380
Do-Not-Disturb On/Off	372	Redirect Call	331
Group Listen	312	Reverse Transfer (Call Pick-Up)	4
Headset On	315	Ring Tone Selection	398
Headset Off	316	Transfer To Ring	345
Headset On/Off	317		

ITP Mode Feature Codes

Table 10-12 shows default feature codes for Inter-Tel ITP mode endpoints.

Table 10-12. *Inter-Tel Protocol IP Default Feature Codes*

Feature	Code	Feature	Code
Account Code – Following Calls	391	Hunt Group Remove	322
Account Code – Optional	390	Hunt Group Replace	323
ACD Agent Log In	326	Hunt Group Remove/Replace	324
ACD Agent Log Out	327	LCD Contrast Control	303
ACD Agent Log In/Out	328	Message	365
ACD Agent Wrap-Up Terminate	329	Message – Cancel Message Left	366
Agent Help Request	375	Message – Cancel Message on Phone	368
Agent Help Reject	376	Message – Silent Message	367
Answer (Ringing Call)	351	Microphone Mute On/Off	314
Automatic Intercom Access On/Off	361	Page	7
Automatic Line Access On/Off	360	Page Receive On/Off	325
Automatic Line Answer	350	Program Buttons	397
Background Music On/Off	313	Program Station Password	392
Call Forward All Calls	355	Queue (Callback) Request	6
Call Forward If Busy	357	Record-A-Call	385
Call Forward If No Answer	356	Redial	380
Call Forward No Answer/Busy	358	Redirect Call	331
Conference	5	Reminder Message	305
Default Station	394	Reminder Message Cancel	306
Directory	307	Remote Programming	359
Display Time And Date	300	Reverse Transfer (Call Pick-Up)	4
Do-Not-Disturb	370	Review Buttons	396
Do-Not-Disturb Cancel	371	Ring Intercom Always On/Off	377
Do-Not-Disturb On/Off	372	Ring Tone Selection	398
Do-Not-Disturb Override	373	Routing Off	304
Feature Button Default	395	Station Speed Dial	382
Group Listen	312	Station Speed Dial Programming	383
Handsfree On/Off	319	System Forward Enable	352
Headset On	315	System Forward Disable	353
Headset Off	316	System Forward On/Off	354
Headset On/Off	317	System Speed Dial	381
Hold – Individual	336	Switch Keymap	399
Hold – System	335	Transfer To Hold	346

Administrator Feature Codes

Table 10-13 summarizes the default feature codes for system administrator endpoints. For feature descriptions, refer to the *Mitel 5000 Endpoint and Voice Mail Administrator Guide*, part number 580.8001.

Table 10-13. *System Administrator Default Feature Codes*

Feature	Code [Europe]
Automatic Diagnostics Delivery On/Off	9823
Clear Network Alarm	9851
Clear System Alarm	9850
Compression On/Off	9982 [9182]
Compression Statistics	9981 [9181]
Diagnostics On/Off	9900 [9100]
Enable Network Day	9862
Enable Network Night	9861
Modem Disable	9867
Modem Enable	9866
Modem Reset	9869
Night Ring On/Off	9860
Periodic Diagnostics On/Off	9825
Program Database	9932 [9132]
Program System Speed Dial	9801
Set Network Date/Time	9810
Set Time/Date	9800
Synchronize Network Time	9811

Diagnostics Mode Feature Codes

The Diagnostics Mode feature code 9900 [9100 in Europe] must be entered before the applicable feature codes can be used.

Table 10-14. *Diagnostics Mode Default Feature Codes*

Diagnostic Feature	Code U.S.	Code Europe
ASAI Snoop Off	9926	9126
ASAI Snoop On	9927	9127
Heap Dump	9943	9143
Dump Extension	9933	9133
Dump Node Information	9936	9136
Heap Statistics	9947	9147
ISDN View	9948	9148
Major Reset	9962	9162
Mark As Leaks	9945	9145
Mark As Quiescent	9946	9146
Minor Reset	9964	9164
Network Freeze Zone, System Histories	9939	9139
Network Unfreeze Zone, System Histories	9989	9189
Network Groups	9963	9163
Print Auxdata	9972	9172
Print Message Log	9975	9175
Print Network Log	9976	9176
Query Node Traffic	9978	9178
Show Version	9928	9128
SIP View	9987	9187
Spare 1–3	9910–9912	9110–9112
System History	9974	9174
Diagnostic – View Displays	9983	9183
Seize Device	9973	9173
System History – Freeze	9993	9193
System History – Unfreeze	9998	9198

Voice Processor System Programming

Introduction	11-4
Program Planning Sheets	11-4
Mitel Voice Processing Systems	11-4
BVM – Enabling and Disabling	11-5
Voice Processor Nodes	11-6
Local Nodes	11-6
Remote Nodes	11-6
Creating a Remote Node	11-6
Programming Remote Node Options	11-7
Start and Stop Times	11-7
Days of the Week	11-7
Remote Node Timers and Limits	11-8
Voice Profile for Internet Mail (VPIM) Networking	11-9
VPIM Messages	11-9
VPIM Programming	11-9
IP Settings for VPIM	11-10
VPIM Domain Name	11-10
SMTP Server Settings for VPIM	11-10
VPIM Nodes	11-11
VPIM Mailboxes	11-11
VPIM Mailbox Personalization	11-12
Network Settings	11-13
Timers and Limits	11-13
Validate Off-Node Mailboxes	11-15
Undeliverable Messages Destination Type	11-15
Voice Processor System Settings	11-16
Dial-0 Destinations	11-18
Total Storage Disk Usage Statistics	11-18
System Administrator Mailbox	11-18
VPIM Home Domain	11-19
Alternate Tone Detection	11-19
Volume	11-20
Save Message on Return Call	11-20
Swap “7 for Save” and “9 for Delete” Message Keys	11-21
Identification Prompt	11-21
Management Command and Event Ports	11-22

Automatic Speech Recognition Settings	11-23
Automatic Speech Recognition (ASR) Setting for Applications	11-24
Automatic Speech Recognition (ASR) Enabled for Applications	11-24
E-Mail Retrieval Interval (minutes)	11-25
Monitor Password	11-25
BS-BVM System Recording Codec	11-26
Time Slot Groups	11-27
Changing Time Slot Descriptions	11-27
Changing Time Slot Maximum Channel Allocations	11-27
Voice Processor Applications	11-28
Creating Voice Processor Applications	11-28
Changing Multiple Application Extensions	11-28
Copying and Pasting Application Attributes	11-29
Auto Attendant	11-30
Auto Attendant Information	11-30
Enable Auto Attendant Directory	11-30
Auto Attendant Transfer Prompt	11-30
Auto Attendant Directory Sort Order	11-30
Auto Attendant Transfer Method	11-31
Auto Attendant Recall	11-31
Call Routing Announcements	11-32
Programming a Call Routing Announcement	11-33
Using Digit Translation	11-33
Using Digit Translation Nodes	11-36
Message Notification/Retrieval	11-37
Programming MNR Classes of Service	11-37
Deleting MNR Classes of Service	11-37
Record-A-Call	11-38
Scheduled Time-Based Application Routing (STAR)	11-39
Programming STAR Schedules	11-39
Programming the Default STAR Application	11-40
Programming Automatic Fax Detection for STAR Applications	11-41
Voice Mail (Application)	11-41
Voice Processing Application Options	11-42
Day and Night Greetings for Voice Processing Applications	11-43
Attendants for Voice Processing Applications	11-44
Music-On-Hold for Voice Processing Applications	11-44
Time Slot Group for Voice Processing Applications	11-45
Transfer Recall Destination for Voice Processing Applications	11-45
Automatic Speech Recognition (ASR) Setting	11-46

Automatic Speech Recognition (ASR) Enabled	11-46
Propagate Original Caller ID on Transfer	11-46
Calling Party Name and Number	11-46
Extension IDs	11-47
Group Lists	11-49
Creating a Group List	11-49
Changing a Group List Extension Number	11-49
Adding Mailboxes to Group Lists	11-49
Removing Mailboxes from Group Lists	11-50
Viewing Group List Members	11-50
Audiotex Recordings	11-51
Voice Mail Directory	11-52
Enabling or Disabling the Voice Mail Directory	11-52
Changing the Voice Mail Directory Sort Order	11-52
Voice Processor Timers and Limits	11-53
Programming BVM Timers and Limits	11-54
DTMF Detection Information	11-57
DTMF Generation Information	11-59
Number of Voice Channels	11-60
Unified Messaging with EM Options	11-61
E-Mail Gateway	11-62
E-Mail Gateway Programming Options	11-62
Administrator E-Mail Address	11-63
E-Mail Address	11-63
E-Mail Real Name	11-63
E-Mail SMTP Port	11-64
E-Mail SMTP Server	11-64
E-Mail System	11-64
E-Mail Username	11-65
Gateway Password	11-65
E-Mail Gateway for Mitel CS-5600 Systems	11-66
Fax-On-Demand	11-69
Fax-on-Demand Timers and Limits	11-69
Fax Documents	11-71
Allow International Calls	11-71
Outgoing Access	11-72
Start/Stop Time	11-72
Days of the Week	11-73
Fax Format	11-73

Introduction

This chapter describes voice processing system features programming for the Mitel 5000 system. For mailbox programming, see “Subscriber Mailboxes” on [page 12-1](#).

For voice processing system installation information, refer to the applicable product installation documentation as described in “Mitel Voice Processing Systems” below.

For more information about voice processing features and systems, refer to the Voice Processing Features chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

Program Planning Sheets

For program planning sheets that list the voice processor system-wide information, refer to the programming planning sheets provided on the software CD-ROM. Program planning sheets are also available on the [edGe Online Manuals and Guides Web site](http://www.inter-tel.com/techpublications) (www.inter-tel.com/techpublications).

Mitel Voice Processing Systems

NOTICE

Voice Processing Unit (VPU) end of sale. VPU is no longer supported in v3.0. The VPU was discontinued in May 2007 and has reached its end of sale. Mitel recommends that current VPU installations upgrade to either Enterprise® Messaging (EM) or NuPoint Messenger. The two EM hardware platforms currently available, Base I and Base II, are separate system components and must be purchased from your local provider. Instructions for converting a VPU database to an EM database are included in the *Enterprise Messaging Installation and Maintenance Manual*, part number 780.8006. You cannot convert a VPU database to an NuPoint Messenger database. Contact your local provider for more information.

The Mitel 5000 supports the following voice processing applications:

- **Basic Voice Mail (BVM):** The preinstalled internal voice mail application that includes basic voice mail functionality. You program BVM options entirely in Mitel 5000 Database (DB) Programming. For more information about BVM, refer to the Voice Processing Features chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.
- **Enterprise Messaging (EM):** An external voice processing system that includes advanced features, such as Automatic Speech Recognition (ASR) and E-Mail Reader. Because EM uses separate hardware and software, you must install and configure EM as a separate system unit connected to the Mitel 5000. However, after installation, you can use DB Programming to configure many EM feature options.

For more information about EM and installation instructions, refer to the following:

- *Enterprise Messaging Installation and Maintenance Manual*, part number 780.8006
- Any addendums that apply the latest manual and software version
- **NuPoint Messenger:** An external voice processing system that resides on the Mitel Application Suite® (MAS) server and uses Session Initiation Protocol (SIP) to communicate with the Mitel 5000 system. Mitel 5000 systems support NuPoint Messenger as the system voice processing application. NuPoint Messenger is installed as a separate, external voice mail processor. For more information, refer to the following resources:
 - *Mitel 5000 and NuPoint Messenger Integration Guide*, part number 580.8008
 - *NuPoint Messenger Technical Documentation Help*
 - *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000
 - *Mitel 5000 DB Programming Help*

BVM – Enabling and Disabling

If you are installing an external voice mail system, you must disable BVM *before* you install and program the external voice processing system.

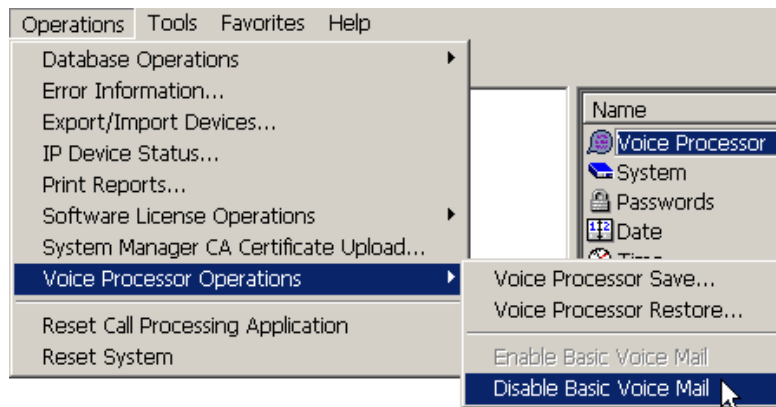
NOTE

After disabling BVM, System Alarm 203 appears on both the LCD panel on the Base Server and on the administrator endpoint (normal functionality). This alarm appears when a voice mail application is disconnected from a Mitel 5000 system that previously had a voice mail system connected.

The Disable Basic Voice Mail menu option is not dimmed after disabling Basic Voice Mail. This allows you to disable BVM if you did not do so before installing and programming the external voice processing system. If necessary, use the Administration Web Session (AWS) to verify that BVM is disabled.

To disable basic voice mail:

1. Open a DB Programming session.
2. Back up the Voice Mail database. You must use a USB flash drive for this operation. See “Saving and Restoring Voice Processing Databases” on [page 13-3](#).
3. From the DB Studio menu bar, select Operations – Voice Processor Operations – **Disable Basic Voice Mail**.



4. Click **OK** at the prompt to disable basic voice mail and terminate the session.
5. Restart the session to configure external voice processing parameters, if needed.

Voice Processor Nodes

The Node programming area is used to identify and define information about each node in the voice processor network. Before the local voice processor can deliver messages to another voice processor node in the network, the remote node must have an entry in this table. Refer to the Voice Processing chapter in the *Mitel 5000 Reference Manual*, part number 580.8007, for a complete description of voice processor networking.

NOTE

Remote voice processor nodes are **not** available when the system is using Basic Voice Mail.

Each node has its own internal message queue, which is similar to mailbox message queues, and will store messages destined for other nodes until they are delivered. Up to 100 nodes can exist in the voice processor network.

Local Nodes

Each Mitel 5000 system has a local node for handling system and subscriber voice processing features. The local node can be a BVM, EM, or NuPoint Messenger voice processor.

BVM and EM voice processing systems can use Voice Profile for Internet Mail (VPIM) protocol to connect to remote node or third-party voice processing applications. For more information, see "Voice Profile for Internet Mail (VPIM) Networking" on [page 11-9](#).

NOTE

VPIM will not be available for EM until the EM v2.0 release.

To view the local voice processing node:

Select Voice Processor – Devices – **Nodes**.

Remote Nodes

The following sections describe remote nodes and options for voice processing systems. For more information about remote nodes for voice processing systems, refer to the "Voice Processing Features" chapter in the 5000 reference manual.

Creating a Remote Node

You can create a remote voice processing node for BVM and EM systems. BVM systems use the VPIM protocol to communicate with the local voice processor. See "Voice Profile for Internet Mail (VPIM) Networking" on [page 11-9](#) for more information.

EM systems can use either TCP/IP or VPIM connection protocols to communicate with the local system. For more information, refer to *Enterprise Messaging Installation and Maintenance Manual*, part number 780.8006.

To create a remote node:

1. Select Voice Processor – Devices – **Nodes**.
2. Right-click in the right pane, and then click **Create Node**. The new node appears in the node list.

Programming Remote Node Options

When the voice processor network type is set to use TCP/IP, you can program the following node options.

Start and Stop Times

These options specify the time of day that messages are delivered to the remote node. If the start time and stop time are the same, it indicates that deliveries are valid the entire day. The default value for this field is 8:00AM to 8:00AM.

To set the time:

1. Select Voice Processor – Devices – **Nodes**.
2. In the **Value** column, select the current Start or Stop Time.
3. Click a time field to change the setting, as shown in the following example. For example, if you want to change the hour, click the hour, and then select the hour from the list. Repeat for the Minutes and AM/PM fields.



4. Click out of the field or press **ENTER** to save the change.

Days of the Week

These options specify the days of the week that messages are delivered to the remote node. Any combination of the days of the week is valid.

To enable a specific day of the week:

1. Select Voice Processor – Devices – **Nodes**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Click out of the field or press **ENTER** to save the change.

Remote Node Timers and Limits

You can program either of the following timers and limits for each node.

- **Latency Time:** This specifies how long the Voice Processor will wait between successful outgoing calls to the remote node if there are pending messages for the remote node. This field is only in effect if the current time on the Voice Processor is within the remote node delivery time/date settings. The range for this field is 0–1440 minutes (24 hours). When this field is programmed to 0, it indicates that the Voice Processor will deliver messages immediately to the remote node. In other words, as soon as the local node receives a message that is destined for the remote node, the Voice Processor will attempt to connect to the remote node and deliver the message (provided that the time is within the remote node delivery time/date settings). If this field is something other than 0, it specifies the amount of time that a message will remain pending on the local node before the Voice Processor attempts to deliver it to the remote node. For example, if this field is programmed to 60 minutes, the next network call to the remote node will occur 60 minutes after the last successful call to the node. The default value for this field is 30 minutes.
- **Priority Latency Time:** This specifies how long the Voice Processor will wait between outgoing calls to the remote node if there are pending priority messages for the node. This field is only in effect if the current time on the Voice Processor is within the remote node delivery start and stop date/time settings. The range for this field is 0–1440 minutes (24 hours). When this field is programmed to 0, it indicates that the Voice Processor will deliver priority messages immediately to the remote node. Any time the Voice Processor delivers pending priority messages, it will also deliver any non-priority messages that are pending for the remote node. Note that this field takes precedence over the Latency Time field. The default value for this field is 5 minutes.
- **Message Threshold:** This specifies the number of messages that must exist in the node message queue to force the Voice Processor to place a call to the remote node. This field is only in effect if the current time on the Voice Processor is within the remote nodes delivery time/date settings. This field can be used to ensure that the local Voice Processor does not get too backed up with messages destined for the remote node. If this field is programmed to 1, every message the local node receives that is destined for the remote node is delivered as soon as it is received by the local node. If this field is programmed to another number, it means that as soon as the remote node message queue has that many messages pending, the Voice Processor will attempt to connect to the remote node and deliver the messages. Note that this field takes precedence over both the Latency Time and Priority Latency Time fields. The range for this field is 0–100 messages and the default value for this is 5 messages.

To program remote node timers and limits:

1. Select Voice Processor – Devices – **Nodes**.
2. Double-click **Timers and Limits** to view the list.
3. In the **Value** column, click the value, and then type the new information in the box.
4. Click out of the field or press **ENTER** to save the change.

Voice Profile for Internet Mail (VPIM) Networking

NOTE

This feature will not be available for EM until the EM v2.0 release.

NuPoint Messenger systems must be configured to use the G.721 codec when using VPIM to communicate with BVM or EM systems.

Voice Profile for Internet Mail (VPIM) is a method for encoding voice mail messages as data, enabling travel via Simple Mail Transfer Protocol (SMTP) over IP networks. When VPIM is configured and enabled on two VPIM-compliant voice processors, the systems can exchange voice messages, sent as e-mail attachments, over the Internet.

This feature requires a “Voice Processor Messaging Networking” software license.

VPIM Messages

When VPIM networking is enabled, voice mail subscribers can send outbound voice messages and receive inbound voice messages for subscribers on another voice mail system. VPIM messages are sent and received as follows:

- **Outbound messages:** To leave a voice mail message, the voice mail subscriber calls the voice mail extension and is then prompted to enter the voice mailbox number. When the subscriber enters the mailbox number, the voice processor recognizes the extension as an off-node mailbox. After the subscriber records the message, the voice processor creates an e-mail and attaches the voice message as an audio file attachment. The voice processor routes the e-mail message, via SMTP, to the correct address using the domain information for the remote voice processing platform.
- **Inbound messages:** When the voice processor receives an e-mail message with a voice mail attachment, the username in the e-mail message specifies to which local mailbox the message belongs. The audio file is removed from the e-mail message and encoded to match the audio format used by the voice processor. The message is then routed to the appropriate subscriber's mailbox and the subscriber is notified that he or she has a new message. From the subscriber's perspective, the message sounds as if it were left locally. The only differences between a message received locally and a VPIM message are:
 - Subscribers with display endpoints see “UNKNOWN SENDER” rather than the name and extension of the caller when they listen to a VPIM message.
 - Subscribers are not presented with a reply option for VPIM messages.

VPIM Programming

To support VPIM, configure the following:

1. “IP Settings for VPIM” on [page 11-10](#)
2. “VPIM Domain Name” on [page 11-10](#)
3. “SMTP Server Settings for VPIM” on [page 11-10](#)
4. “VPIM Nodes” on [page 11-11](#)
5. “VPIM Mailboxes” on [page 11-11](#)
6. “VPIM Mailbox Personalization” on [page 11-12](#)

For VPIM programming troubleshooting information, see [page 17-88](#).

IP Settings for VPIM

To configure IP settings for the system:

1. Select System – **IP Settings**.
2. Program the following options (refer to *Mitel 5000 DB Programming Help* for details):
 - Base Server Hostname—must match the DNS server hostname (for a CS-5200/5400 system)
 - Processing Server Hostname—must match the DNS server hostname (for a CS-5600 system)
 - Static IP Address

VPIM Domain Name

NOTE

To receive and send e-mail messages using VPIM, the Base Server Hostname or Processing Server Hostname in System/IP Settings must be identical to the DNS hostname programmed in the Domain Name field. If the hostname does not match the DNS server hostname or an alias is used for the address, the system cannot resolve the name and its destination, and the VPIM server may reject the message.

To configure the VPIM domain name for BVM:

1. Select System – **IP Settings**.
2. In the **Domain Name** text box, type the domain name that you want to use. Type the domain that identifies the local system. For example, the following VPIM address “Doe, John <1000@localDomain.com>” has a VPIM Domain of “localDomain.com.” When a VPIM message is sent out from the local system, the “From” address contains the VPIM Domain. When other VPIM systems send messages to the local system, the “To” address contains an address with the domain being the VPIM Domain on the local system. See [page 11-11](#) for VPIM node information and guidelines.

To configure the VPIM domain name for EM:

1. Select **Voice Processor**.
2. In the **VPIM Home Domain** text box, type the domain that identifies the local system. For example, the following VPIM address “Doe, John <1000@localDomain.com>” has a VPIM Home Domain of “localDomain.com.” When a VPIM message is sent out from the local system, the “From” address contains the VPIM Home Domain. When other VPIM systems send messages to the local system, the “To” address contains an address with the domain being the VPIM Home Domain on the local system. See [page 11-11](#) for VPIM node information and guidelines.

SMTP Server Settings for VPIM

To set the SMTP server:

1. Select System – **E-mail Gateway**.
2. Set the E-mail System to **SMTP**.
3. Program the E-mail SMTP Server option (refer to *Mitel 5000 DB Programming Help* for details).

VPIM Nodes

To configure VPIM networking, you need to identify the voice processor that your system will be networked with. To do this, you create and configure nodes for each system in DB Programming. Keep the following considerations in mind when creating VPIM nodes:

- You can create up to 99 remote VPIM nodes.
- Each VPIM node has its own internal message queue (similar to a mailbox's message queues) and stores messages destined for other nodes until they are delivered.
- If some of the fields under a VPIM networked node have a red "X," it is because they do not apply.
- The value in the System Number/Domain field is the Fully Qualified Domain Name (FQDN) of the remote VPIM node (for example, node1.mitel.com).
- If you attempt to change the network type for a remote node to "VPIM" without configuring the SMTP server, an error message appears. You must first program the SMTP Server in the E-mail Gateway folder.
- If you attempt to change the network type from "VPIM" to "None" with one or more VPIM nodes programmed, an error message appears. You must first remove the VPIM nodes.
- If you attempt to change the network type from "VPIM" to "None" with System Health Report (Mitel 5000 only) enabled, an error message appears. You must first disable the "Enable E-mail Delivery" option in the System Health Report folder.

To create VPIM nodes:

1. Select Voice Processor – Devices – **Nodes**.
2. Right-click and select **Create Node**. After the VPIM node is created, DB Programming shuts down.
3. Reopen DB Programming and go to Voice Processor – Devices – **Nodes**. For the new node's Network Type, select **VPIM**.
4. Configure the **System Number/Domain** field for the node. The value in the System Number/Domain field is the Fully Qualified Domain Name (FQDN) of the remote VPIM node (for example, node1.mitel.com).

VPIM Mailboxes

VPIM networking is supported between Mitel voice processors such as EM and BVM. It can also be used to network a Mitel voice processor to NuPoint Messenger or a third-party voice processor.

To provide VPIM networking functionality for a voice processor, configure the VPIM fields in DB Programming. Then you must create one of the following mailbox types for each subscriber you want to configure for VPIM networking:

- **Associated off-node mailboxes:** When BVM or EM is networked with the same voice processor type or with a different voice processor type (BVM to BVM, BVM to EM, EM to EM), you must create associated off-node mailboxes for those mailboxes that you want networked. The associated off-node mailboxes you create will mirror the existing mailboxes on the local node.
- **Non-associated off-node mailboxes:** When BVM or EM is using VPIM networking with Mitel NuPoint Unified Messenger or a third-party voice processor, you must create nonassociated, you must create non-associated mailboxes on the local node for those mailboxes that you want networked. The non-associated mailboxes you create will mirror the existing mailboxes on the local node.

VPIM mailboxes act as proxy mailboxes to receive messages from other voice messaging systems.

NOTE

To receive and send e-mail across the Internet to a remote site, BVM or EM needs access outside its local network. Information needs to come into port 25 on the Mitel 5000. This may require changes to any firewall between the Mitel 5000 and the Internet.

To create VPIM associated mailboxes (the originating voice processor is networked with the destination voice processor):

NOTES

The following instructions assume that you have already imported the device extensions of the system node.

When creating an associated mailbox, the Remote Mailbox Extension field for the associated mailbox is automatically populated with the extension of the destination mailbox.

1. Select Voice Processor – Devices – Mailboxes – *<VPIM node>* – **<97XXX (associated mailbox)>**.
2. Right-click and select **Create Associated Off-Node Mailboxes**. A window appears prompting you to select the type of device to include.
3. Select the type of device, and then click **Next**. The list of devices appears. To view items in a list, click **List**.
4. Select the devices for which you want to create mailboxes. Then click **Add Items**. Your selections appear in the mailbox list. Click **Finish** to exit.
5. To select a series of devices, hold down the **SHIFT** key while selecting the first and last devices you want. To select two or more that are not next to each other, hold down the **CTRL** key while selecting the desired devices.

To create VPIM non-associated mailboxes (the originating voice processor is not networked with the destination voice processor):

1. Select Voice Processor – Devices – Mailboxes – *<VPIM node>* – **Local**.
2. Right-click, and then select **Create Non-Associated Mailboxes**. A window appears prompting you to select the type of device to include.
3. Enter the extension number you want to use for the first item in the Starting Extension field. Then indicate the number of items you want to create in the Number of Extensions field. The new mailboxes will be assigned sequentially to the next available numbers. When created, they appear in the programming window.
4. Program the Remote Mailbox Extension field to match the extension of the destination mailbox on the local node.

NOTE

When creating a non-associated mailbox, you must manually set the Remote Mailbox Extension field for the non-associated mailbox to match the extension number of the destination mailbox.

VPIM Mailbox Personalization

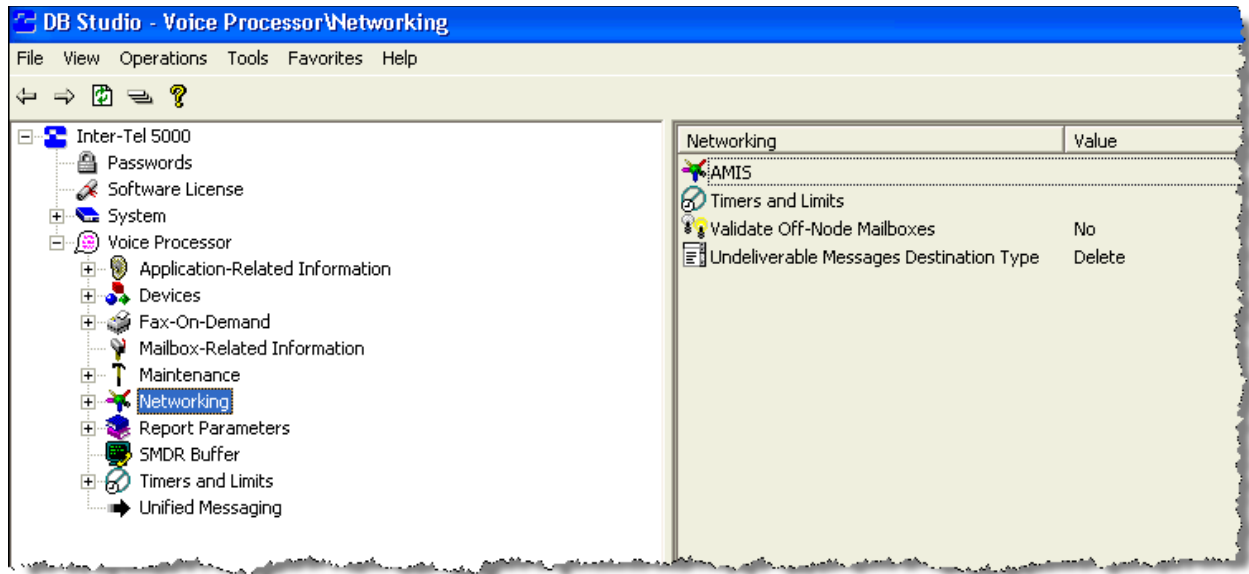
After you configure VPIM mailboxes in DB Programming, instruct subscribers to personalize their VPIM mailbox by recording a personal greeting and recording their name for the directory. For security reasons, subscribers should change the default mailbox password. Refer to the applicable endpoint user guide for instructions.

For Associated off-node mailboxes, the voice mail extension number is the voice mail extension for the *remote* node. For non-associated mailboxes, the voice mail extension number is the voice mail extension for the *local* node.

Network Settings

The following settings are located under Voice Processor – Networking, as shown in [Figure 11-1](#)

Figure 11-1. Network Settings



Timers and Limits

You can program the following timers and limits for the voice processor networking feature:

- Failed Connection Retry Interval:** Select the number of seconds that the system will wait between attempts to connect to another Voice Processor. When a connection fails, the system waits this number of seconds and then tries the connection again. The range is 0–32767 seconds; the default value is 60.
- Failed Connection Timeout:** Select the number of seconds that the system will wait for the other voice processor to respond before the connection attempt is considered a failure. After this timer expires, the system waits until the Failed Connection Retry Interval timer expires before it attempts to connect again. The range is 0–32767 seconds; the default value is 60.
- Maximum Messages Per Network Call:** Determines the maximum number of messages the voice processor will transmit to a remote node during one call. When this field is programmed to 0, the number of messages per network call is unlimited. Since messages transmitted via e-mail do not tie up any voice processing resources on the voice processor, this field does not apply to e-mail networking. The range is 0–1000 messages; the default value is 0.
- Maximum Network Call Attempts:** Determines the maximum number of consecutive, unsuccessful call attempts the voice processor will make to a remote node. When call attempts have reached the Maximum Network Call Attempts for a node, all pending messages for the node are returned to the destination programmed in the Undeliverable Messages Destination Type field. See “Undeliverable Messages Destination Type” on [page 11-15](#). No more calls are attempted for the node until the delivery start and stop date and time are active again. The range is 1–99; the default value is 30.

- **Maximum Network Calls:** *BVM only.* Limits the total number of simultaneous network calls. If the voice processor receives a network call when it already has the maximum number of network calls in progress, it will reject the new call. If the voice processor needs to deliver messages to a remote node when it already has the maximum number of network calls in progress, the message delivery will be delayed until the number of current network calls drops below the maximum. This range is 1 to 32; the default is 2.
- **Maximum Network Inbound Connections:** Select the number of inbound connections that the EM system will support at one time. This limits the number of TCP/IP networking and e-mail networking protocols used to network voice processing system. The valid range is 0–32767 connections, and the default value is 1.
- **Maximum Network Outbound Connections:** Select the number of outbound connections that the EM system will support at one time. This limits the number of TCP/IP networking and e-mail networking protocols used to network voice processing systems. The range is 0–32767; the default value is 1.
- **Maximum Network Message Length:** Determines the maximum length of a message the voice processor will transmit to a remote node. It is applied as the message is being recorded. When this field is programmed to 0, the message length is unlimited. The range is 1–600 minutes; the default message length is 15 minutes.
- **Network Call Failure Threshold:** Determines the maximum number of attempted calls to a node before a diagnostic alarm is printed. The alarm continues to be printed until the Maximum Network Call Attempts for the node has been reached, or a successful call has been completed. The value of this field can equal the value of the Maximum Network Call Attempts field, but it cannot exceed it. The range is 1–999; the default value is 15.
- **Network Call Retry Timer:** Determines the amount of time the voice processor waits before retrying a network call when the remote site does not answer or the number is busy. The system ignores this timer if the message threshold has been reached. The range is 1–60 minutes; the default is 5 minutes.
- **Update Message Latency Period Timer:** Determines the length of time the AVDAP will wait between update message delivery attempts. When this field is programmed the update message latency time for an update message will be reset. The notification tasks scan each AVDAP node to determine if the message threshold or message latency has expired. If either is true, the AVDAP will spawn a TCP/IP client task which attempts a connection to a remote AVDAP node. However, if there are only update messages in the node queue, the AVDAP checks if the update message latency time has expired when it checks the message threshold or message latency. If the update latency time has not expired, that is, it has not been 15 minutes since the last delivery of updates, a TCP/IP client is not spawned. This range is 1–1440 minutes; the default is 15 minutes

To program a timer or limit:

1. Select Voice Processing – Networking – Timers and Limits – **<timer or limit>**.
2. In the **Value** column, select the value, and then type the new setting in the box.
3. Click out of the field or press **ENTER** to save the change.

Validate Off-Node Mailboxes

The Validate Off-Node Mailboxes option indicates whether or not mailbox numbers are checked against DB Programming when a user attempts to deliver a message through a node network mailbox.

When this option is enabled, the mailbox number entered must be a valid network mailbox number on the local node. This means that the local node can only send messages to mailboxes on the remote node that have network mailboxes programmed on the local node. When this option is disabled, the mailbox number is not checked. This means the local node can send messages to any mailbox on the remote node, even if it does not have a local direct network mailbox.

To enable the Validate Off-Node Mailboxes flag:

1. Select Voice Processing – Networking – Timers and Limits – **Validate Off-Node Mailboxes**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Click out of the field or press **ENTER** to save the change.

Undeliverable Messages Destination Type

This field is used to determine the destination for all network messages which are undeliverable. It can have a value of Delete, Sender, or System Administrator.

- When the field is set to **Delete** (default), all undeliverable messages are deleted.
- When the field is set to **Sender**, all undeliverable messages are returned to the sender if possible. If the sender is unknown, the messages are returned to the System Administrator's mailbox. If the System Administrator's mailbox does not exist, the messages are deleted.
- When the field is set to System Administrator, all undeliverable messages are returned

To set the Undeliverable Messages Destination Type:

1. Select Voice Processing – Networking – Timers and Limits – **Undeliverable Messages Destination Type**.
2. In the **Value** column, select the option from the list.
3. Click out of the field or press **ENTER** to save the change.

Voice Processor System Settings

Voice processor system settings apply to BVM and EM systems only. If you are using an NuPoint Messenger system, see [page 11-4](#) for system settings information.

Voice Processor system settings include the following:

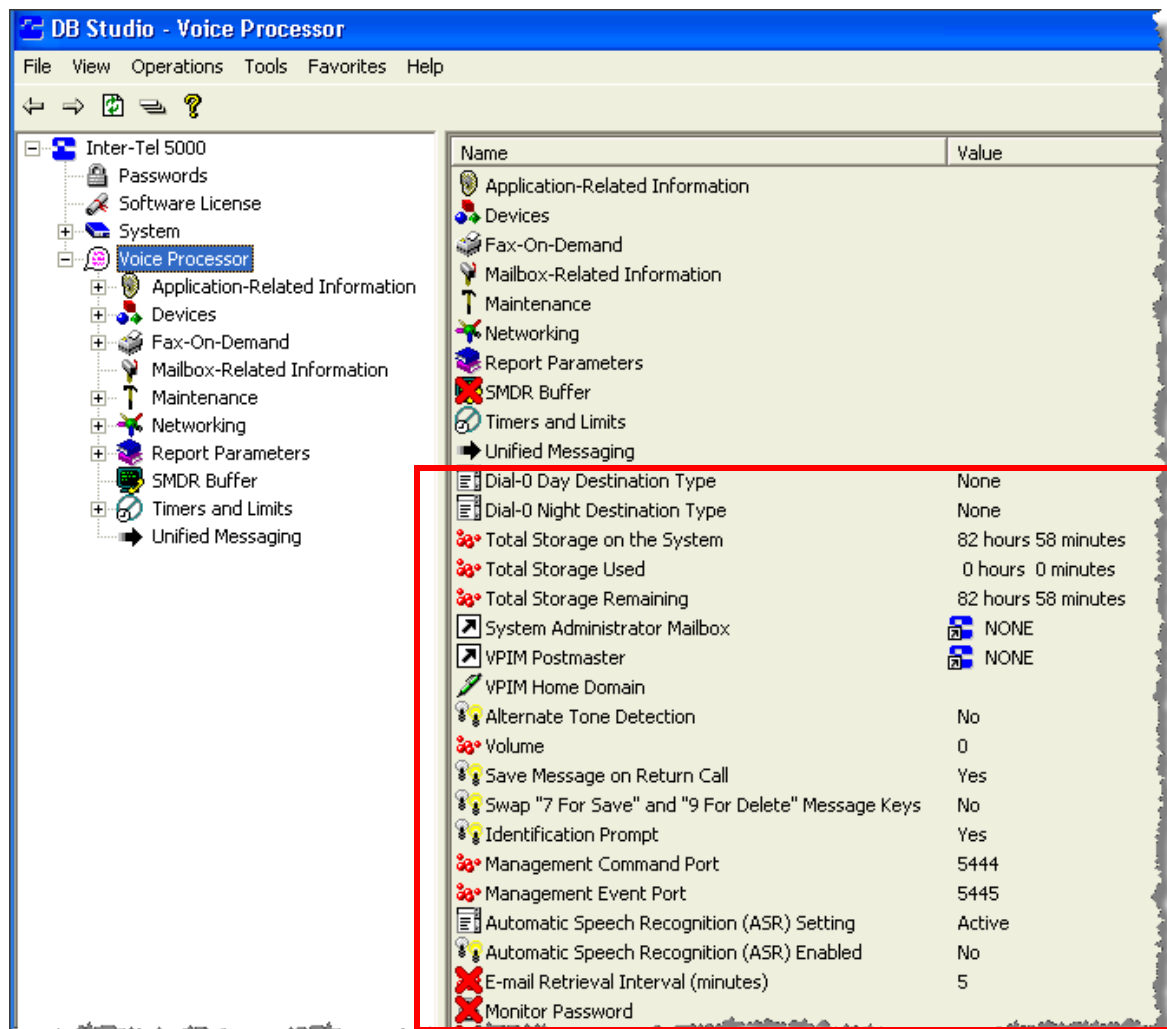
- “Dial-0 Destinations” on [page 11-18](#)
- “Total Storage Disk Usage Statistics” on [page 11-18](#)
- “System Administrator Mailbox” on [page 11-18](#)
- “VPIM Home Domain” on [page 11-19](#)
- “Alternate Tone Detection” on [page 11-19](#)
- “Volume” on [page 11-20](#)
- “Save Message on Return Call” on [page 11-20](#)
- “Swap “7 for Save” and “9 for Delete” Message Keys” on [page 11-21](#)
- “Identification Prompt” on [page 11-21](#)
- “Management Command and Event Ports” on [page 11-22](#)
- “Automatic Speech Recognition Settings” on [page 11-23](#)
- “Monitor Password” on [page 11-25](#)
- “BS-BVM System Recording Codec” on [page 11-26](#)

You can view or program voice processor system settings from the Voice Processor level in DB Programming, as shown in Figure 11-2 on [page 11-17](#).

NOTE

“Windows Networking” settings apply to VPU systems only and are no longer supported.

Figure 11-2. Voice Processor System Settings



Voice processing system settings

Dial-0 Destinations

System Dial-0 Destination options are the same as mailbox Dial-0 Destination options. See [page 12-18](#).

Total Storage Disk Usage Statistics

Total Storage options show voice processing computer disk storage status. The information is presented for reference only and cannot be programmed. Disk Usage Statistics include the following:

- **Total Storage on the System:** The amount of disk space (in hours) available on the voice processing computer.
- **Total Storage Used:** The amount of disk space (in hours) that has been used by the voice processing applications.
- **Total Storage Remaining:** The amount of disk space (in hours) remaining in the voice processing computer. If the disk is nearly full, you can increase disk space by clearing the SMDR buffer or mailbox messages. If available disk space is frequently low, you should install a larger-capacity disk drive in the voice processing computer.

To view Disk Usage Statistics:

Select **Voice Processor**. Disk Usage Statistics are shown in the right pane.

System Administrator Mailbox

The system administrator mailbox is used to:

- Record custom audiotex recordings for voice processing applications.
- Send broadcast messages to all subscribers.
- Perform mailbox and group list maintenance.

For more information about using the administrator mailbox, refer to the *Mitel 5000 Endpoint and Voice Mail Administrator Guide*, part number 580.8001.

To assign the System Administrator Mailbox:

1. Select Voice Processor – **System Administrator Mailbox**.
2. In the **Value** column, right-click the existing value, and then select **Change System Administrator Mailbox**. A window appears prompting for the device type to include.
3. Select **Mailbox**, and then click **Next**. The items with details appear. To view items in a list only, click **List**.
4. Select the desired mailbox, and then click **Finish**. The selection appears in the System Administrator Mailbox field.

VPIM Home Domain

Applies to EM systems only. The VPIM Home Domain is the domain that identifies the local system. For example, the following VPIM address “Doe, John <1000@localDomain.com>” has a VPIM Home Domain of “localDomain.com.” When a VPIM message is sent out from the local system, the “From” address contains the VPIM Home Domain. When other VPIM systems send messages to the local system, the “To” address contains an address with the domain being the VPIM Home Domain on the local system.

NOTE

You must program the E-Mail Gateway SMTP Server before you can program a VPIM domain name (see “E-Mail SMTP Server” on [page 11-64](#)).

To program the VPIM Home Domain:

1. Select Voice Processor – **VPIM Home Domain**.
2. In the **Value** column, type the domain name.
3. Click out of the field or press **ENTER** to save the change.

Alternate Tone Detection

In some remote messaging situations, the device being called uses signaling tones that the voice processor does not recognize, at default. If remote messaging is not properly signaling the device, enable this option to allow the voice processor to detect alternate tones.

To enable the Alternate Tone Detection option:

1. Select Voice Processor – **Alert Tone Detection**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Click out of the field or press **ENTER** to save the change.

Volume

You can set at the same time the volume level for all of the voice channels used by the voice processor. This includes all prompts, voice mail messages, and audiotex recordings. These options cannot be adjusted separately and only the playback volume is affected, not the recording volume.

When a voice mail user increases or decreases the volume during the call, the system volume level currently programmed does not change. Only the voice channel being used by the caller is temporarily altered. When the user has completed the call, the system resets the volume of the voice channel used to the selected setting. The volume range is -8 for the softest setting to +8 for the loudest. The normal setting is 0.

To set the volume level:

1. Select Voice Processor – **Volume**.
2. In the **Value** column, enter the new value in the box.
3. Click out of the field or press **ENTER** to save the change.

Save Message on Return Call

The Return Call feature allows a voice mail user to place return calls to message senders (with Caller ID or extension numbers) directly from the voice mailbox. The Save Message on Returned Call flag tells the voice processor whether or not to save the message that the user is listening to at the time the user chooses to make the return call.

If the flag is set to **Yes**, the voice processor automatically moves the message to the user's saved message queue when the user places the return call. If the message is already in the saved message queue when the user places the return call, then it is unchanged. This applies to both the new message queue and deleted messages. If the flag is enabled and the user places a return call from a deleted message, that message is moved to the saved message queue, restoring the message. If the flag is set to **No**, the voice processor leaves the message in the same queue it was in before the user placed the return call. Note that if the flag is set to **No** and the message is in the new message queue, the voice processor refreshes the message lamp on the user endpoint.

To enable the Save Message On Return Call option:

1. Select Voice Processor – **Save Message on Return Call**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Click out of the field or press **ENTER** to save the change.

Swap “7 for Save” and “9 for Delete” Message Keys

NOTE This feature will not be available for EM until the EM v2.0 release.

You can swap the 7 and 9 keys for all mailboxes. This changes the default value for any *new* mailboxes. All existing mailboxes are not changed. You must manually change existing mailboxes. For more about the feature and individual mailbox programming instructions, see [page 12-25](#).

To swap the 7 and 9 message keys:

1. Select Voice Processor – **Swap “7 for Save” and “9 for Delete” Message Keys**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Click out of the field or press **ENTER** to save the change.

Identification Prompt

The Identification Prompt option enables or disables a custom message that identifies the voice processing system. When enabled, this prompt is heard before the voice mail greeting and states, “Your call is being handled by the voice processing system.” This prompt automatically plays when external callers:

- Are transferred to a voice mailbox. The system plays the ID prompt before playing the mailbox greeting (primary, alternate, or system).
- Are forwarded to a voice mailbox. The system plays the ID prompt before playing the mailbox greeting (primary, alternate, or system).

If the identification prompt is disabled, it is not played before the voice mailbox greeting when an external caller accesses a mailbox. By default, this flag is enabled.

To disable the Identification Prompt:

1. Select Voice Processor – **Save Message on Return Call**.
2. In the **Value** column, clear the check box. The field changes to **No**. To enable the feature, select the check box.
3. Click out of the field or press **ENTER** to save the change.

Management Command and Event Ports

EM system supports an Operations, Administration, and Management (OAM) interface that allows you to send commands to and receive responses from the system. To use this interface, you must program the following ports:

- **Management Command Port:** Enter the port number that the system will use for receiving commands and sending responses. The valid range is 0–65535, and the default is 4444.
- **Management Event Port:** Enter the port number that the system will use for sending event messages to the connected console. The valid range is 0–65535, and the default is 4445.

NOTE

Make sure these ports are open on firewalls/routers if the computer issuing these commands is located outside of the current subnet.

To set program a Management Command or Event Port:

1. Select Voice Processor – **Management Command** (or **Event**) **Port**.
2. In the **Value** column, enter the new value in the box.
3. Click out of the field or press **ENTER** to save the change.

Automatic Speech Recognition Settings

The EM voice processing system supports Automatic Speech Recognition (ASR). ASR allows users to access voice processing applications, such as voice mail, by speaking menu options instead of dialing digits on your dialpad. Although you can enable this feature at a system, application, or mailbox level, if it is enabled at a top-level folder, that setting overrides any subfolder programming. For example, if you enable the feature at the system level, the feature is automatically enabled at the application and mailbox levels. If you enable the feature at the application level only, it is available for the programmed applications and mailboxes only. If you enable the feature at the mailbox level only, it is available for mailboxes only.

Table 11-1 shows several ways to enable or disable ASR. The system determines the setting in a top-down approach. So, if the ASR Setting is set to Active at the top-level, the ASR Enabled value is applied to that level and any levels below it.

Table 11-1. Sample Speech Recognition Combinations

Voice Processor	Application	Mailbox	Results
ASR Setting: Active ASR Enabled: Yes	N/A (settings are ignored)	N/A (settings are ignored)	ASR is enabled for all applications and mailboxes.
ASR Setting: Active Speech Recognition Enabled: No	N/A (settings are ignored)	N/A (settings are ignored)	ASR is disabled for all applications and mailboxes.
ASR Setting: Delegated ASR Enabled: N/A (ignored)	ASR Setting: Active ASR Enabled: Yes	N/A (settings are ignored)	Speech recognition is enabled for all applications and mailboxes.
ASR Setting: Delegated ASR Enabled: N/A (ignored)	ASR Setting: Active ASR Enabled: No	N/A (settings are ignored)	ASR is disabled for all applications and mailboxes.
ASR Setting: Delegated ASR Enabled: N/A (ignored)	ASR Setting: Ignored ASR Enabled: N/A (ignored)	N/A (settings are ignored)	ASR is disabled for all applications and mailboxes.
ASR Setting: Delegated ASR Enabled: N/A (ignored)	ASR Setting: Delegated ASR Enabled: N/A (ignored)	ASR Setting: Active ASR Enabled: Yes	ASR is enabled for all applications and mailboxes.
ASR Setting: Delegated ASR Enabled: N/A (ignored)	ASR Setting: Delegated ASR Enabled: N/A (ignored)	ASR Setting: Active ASR Enabled: No	ASR is disabled for all applications and mailboxes.
ASR Setting: Delegated ASR Enabled: N/A (ignored)	ASR Setting: Ignored and Delegated ASR Enabled: N/A (ignored)	ASR Setting: Active ASR Enabled: Yes	ASR is enabled for mailboxes only.
ASR Setting: Delegated ASR Enabled: N/A (ignored)	ASR Setting: Ignored and Delegated ASR Enabled: N/A (ignored)	ASR Setting: Active ASR Enabled: No	ASR is disabled for all applications and mailboxes.

To enable ASR:

Program the following options:

- Voice Processor – **Automatic Speech Recognition (ASR) Setting** (see below).
- Voice Processor – **Automatic Speech Recognition (ASR) Enabled** (see below).

Automatic Speech Recognition (ASR) Setting for Applications

EM systems only. Determines whether the system will use the ASR Enabled setting in the current level or in the next level. Depending on the level, you may have one or more of the following options:

- **Active:** (*system, applications, and mailboxes*) Indicates that the system will use the ASR Enabled setting for the current folder. If selected, any subfolders that have the speech recognition options automatically use the ASR Enabled setting for this folder. This is the default for all folder levels.
- **Delegated:** (*system and applications only*) Indicates that the system will use the ASR Enabled setting for the next folder level.
- **Ignored:** (*applications and mailboxes only*) Indicates that the system will ignore the ASR Enabled setting for this folder. This folder will then use the settings programmed for the parent level. For example, mailboxes will use the setting specified for the application, and applications will use the setting specified for the system.
- **Ignored and Delegated:** (*applications only*) Indicates that the system will ignore the ASR Enabled setting for this folder and use the parent level folder (that is, the Voice Processor folder). If, however, the Voice Processor folder ASR Setting field is set to Delegated, this folder will use the settings programmed for the next folder level; that is, the mailbox folder.

To select the ASR level:

1. Select Voice Processor – **Automatic Speech Recognition (ASR) Setting**.
2. In the **Value** column, select the option from the list.
3. Click out of the field or press **ENTER** to save the change.

Automatic Speech Recognition (ASR) Enabled for Applications

EM systems only. Determines whether ASR is enabled for the current folder, as well as any subfolders or parent folders based on the ASR Setting field. If enabled, the system, application, or mailbox supports voice recognition for accessing that particular feature. If disabled, the system, application, or mailbox will **not** support voice recognition.

The ASR Enabled field is ignored (displays a red “X”) if the ASR Setting is set to Delegated, Ignored, or Ignored and Delegated.

NOTE

The ASR Enabled field is ignored (that is, displays a red “X”) if the ASR Setting is set to Delegated, Ignored, or Ignored and Delegated.

To select the ASR level:

1. Select Voice Processor – **Automatic Speech Recognition (ASR) Enabled**.
2. In the **Value** column, select the option from the list.
3. Click out of the field or press **ENTER** to save the change.

E-Mail Retrieval Interval (minutes)

For BVM systems only. This option indicates how often Email/VPIM messages are retrieved from the networked node. The range is 1–60 minutes; the default is 5 minutes. This option appears with a red “X” for voice-processing systems other than BVM.

To set the E-Mail Retrieval Interval (minutes) option:

1. Select Voice Processor – **E-Mail Retrieval Interval (minutes)**.
2. In the **Value** column, select the option from the list.
3. Click out of the field or press **ENTER** to save your changes.

Monitor Password

To protect the voice processor against unauthorized access, you can require a password for the AVDAPMon utility.

To program the password:

1. Select Voice Processor – **Monitor Password**.
2. Right-click **Monitor Password**, and then select **Edit Password**. The Edit Monitor dialog box appears.
3. Enter the current password, if one exists.
4. Type the new password (up to 40 characters) in the New password box. Typed characters appear as asterisks (**).
5. Retype the password in the **Confirm password** box.
6. Click **OK** to exit and save the password. If the entered passwords match, you return to the Password field. If not, you must re-enter the new password and verify it again.

NOTE

To provide system security, the e-mail system must have a password. To make the passwords difficult to guess, they should not consist of predictable patterns, such as one digit repeated several times.

BS-BVM System Recording Codec

This audio enhancement for system recordings applies to CS-5200 and CS-5400 Base Server (BS) BVM systems only. For BS-BVM systems, you can use either the default G.729A codec or the G.726-32 codec.

G.726-32 codec recordings offer higher voice quality and result in a higher Mean Opinion Score (MOS), especially if other G.729 codecs are in the call path. However, G.726-32kbps recordings require four times the space on the compact flash-type memory card to store the same recording lengths. If you use the G.726-32 codec, you may want to upgrade to a larger compact flash-type memory card.

NOTE | Selecting the G.726-32 codec prompts a BVM reset.

To program the system recording codec:

1. Select Voice Processor – **BS-BVM System Recording Codec**.
2. In the **Value** column, select the option from the list.
3. Click out of the field or press **ENTER** to save your change. If you selected G.726-32, a message appears to notify you that changing the codec to G.726-32 does the following:
 - Causes BVM to reset.
 - Affects the storage space on the compact flash-type memory card.
 - Does not affect all previous recordings that use the G.729A codec.
4. Click **Yes** to proceed. BVM is reset.

Time Slot Groups

NOTE

Complete time slot group and voice channel programming before you create and program applications. See “Voice Processor Applications” on [page 11-28](#).

Applies to BVM and EM voice processors only. Each application is assigned to a “Time Slot Group,” which determines the maximum number of voice channels (up to 32) used by the applications in that group. Voice channels are used for processing calls between the system and the applications.

The voice channel limit for the time slot group may exceed the number of voice channels actually provided by the hardware, due to programmed limits being set higher than the hardware limits and/or heavy system traffic.

For example, if an Automated Attendant application is assigned to a time slot group that has a programmed limit of five voice channels, it can normally support five simultaneous transfers of outside calls to extensions. However, if only four voice channels are available, a fifth call cannot be completed to that or any other application. When all voice channels are busy, intercom callers hear reorder tone and CALL CANNOT BE COMPLETED displays on display endpoints. Outside callers will hear ringing but their calls will not be answered.

Call Routing Announcement digit translation nodes do not have assigned time slot groups.

Changing Time Slot Descriptions

The Time Slot Group list shows the time slot groups and the number of channels currently assigned to the groups.

To change the description of a time slot group:

1. Select – Voice Processor – Application-Related Information – **Time Slot Groups**.
2. Click once on the current description.
3. Type the new description in the box, using up to 20 characters.
4. Click out of the option or press **ENTER** to save the change.

Changing Time Slot Maximum Channel Allocations

The Maximum Channel Allocation determines the maximum number of voice channels that are used by the applications assigned to this time slot group. By default, this field displays the maximum available voice channels, as determined by the hardware configuration.

The combined total of voice channels assigned to all time slot groups may exceed the number of voice channels provided by the hardware. This is allowed because it is not likely that all time slot groups will be busy at once. However, an individual time slot group is limited to the Maximum Channel Allocation. This parameter is used for setting the limit of voice channels that will be used by the associated application.

To change the Maximum Channel Allocation of a time slot group:

1. Select – Voice Processor – Application-Related Information – **Time Slot Groups**.
2. In the Maximum Channel Allocation column, enter the maximum number of voice channels to be used by the applications.

Voice Processor Applications

NOTE

Voice processor applications apply to BVM and EM voice processors only. Complete time slot group and voice channel programming before you create and program applications. See “Voice Processor System Settings” on [page 11-16](#).

The following are voice processing applications:

- “Auto Attendant” on [page 11-30](#)
- “Auto Attendant Recall” on [page 11-31](#)
- “Call Routing Announcements” on [page 11-32](#)
- “Message Notification/Retrieval” on [page 11-37](#)
- “Record-A-Call” on [page 11-38](#)
- “Scheduled Time-Based Application Routing (STAR)” on [page 11-39](#)
- “Voice Mail (Application)” on [page 11-41](#)

Creating Voice Processor Applications

You can create up to 150 voice processor applications, but there can be only one Message Notification/Retrieval application. In the default database, extension numbers 2500–2649 are reserved for applications, but any available extension number can be used.

NOTE

Complete Time slot group and voice channel programming before creating and programming applications. See “Time Slot Groups” on [page 11-27](#).

To create a new application:

1. Select Voice Processor – Devices – **Local** (“Local” is applicable only if a remote node is connected).
2. Double-click **Applications**.
3. Right-click in a blank area of the right pane. A list of options appears to create applications. After you create an application, you cannot change the application type. You can, however, delete it by selecting it, right-clicking and selecting **Delete**.
4. Type the description (up to 20 characters) and user name (up to 16 characters) for each application. The description appears wherever the application is listed and in the system directory. The username appears on endpoint displays when the application is used.
5. Click out of the field or press **ENTER** to save the change.

Changing Multiple Application Extensions

You can change several voice processing application extensions at the same time.

To change several extensions at the same time:

1. Select Voice Processor – Devices – **Local** (the “Local” option is shown only if a remote node is connected).
2. Double-click **Applications**.
3. Select the applications that you want to change. You can use the CTRL and SHIFT keys to select multiple applications.
4. Right-click, and then select **Batch Extension Change**.
5. In the Create Extension dialog box, select the starting extension number. The other selected applications are numbered consecutively after this number.
6. Click **OK** and the extensions are automatically renumbered and resorted in the list.

Copying and Pasting Application Attributes

The copy and paste operations in DB Programming allow you to copy certain attributes from one application and paste the attributes into several other like applications. This allows you to quickly program several similar devices at one time.

To copy an application:

1. Select Voice Processor – Devices – **Local** (the “Local” option is shown only if a remote node is connected).
2. Double-click **Applications**.
3. Right-click the application extension, and then select **Copy**.
4. To paste the programming information into another application, right-click the application where you want to paste the information, and then select **Paste**. The Copy dialog box allows you to select the attributes you want to copy.
5. Select the desired attributes, and then click **OK**.

Auto Attendant

Applies to BVM and EM voice processors only. The Auto Attendant provides automated call answering service. Calls can be transferred, forwarded, or can directly ring in to an Automated Attendant application. When an automated attendant answers a call, it plays a recording that gives dialing instructions. After hearing the recording, the caller may then directly dial an endpoint extension number, voice mail application number, or hunt group extension number. For information about programming voice processing application options, see [page 11-42](#).

Auto Attendant Information

You can enable or disable the automated attendant directory and determine whether the directory is sorted by first or last name using these fields. You can also determine whether the system automated attendant transfer prompt plays when calls are transferred to endpoints without mailboxes or extension IDs.

Enable Auto Attendant Directory

If the Auto Attendant Directory is enabled, the system allows anyone routed to an Auto Attendant application to access the company directory. If the option is disabled, the Auto Attendant does not prompt the caller for the directory option while in the Auto Attendant area.

To enable or disable the Auto Attendant Directory:

1. Select – Voice Processor – Application-Related Information – Auto Attendant Information – **Enable Auto Attendant Directory**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Click out of the option or press **ENTER** to save the change.

Auto Attendant Transfer Prompt

The Auto Attendant Transfer Prompt determines if the transfer prompt (“Please hold while your call is being transferred to...”) plays after a caller has entered an extension number that does not have an associated mailbox or extension ID. This applies to transfers from CRA applications that use the “Transfer To Extension” action, which is described on [page 11-33](#).

To enable or disable the Auto Attendant Transfer prompt:

1. Select – Voice Processor – Application-Related Information – Auto Attendant Information – **Auto Attendant Directory**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Click out of the option or press **ENTER** to save the change.

Auto Attendant Directory Sort Order

This option is only for Auto Attendant calls. The Auto Attendant Directory Sort Order determines if the mailbox and extension ID descriptions in the directory will be sorted by first name or last name. To change the Voice Mail Directory Sort Order, see “Changing the Voice Mail Directory Sort Order” on [page 11-52](#).

1. Select – Voice Processor – Application-Related Information – Auto Attendant Information – **Directory Sort Order**.
2. From the **Value** column, select the option from the list.
3. Click out of the option or press **ENTER** to save the change.

Auto Attendant Transfer Method

Determines how transfers will be made to other applications from Call Routing Announcement applications. The options are Announce Only, Screened, and Unannounced (the default setting is Unannounced). For more information about transfer methods, refer to the System Features chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

To set the Auto Attendant transfer method:

1. Select – Voice Processor – Application-Related Information – Auto Attendant Information – **Auto Attendant Transfer Method**.
2. From the **Value** column, select the option from the list.
3. Click out of the option or press **ENTER** to save the change.

Auto Attendant Recall

Applies to BVM and EM voice processors only. If a call that was transferred by the Auto Attendant application is not answered before the Transfer Voice Processor timer expires, the call recalls the Automated Attendant Recall application. The recall destination announces that the endpoint is unavailable and allows the caller to choose to leave a message—if a mailbox is programmed for that endpoint—or dial another extension number.

To program Auto Attendant Recall options:

1. Select Voice Processor – Devices – **Local** (“Local” is applicable only if a remote node is connected).
2. Double-click **Applications**.
3. Double-click **Auto Attendant Recall**.
4. Program the options described “Voice Processing Application Options” on [page 11-42](#).

Call Routing Announcements

Applies to BVM and EM voice processors only. For a detailed description of CRAs, refer to the Voice Processing chapter in the *Mitel 5000 Reference Manual*, part number 580.8007. Call Routing Announcements (CRAs) can be used two ways:

- A CRA can be used in place of a playback device. The playback device function is especially useful for programming hunt group announcement and overflow endpoints. When called, the CRA application plays a recording and then hang up.
- The CRA can use Digit Translation (see [page 11-33](#)), which allows the caller to press a single digit for access to a mailbox, a Fax-On-Demand function (external voice processing systems only), or to an endpoint or a hunt group that has an associated mailbox or extension ID. Digit translation can be programmed for each digit 0–9, #, and *, plus a Timeout that is used when the caller does not enter a digit. Each digit can lead to a “digit translation node” that has its own digit translation values. This layered CRA digit translation creates a “tree” of programmable digit translation nodes. There can be up to 200 digit translation nodes in the system and up to 20 for each CRA application.

Use the following guidelines to design an effective CRA application:

- Design with the caller in mind, not just the information you want to include.
- Keep menus as simple as possible, with four or fewer options per menu.
- Number options sequentially and do not skip numbers. List “transfer to operator” last.
- Use consistent digits for options, such as 1 for Yes, 2 for No, and 0 for the operator.
- State the option before the digit. For example, say, “For account information, press 1,” instead of, “Press 1 for account information.”
- Draw a map of your arrangement to avoid “dead ends” or endless loops.
- Take advantage of Caller ID [CLID] and DNIS to route calls to suitable menus.
- Keep recordings short (under 60 seconds) and do not use jargon.
- Give the most frequently requested information in the first 10 seconds, without requiring the caller to press a digit.
- Make sure the recordings are clear and the voice is consistent from prompt to prompt. Avoid heavy regional accents.
- Do not repeat the main greeting on any other level.
- Make seasonal changes when necessary, but keep menu options the same because callers get used to them. Tell the caller if option changes have been made.
- Include an option for overriding the Primary Language. For example, say, “For English, press 1. Para Español, empuje 2.”
- Test your application any time you make a change. Listen to your prompts periodically.

Programming a Call Routing Announcement

Make sure you read the guidelines on [page 11-32](#) before you program the CRA.

To program a CRA:

1. Create the CRA (see [page 11-28](#)).
2. Change the day and night greetings to custom recordings. Remove the default recordings and assign new recording numbers. Write down the recording numbers and their assignments. You will record them later.
3. If you are using Digit Translation, create the digits and nodes you are using as follows.
 - a. Appropriately name the descriptions and usernames. For example: Sales 1, Service 2, Repair 3, and so on.
 - b. Return to the Applications Programming screen and expand the Call Routing application that you have just created.
 - c. Program each digit or node individually and set the greetings as desired. Repeat this step for all nodes and digits.
4. Use the System Administrator's mailbox (see [page 11-18](#)) to record your custom greetings.
5. Test the application and all of its nodes by calling the application and checking each digit and node.

Using Digit Translation

Applies to BVM and EM voice processors only. Digit translation allows callers to dial a single digit to select a designated extension number, modem, mailbox, or hunt group extension number. Digit translation can be programmed for each digit 0–9, #, and *, plus a Timeout that is used when the caller does not enter a digit. Each digit can lead to a digit translation node (see [page 11-36](#)) that has its own digit translation actions. This CRA digit translation creates a tree of programmable digit translation nodes. For a detailed explanation of CRA digit translation nodes and a sample tree, refer to the Voice Processing Features chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

After you create a digit translation node, you can assign it to more than one CRA application. This allows entire node hierarchies to be shared or moved without reprogramming. When using a CRA application with digit translation, you can program individual voice processing applications assigned to the digits to override the device language and provide prompts in one language only.

To program digit translations for the CRA:

1. Select Voice Processor– **Devices**.
2. Double-click **Digit Translations**. A list of the digits and their actions and destinations appears.
3. Program the following options:
 - **Name:** The digit that callers press. Timeout represents no digits being entered.
 - **Action:** From the list, select the action for digit. The Actions that can be selected for the digits (*, #, 0–9) and for the Timeout option are as follows:
 - **Cancel Fax Selections:** Usually assigned to the digit *. It is used for canceling fax document selections that a caller has entered.
 - **Company Directory – First Name:** Sends the caller to the directory prompt that asks the caller to enter the first name of the desired party.
 - **Company Directory – Last Name:** Sends the caller to the directory prompt that asks the caller to enter the last name of the desired party.

- **End Fax Selections:** Usually assigned to the digit #. It is required for signaling the system that the caller has entered all desired fax document selections (either through a Select Fax Document By Number or a Select Fax Document Action). You see a warning message when you exit if you have programmed a Select Fax without creating an End Fax Selections action.
- **Invalid:** (Not available for Timeout.) The digit will not be used. Callers who press this digit hear a recording that tells them that it is invalid.
- **Select Fax Document:** (Not available for Timeout.) Selects a specific document for faxing. Callers should be prompted to select this digit with a recording that tells them the name of the document. For example, "Press 2 for a price list." This must be accompanied by an End Fax Selection and should also be accompanied by a Cancel Fax Selection Action.
- **Select Fax By Document Number:** (Not available for Timeout, or digits * or #.) This is similar to the Transfer to Collected Extension described below. It allows callers to enter the exact four-digit numbers for documents. Assign this Action to the digit(s) that correspond to the first digits of the document numbers. For example, if you have documents numbered 0001-1000, program digits 0 and 1 to have a Select Fax By Document Number Action. Callers can then dial four-digit document numbers that begin with 0 or 1.

When document numbers begin with 0, the caller can select documents by entering the number without 0 and pressing # (but the Select Fax By Document Number action must be assigned to the digit 0). For example, the caller can enter 99# for document number 0099. This must be accompanied by an End Fax Selection and should also be accompanied by a Cancel Fax Selection Action.
- **Subscriber Access:** Sends the caller to the voice mail application that prompts the caller to enter a mailbox number.
- **Transfer To Collected Extension:** (Cannot be used for Timeout, *, #, or 0). To allow callers to dial extension numbers of endpoints and hunt groups (including off-node devices) that have a mailbox or extension ID, use this Action for digits that correspond to the first digits of extension numbers. For example, if digit 1 is "Transfer To Collected Extension," callers can dial extension numbers that begin with 1. However, if digit 1 is "Transfer to Extension 2000," as described below, callers attempting to dial an endpoint extension number that begins with 1 will instead be transferred to 2000.

NOTE

If a caller dials an extension number of a mailbox that does not have an associated endpoint, the call is delivered to the mailbox instead of an extension.

- **Transfer To Extension:** Sends the call to the extension (endpoint, hunt group, application, or off-node device) that appears in the Transfer Destination field.
- **Transfer To Mailbox:** Sends the call to the designated mailbox.
- **Transfer To Node:** (Not available for Timeout.) Sends the call to a digit translation node that allows access to further digit translation options. See [page 11-36](#). See ["Using Digit Translation Nodes"](#) on [page 11-36](#).

- **Transfer To Operator:** Transfers the call to the programmed Dial-0 Destination.

NOTE

If you select Transfer To Operator but a Dial-0 Destination has not been programmed, a warning message appears, and you must program the Dial-0 Destination before proceeding. For details, see “Dial-0 Destinations” on [page 12-18](#).

- **Hang Up:** This option applies to Timeout only. When applied, the system disconnects from the call if the user does not enter a digit.
- **Transfer Destination:** The actions Select Fax Document, Transfer To Extension, Transfer To Mailbox, and Transfer To Node each require a Transfer Destination. See [Table 11-2](#) to determine the type of destination, if any, to be programmed for the digit translation.

Table 11-2. *Transfer Destination Actions*

Action	Transfer Destination
Cancel Fax Selections	None
Company Directory - First Name	None
Company Directory - Last Name	None
End Fax Selections	None
Invalid	None
Select Fax By Document Number	None
Select Fax Document	Document number
Subscriber Access	None
Transfer To Collected Extension	None
Transfer To Extension	Extension number
Transfer To Mailbox	Mailbox number
Transfer To Node	Digit translation node number
Transfer To Operator	None
Hang Up	None

To program the Transfer Destination, use one of the following methods:

Method A

- a.) Select the current Value, then enter the new value in the text box.
- b.) Press **ENTER**. A screen appears displaying what is associated with the number entered.
- c.) Click **OK**. The new number appears in the field.

Method B

- a.) To change the destination, right-click **Transfer Destination** and choose **Change Transfer Destination**.
- b.) Select the desired destination type, then click **Next**. A list of fax documents, devices, or digit translation nodes that are present in the system appears.
- c.) Select the desired destination, then click **Finish**. The selected destination appears in the Transfer Destination field.

- **Override Language:** If this flag is enabled, the Call Routing Announcement application will use the application language (indicated below) for voice prompts. If the flag is disabled, the calling endpoint or trunk programmed language will be used whenever the application receives a call. By default, this flag is disabled. To enable it, select the check box. To disable it, clear the check box.
- **Language:** If Override Language is enabled, you can select the language from the list. This field now can be set to any specific language so that the system can support more than two languages. For more information, see “Language” on [page 6-18](#).

Using Digit Translation Nodes

Applies to BVM and EM voice processors only. A digit translation node can be used in one or more Call Routing Announcement application. This allows entire digit translation node trees to be shared or moved without reprogramming. There can be up to 200 digit translation nodes in the system.

Each digit translation node can have its own description, username, digit translation programming, and greetings. The digit translation node is assigned as a destination for a digit translation “Transfer To Node” Action. See [page 11-33](#). A digit translation node can only be deleted if it is not associated with a Call Routing Announcement application. Digit translation node programming is very similar to that for a Call Routing Announcement application. The programming fields are described in detail below.

To program a Digit Translation Node:

1. Select Voice Processor – Devices – **Digit Translation Nodes**.
2. Right-click in the right pane, and then click **Create Digit Translation**. The Create Digit Translation Node dialog box appears.
3. Enter the starting extension number and number of extensions, and then click **OK**. The Digit Translation Node appears in the node list.
4. *Optional.* In the Description column, type a description (up to 20 characters). This description is used in the mailbox directory and should be entered in the form “last name, first name” with a comma and space separating the names. Do **not** use Control characters in descriptions.
5. Double-click the new Digit Translation Node.
6. Program the Digit Translations as described on [page 11-33](#).
7. Program the Day and Greetings as described on [page 11-43](#).

Message Notification/Retrieval

Applies to BVM and EM voice processors only. The Message Notification/Retrieval (MNR) application is required for message notification, Remote Messaging, and Fax-On-Demand. You must create one (only) MNR application for the system to allow voice mail message notification and quick mailbox access.

Because the MNR application places outgoing calls for remote notification and Fax-On-Demand, it can have toll restriction classes of service. Fax-On-Demand is **not** available in BVM.

Programming MNR Classes of Service

To program the toll restrictions, double-click **Classes of Service**; you have the option of choosing **Day** or **Night**. Double-click the desired time period to view a list of current classes of service.

To add a class of service:

1. Right-click in the window and select **Add To List**.
2. A window appears that allows you to select the types of toll restrictions you want to program. Select **ARS Only & Deny Area/Office** and/or **Classes of Service**, then click **Next**.
3. Another window appears that shows you a list of available classes of service. You can view them in a list by selecting the List button or view details by selecting the Details button.
4. Select the desired class(es) of service, then select **Add Items**. The selected classes of service appear in the list. Click **Finish** to exit.
5. *(U.S. only)* If you selected *Deny Area/Office class of service*, the application must also be assigned to a user group. To change the user group, right-click **User Group** and select **Change User Group**. In the first window that appears, select **User Groups**, then click **Next**. In the next window, select the desired user group, then click **Finish** to exit and save the change.

Deleting MNR Classes of Service

To delete a class of service:

1. Select the item(s).
2. Right-click and select **Remove Selected Items**. To select a series of items, hold down **SHIFT** while selecting the first and last item in the range. To select two or more that are not consecutive, hold down **CTRL** while selecting the desired items.

Record-A-Call

Applies to BVM and EM voice processors only. This feature allows users to record an ongoing call and place it in a voice mailbox. When a user enters the Record-A-Call feature code, the system places a call to the endpoint assigned Record-A-Call application using the endpoint Record-A-Call mailbox. When the application answers, the system sets up a conference call. If programmed, the mailbox plays a greeting to indicate that the recording is in progress. There can be separate greetings for day and night modes. For information about using Record-A-Call for endpoints, see “Record-A-Call” on [page 11-38](#). For more information about the Record-A-Call feature, refer to the “System Features” chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

To enable Record-A-Call:

1. Select Voice Processor – Devices – **Record-A-Call**.
2. Right-click in the right pane, and then click **Create Record-A-Call**. The Create Record-A-Call dialog box appears.
3. Enter the starting extension number and number of extensions, and then click **OK**. The Record-A-Call extension appears in the node list.
4. *Optional.* In the Description column, type a description (up to 20 characters). This description is used in the mailbox directory and should be entered in the form “last name, first name” with a comma and space separating the names. Do **not** use Control characters in descriptions.
5. Click out of the field or press **ENTER** to save the change.

Scheduled Time-Based Application Routing (STAR)

Applies to BVM and EM voice processors only. STAR allows you to have applications with alternate greetings or different programming set up for holidays, weekends, and other scheduled events. Scheduled Time-Based Application Routing (STAR) allows you to have applications with alternate greetings or different programming set up for holidays, weekends, and other scheduled events.

A STAR application is basically a “routing table” for voice processor applications. When a direct ring-in call (from a trunk group or call routing table) rings in to a STAR application, it sends the call to another voice processor application, according to its programmed schedule. The caller is not aware of this transfer, but hears the programmed day or night greeting for the destination application. (The STAR application itself does not play a greeting.)

STAR can be used with any type of voice processor application except Auto Attendant Recall and Record-A-Call. You can even send calls from one STAR application to another, thereby “chaining” the applications together to increase the number of available schedules.

There can be as many STAR applications as desired, so long as the maximum limit for the number of voice processing applications is not exceeded. For more information and a sample STAR setup, refer to the Voice Processing chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

Programming STAR Schedules

Each schedule can have a description. To enter the description, select the current Value and then enter a description for the schedule, up to 20 characters. To program the remaining information for each schedule, double-click the schedule to display the following fields:

- **Application:** This is the extension number of the application that will be invoked when the time-based information in the table matches that of the incoming call. To assign the application, use one of the following methods:

Method A

- a. Select the current Value, and then enter the new value in the text box.
- b. Press **ENTER**. A screen appears displaying what is associated with the number entered.
- c. Click **OK**. The new number appears in the field.

Method B

- a. Right-click the current Value and select **Change Application**. A window appears prompting for the type to include.
 - b. Select the desired application, and then click **Next**. A list of applications appears. You can view them in a list by selecting the List button or view details by selecting the Details button.
 - c. Select the desired application, and then click **Finish**. The new value appears in the field. To view programming options, double-click the application.
- **Specific Date:** If you want the schedule to be active on a single day or for a period of days, enable this flag.

To enable this flag:

- a. Select the check box. The field changes to **Yes**. To disable the option, clear the check box.
- b. Click out of the field or press **ENTER** to save the change.

- **Start and Stop Date:** If the Specific Date field is set to **Yes**, use these fields to set the date(s) that this schedule will be active (such as a holiday).
 - a. Enter the date you want the schedule to begin in the **Start Date** box and the date you want it to end in the **Stop Date** box. To have the schedule active on only one day, set the Start and Stop Dates to the same day.
 - b. After entering information, click out of the field or press **ENTER** to save the changes.
- **Days of the Week:** If the Specific Date field is set to **No**, you can use these fields to determine which days of the week the schedule will be active.

To enable a specific day:

 - a. Select its check box to place a mark in it and change the setting to **Yes**. To disable the day, select the check box again to remove the mark and set it to **No**.
 - b. Click out of the field or press **ENTER** to save the changes.
- **Specific Times:** If you want the schedule to be active for a specific period of time on the selected day(s), enable this option.

To enable this option:

 - a. Select the check box. The field changes to **Yes**. To disable the option, clear the check box.
 - b. Click out of the field or press **ENTER** to save the change.
- **Start and Stop Time:** If the Specific Time field is set to **Yes**, use these fields to set time period that this schedule will be active (such as a after hours).
 - a. Enter the time you want the schedule to begin in the **Start Time** box and the time you want it to end in the **Stop Time** box.
 - b. After entering information, press **ENTER** or click another field to save the changes.
- **Day/Night Mode:** If the Specific Time field is set to **No**, you can use this field to determine whether the schedule will be active in day and/or night mode.

To change this field:

 - a. Select the option from the list.
 - b. Click out of the field or press **ENTER** to save the change.

Programming the Default STAR Application

The default application is where calls go that do not match any of the time-based criteria in tables 1–20.

To assign the application, use one of the following methods:

Method A

1. Select the current Value, then enter the new value in the text box.
2. Press **ENTER**. A screen appears displaying what is associated with the number entered.
3. Click **OK**. The new number appears in the field.

Method B

1. Right-click the current Value and select **Change Application**. A window appears prompting for the type to include.
2. Select the desired application, then click **Next**. A list of applications appears. You can view them in a list by selecting **List** or view details by selecting **Details**.
3. Select the desired application, then click **Finish**. The new value appears in the field. To view programming options, double-click the application.

Programming Automatic Fax Detection for STAR Applications

With Automatic Fax Detection, CRA applications can be programmed to automatically route incoming fax calls to a specified extension or to an e-mail address. CRA applications can detect fax tones during the greeting and up to timeout. However, the fax tone detection is disabled if the caller performs an action that removes them from the CRA, such as transferring to an extension, transferring to a mailbox, and so on.

NOTE EM requires a fax port license to detect fax tone.

The following two fields control the Automatic Fax Detection feature:

- **Fax Delivery Destination:** This field, if programmed, specifies the extension of the fax machine that will receive incoming faxes.
- **Fax Delivery E-Mail Address:** This field, if programmed, specifies the e-mail address of the account that receives incoming faxes. The fax is converted to a TIFF file and sent to the e-mail address as an attached file. The address can contain up to 127 characters. To view a message, use any TIFF file viewer, such as Imaging for Windows. If you enter an invalid character (: ; " \ | () , < > '), an error tone occurs.

If both fields are programmed with extension numbers, the fax tries delivery at the e-mail address. If all fax ports are unavailable, the fax goes to the extension specified in the Fax Delivery Destination field.

Voice Mail (Application)

Applies to BVM and EM voice processors only. The Voice Mail application handles all calls that are directed to voice mail by subscribers and non-subscribers, other than to the Message Notification/Retrieval application (see [page 11-37](#)). Callers hear the main company greeting, followed by a menu of available options. Endpoints can forward or transfer calls directly to their mailbox using this application extension number.

You can create up to 1,000 voice mail applications. With more than several hundred voice mail applications, the system will take longer to come up to the operational state. For instance, DB Programming may not be able to connect for 10–20 minutes until Call Processing and Voice Mail have acknowledged all of these applications. Also, system monitor dumps (performed through the Diagnostics Monitor app) may take a few minutes to complete. As a workaround, create these applications in local mode, then restore the database.

For more information about voice processing applications, refer to the Voice Processing chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

Voice Processing Application Options

Applies to BVM and EM voice processors only. After creating voice processing applications, you must program the options for each application. [Table 11-3](#) shows options you can program for voice processing applications.

Table 11-3. Voice Mail Application Programming Fields

Field	AA ¹	AAR	CRA	MNR	RAC	STAR	VM	Page
Digit Translation			✓					11-33
Greetings	✓		✓		✓		✓	11-43
Class of Service				✓				11-37
Attendant	✓	✓	✓	✓			✓	11-44
Auto Fax Detection – Fax Delivery Destination – Fax Delivery E-Mail Address			✓ ²					11-41
Music-On-Hold Parameters – Audio for Calls Camped onto this Device – Audio for Calls Holding for this Device – Audio for Calls Ringing this Device	✓	✓	✓	✓	✓	✓	✓	11-45
Time Slot Group	✓	✓	✓	✓	✓	✓	✓	11-45
Transfer Recall Destination	✓	✓	✓	✓			✓	11-45
Schedules						✓		
Default Application 1-20						✓		11-40
Automatic Speech Recognition (ASR) Enabled	✓	✓	✓	✓	✓	✓	✓	11-24
Automatic Speech Recognition (ASR) Setting	✓	✓	✓	✓	✓	✓	✓	11-24
Propagate Original Caller ID on Transfer	✓	✓	✓	✓	✓	✓	✓	11-46
Calling Party Name and Number	✓	✓	✓	✓	✓	✓	✓	11-46

1. Your Automated Attendant application may also require Extension ID programming for endpoints that do not have mailboxes.
2. If the system is running Basic Voice Mail, these fields are marked with a red "X."

Day and Night Greetings for Voice Processing Applications

Applies to BVM and EM voice processors only. When the application receives a call, a custom audiotex recording plays. For more information about creating audiotex recordings, refer to the *Mitel 5000 Endpoint and Voice Mail Administrator Guide*, part number 580.8001. You can select any greeting number for the Day and Night Greetings. The Day message is played when the system is in day mode, and the night message is played during night mode. The greetings can be changed or you can use the default greetings.

When used on Automated Attendants and CRAs, the greeting can include pauses and can announce queue position and time to wait using special audiotex selections. The special characters that can be used for programming greetings include the following:

- **Short Pause:** Inserts a 1-second pause.
- **Intermediate Pause:** Inserts a 5-second pause.
- **Long Pause:** Inserts a 10-second pause.
- **Position in Queue:** *(Used for hunt group Call Routing Announcements only.)* Tells the caller how many calls are waiting ahead of his or her call.
- **Time To Wait:** *(Used for hunt group Call Routing Announcements only.)* Tells the caller how long he or she can expect to wait, based on the number of calls waiting and the Average Call Length programmed for the hunt group.

To add or change a greeting:

1. Double-click **Day Greeting** or **Night Greeting** to view the current list of greetings.
2. *To add a greeting above an existing one*, select that greeting, right-click, and then select **Add To Day Greeting List** or **Add To Night Greeting List**.
To add to the end of the list, right-click in any blank area of the screen and then select **Add to Greeting List** or **Add To Night Greeting List**. A window appears prompting for the type to include.
3. Select **Audiotex Recording**, and then click **Next**. The list of Audiotex Recordings with details appears. To view items in a list only, click **List**.
4. Select the recording(s) and/or special characters or pauses you want to use, and then select **Add Items**. The selections appear in the list. When done, click **Finish**.

To move a greeting to another location in the list:

1. Double-click **Day Greeting** or **Night Greeting** to view the current list of greetings.
2. Drag and drop the greeting to the new position. Or, select the greeting to move and press **CTRL** + the up/down arrow to move the greeting up or down in the list.

To delete a greeting:

1. Double-click **Day Greeting** or **Night Greeting** to view the current list of greetings.
2. Select the greeting(s).
3. Right-click and select **Remove Selected Items**. To select a series of recordings, hold down **SHIFT** while selecting the first and last recordings in the range. To select two or more recordings that are not consecutive, hold down **CTRL** while selecting the desired greetings.

Attendants for Voice Processing Applications

Applies to BVM and EM voice processors only. An endpoint, hunt group, or other application can serve as the attendant endpoint for an application. This attendant will receive recalls when the Transfer Recall Destination does not answer or is unavailable.

To program the attendant for the application, use one of the following methods:

Method A

- a. Select the current value, and then enter the new value in the box.
- b. Press **ENTER**. A screen appears displaying what is associated with the number entered.
- c. Click **OK**. The new number appears in the field.

Method B

- a. Right-click **Attendant** and select **Change Attendant**. A window appears prompting for the type to include.
- b. Use the drop-down list box to scroll to **Keyset**, and then click **Next**. A list of endpoints with details appears. To view the items in a list only, click **List**.
- c. Select the desired endpoint, and then click **Finish**. The new attendant appears in the Attendant field. To view programming options, double-click the attendant.

Music-On-Hold for Voice Processing Applications

Applies to BVM and EM voice processors only. You can program the following audio options that callers hear when waiting for system users:

- Audio for Calls Camped onto this Device
- Audio for Calls Holding for this Device
- Audio for Calls Ringing this Device

For more information about these options, see “Device Audio for Calls Settings” on [page 7-65](#).

To program Music-On-Hold for applications:

1. Select Voice Processor – Devices – **Applications**.
2. Double-click the application.
3. Select the audio type.

Time Slot Group for Voice Processing Applications

Applies to BVM and EM voice processors only. You must program Time Slot Groups to specify the total number of voice channels available for each application for processing calls. See “Voice Processor System Settings” on [page 11-16](#).

To select the Time Slot Group for the application:

1. Select Voice Processor – Devices – **Applications**.
2. Double-click the application.
3. Right-click **Time Slot Group**, and then select **Change Time Slot Group**. A window appears prompting for the type to include.
4. Select **Time Slot Group**, and then click **Next**. A list of time slot groups with details appears. To view items in a list only, click **List**.
5. Select the desired group, and then click **Finish**. The new time slot group appears in the field. To view programming options, double-click the time slot group.

Transfer Recall Destination for Voice Processing Applications

Applies to BVM and EM voice processors only. This is the endpoint, hunt group, or application that receives any calls that recall after being transferred by the application. For the Auto Attendant, this is usually the Automated Attendant Recall application.

To select the Transfer Recall Destination for the application, use one of the following methods:

Method A

1. Select Voice Processor – Devices – Applications – *<application>* – **Transfer Recall Destination**.
2. Select the current value, and then enter the new value in the text box.
3. Press **ENTER**. A screen appears displaying what is associated with the number entered.
4. Click **OK**. The new number appears in the field.

Method B

1. Select Voice Processor – Devices – Applications – *<application>*.
2. Right-click **Transfer Recall Destination** and select **Change Transfer Recall Destination**. A window appears prompting for the type to include.
3. Select **Auto Attendant Recall** or your desired destination, then click **Next**. A list of Auto Attendant recall applications appears. You can view them in a list by selecting the List button or view details by selecting the Details button.
4. Select the desired application, then click **Finish**. The new destination appears in the Transfer Recall Destination field. To view programming options, double-click **Transfer Recall Destination**.

Automatic Speech Recognition (ASR) Setting

Applies to BVM and EM voice processors only. Determines whether the system uses the ASR Enabled setting in the current folder level or in the next folder level. See “Automatic Speech Recognition Settings” on [page 11-23](#).

Automatic Speech Recognition (ASR) Enabled

Applies to BVM and EM voice processors only. Determines whether ASR is enabled for the current folder, as well as any subfolders or parent folders based on the ASR Setting field. See “Automatic Speech Recognition Settings” on [page 11-23](#).

NOTE

The ASR Enabled field is ignored (that is, displays a red “X”) if the ASR Setting is set to Delegated, Ignored, or Ignored and Delegated.

Propagate Original Caller ID on Transfer

Also applies to SIP voice mail applications. When this option is enabled, if the endpoint is on a call with an outside trunk that had caller ID information, the application propagates the caller ID when a voice mail application transfers a call to an endpoint and the endpoint performs a transfer back to the PSTN. To propagate the caller ID to the PSTN, the eventual trunk must be ISDN and the “Propagate Original Caller ID” flag in its CO trunk group must be set to **Yes**. The default of this flag is set to **Yes** (which means propagate caller ID on transfer PSTN calls). The application must be able to perform transfers (for example, Auto Attendant, Auto Attendant Recalls and Call Routing Announcements).

To propagate caller ID when a Voice Mail application transfers a PSTN call:

1. Select Voice Processor – Devices – Applications – **<application>**.
2. Set the **Propagate Original Caller ID on Transfer** flag to **Yes**.
3. Press **ENTER** or click another field to save the change.

Calling Party Name and Number

You can enable the Calling Party Name and Calling Party Number features for voice processing applications. For feature descriptions, see “Calling Party Name” on [page 7-63](#) and “Calling Party Number” on [page 7-64](#).

1. Select Voice Processor – Devices – Applications – **<application>**.
2. Select **Calling Party Name** or **Calling Party Number**.
3. In the **Value** column, select the current value, and then type the name in the box.
4. Click out of the field or press **ENTER** to save the change.

Extension IDs

Applies to BVM and EM voice processors only. Extension IDs provide the Auto Attendant application with a means for transferring calls to extensions and off-node devices that do not have mailboxes. An extension ID allows the owner to record a name for the directory and establish a password. Extension IDs can be created for endpoints, hunt groups, modems, and applications. To create a mailbox for an extension that currently has an extension ID, first delete the extension ID, then create the mailbox. Extension IDs cannot be created for off-node device wildcard extensions.

To create an Extension ID:

1. Right-click in any area of the screen and select **Create Extension ID**. A window appears prompting for the device type to include.
2. Select the device type, and then click **Next**. The list of devices appears. You can view them in a list by selecting **List** or view details by selecting **Detail**.
3. Select the devices for which you want to create IDs.
4. Select **Add Items**. The selections appear in the mailbox list. (You can use the SHIFT or CTRL keys to select more than one item.)
5. Click **Finish** to exit.

To delete an Extension ID:

1. Select the IDs.
2. Right-click, and then select **Delete**.

Extension ID programming includes the following fields:

- Allow Transfer Method Programming
- Auto Attendant Transfer Prompt
- Unlisted Number
- Private Extension
- Password
- Transfer Method

To program an Extension ID: The description and username fields cannot be changed. They are programmed as part of device programming.

- *Allow Transfer Method Programming:* Determines whether the extension ID user (or the voice mail System Administrator) will be allowed to change the Transfer Method, using the voice mail Personal Options prompts.
 - a. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
 - b. Click out of the field or press **ENTER** to save the change.
- *Auto Attendant Transfer Prompt:* Determines whether the transfer prompt ("Please hold while your call is being transferred to...") plays after a caller has entered the extension number of the endpoint associated with this extension ID. This applies to calls transferred by Automated Attendant and Call Routing Announcement applications, including transfers to the operator's mailbox or extension ID.
- *To disable the prompt:*
 - a. In the **Value** column, clear the check box. The field changes to **No**. To enable the option, select the check box.
 - b. Click out of the field or press **ENTER** to save the change.

- *Unlisted Number/Private Extension:* Unlisted numbers are not included in the directory, but can be dialed if the caller knows the extension number. Private numbers can be dialed, but only the name is played in the directory.
 - a. In the **Value** column, select the check boxes to enable the options. The fields change to **Yes**. To disable the options, clear the check boxes.
 - b. Click out of the field or press **ENTER** to save the change.
- *Password:* To program a password for the Extension ID:
 - a. Right-click the Password field and select **Edit Password**. The Edit Password dialog box below appears.
 - b. In the **New Password** box, type the new password (up to 12 digits, using digits 0–9). Typed characters appear as asterisks (***)
 - c. Retype the password in the Confirm Password box.
 - d. Click **OK** to exit and save the password. If the entered passwords match, you will return to the Password field. If they do not match, you must re-enter the new password and verify it again. If you make a mistake while entering the password or want to leave it unchanged, select **Cancel**.

NOTE

To provide system security, *all* extension IDs should have a password. To make the passwords difficult to guess, they should **not** match the mailbox number or consist of one digit repeated several times.

- *Transfer Method:* Determines how transfers will be made to this extension ID. The options are: Announce Only, Screened, and Unannounced. (Defaults to Unannounced.) For more information, refer to the “Voice Processing Features” chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.
 - a. Select the option from the list.
 - b. Click out of the field or press **ENTER** to save the change.

Group Lists

Applies to BVM and EM voice processors only. Voice Mail group lists can be used by any subscriber for sending messages to several mailboxes simultaneously. There can be up to 1000 group lists per node and up to 1500 members per group list.

Creating a Group List

To create a Group List:

1. Select Voice Processor – Devices – **Group Lists**.
2. Right-click anywhere in the right pane. The Create Group List Extension dialog box appears.
3. Enter the Group List number, and then click **OK**.
4. Type a description of up to 20 characters in the Description text box.
5. Type a name of up to 10 characters in the Username text box. This is the name that will appear on endpoint displays. Do **not** use slash (/), backslash (\), vertical slash (|) or tilde (~) characters in usernames. Do **not** use control characters in descriptions or usernames.

Changing a Group List Extension Number

To change a Group List Extension number:

1. Select Voice Processor – Devices – **Group Lists**.
2. Type the desired number in the text box *or* use the arrow to scroll to an available number. If you attempt to enter an invalid number, a number that conflicts with an existing extension, or a number that is already assigned, you will see a warning window that allows you to fix the error. Type a new number, and then click **OK** to continue.
3. Press **ENTER** or click another field to save the change.

Adding Mailboxes to Group Lists

To determine the mailboxes that will be included in the Group List, double-click the Group List entry. The current list of mailboxes appears in the right screen.

To add a mailbox to the Group List:

1. Select Voice Processor – Devices – **Group Lists**.
2. Right-click in any area of the screen and select **Add To List**. A window appears prompting for the type to include.
3. Select **Mailbox** and/or **Off-Node Mailbox**, and then click **Next**. The list of mailboxes appears. You can view them in a list by selecting the **List** button or view details by selecting the **Details** button.
4. Select the mailboxes you want to add, then select **Add Items**. The selections appear in the list.
5. Click **Finish** to exit.

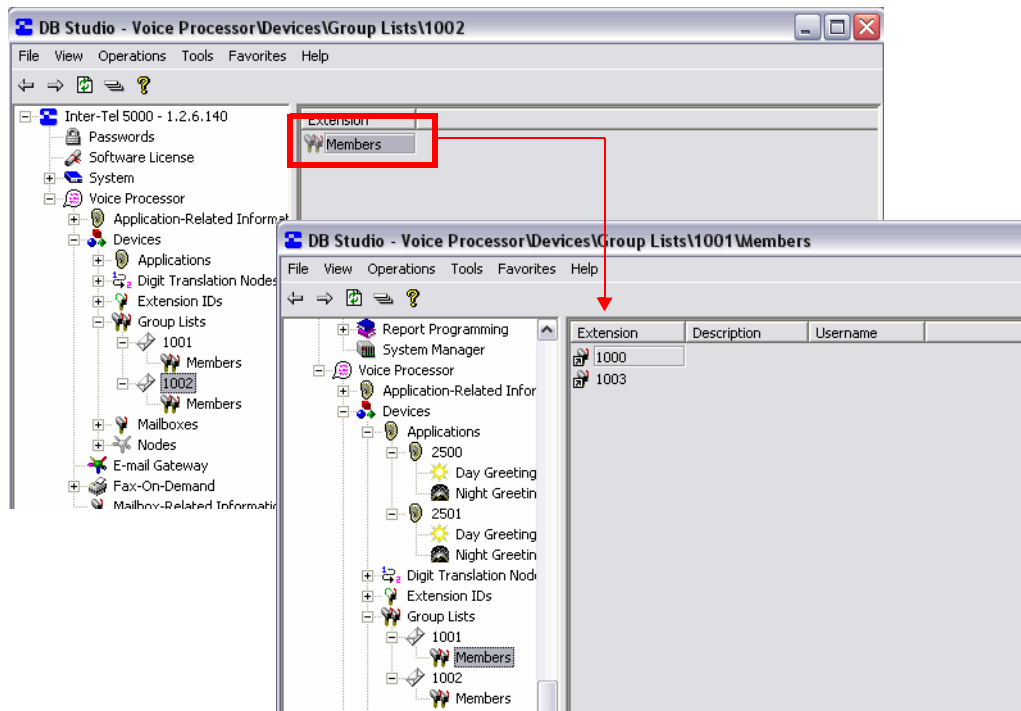
Removing Mailboxes from Group Lists

To remove a mailbox from the list:

1. Select Voice Processor – Devices – **Group Lists**.
2. Select the mailboxes that you want to remove.
3. Right-click and select **Remove Selected Items**. The information is automatically removed from the list. To select a series of mailboxes, hold down **SHIFT** while selecting the first and last mailboxes in the range. To select two or more that are not next in consecutive order, hold down **CTRL** while selecting the desired mailboxes.

Viewing Group List Members

Instead of the members of a group list being displayed directly in the individual group list, the members reside in a separate folder called Members, as shown in the following two illustrations.



Audiotex Recordings

Applies to BVM and EM voice processors only. Audiotex recordings are custom recordings used by voice processing applications. Audiotex recordings are recorded using an endpoint and the voicemail administrator mailbox. For more information about creating and changing Audiotex recordings, refer to the *Mitel 5000 Endpoint and Voice Mail Administrator Guide*, part number 580.8001.

The recording length is shown in seconds for reference only. You cannot change the recording time.

NOTE

You can view recording information (recording number, description, and recording length) for audiotex recordings that have been re-recorded.

To change the description of a recording:

1. Select – Voice Processor – Application-Related Information – **Audiotex Recordings**.
2. Click once on the current description.
3. Type the new description in the box, using up to 20 characters. If desired, you can right-click in the box and cut, paste, copy, or delete the description.
4. Click out of the field or press **ENTER** to save the change.
5. When the current description is selected in the text box, right-click and select the desired operation.

Voice Mail Directory

Applies to BVM and EM voice processors only. The following options enable or disable the voice mail directory and determine the directory sort order.

Enabling or Disabling the Voice Mail Directory

If you enable the Voice Mail Directory, the system allows anyone routed or answered by voice mail or any mailbox users while in their mailbox to be presented with the directory option. If the flag is disabled, the voice mail will not prompt the caller for the directory option while in the voice mail areas (non AA or CRA).

NOTE

If the voice mail mailbox directory is disabled, callers using the voice mail system do **not** receive a system prompt giving the option to search the directory for the person to whom they want to speak. If the caller presses the dialpad button normally associated with access to the mailbox directory, the caller is informed that the selection is invalid.

To enable the Voice Mail Directory:

1. Select – Voice Processor – Application-Related Information – **Voice Mail Information**.
2. Select **Enable Voice Mail Directory**.
3. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
4. Click out of the option or press **ENTER** to save the change.

Changing the Voice Mail Directory Sort Order

This option is for voice mail calls only. You can change the directory sort order, or whether the directory searches by subscribers' first or last names. The Directory Search Order also determines which system voice prompt plays (first or last name) when directing callers to spell a name. To change the Auto Attendant Sort Order, see "Auto Attendant Directory Sort Order" on [page 11-30](#).

To change the Directory Sort Order:

1. Select – Voice Processor – Application-Related Information – **Voice Mail Information**.
2. Select **Directory Sort Order**.
3. From the **Value** column, select the option from the list.
4. Click out of the option or press **ENTER** to save the change.

Voice Processor Timers and Limits

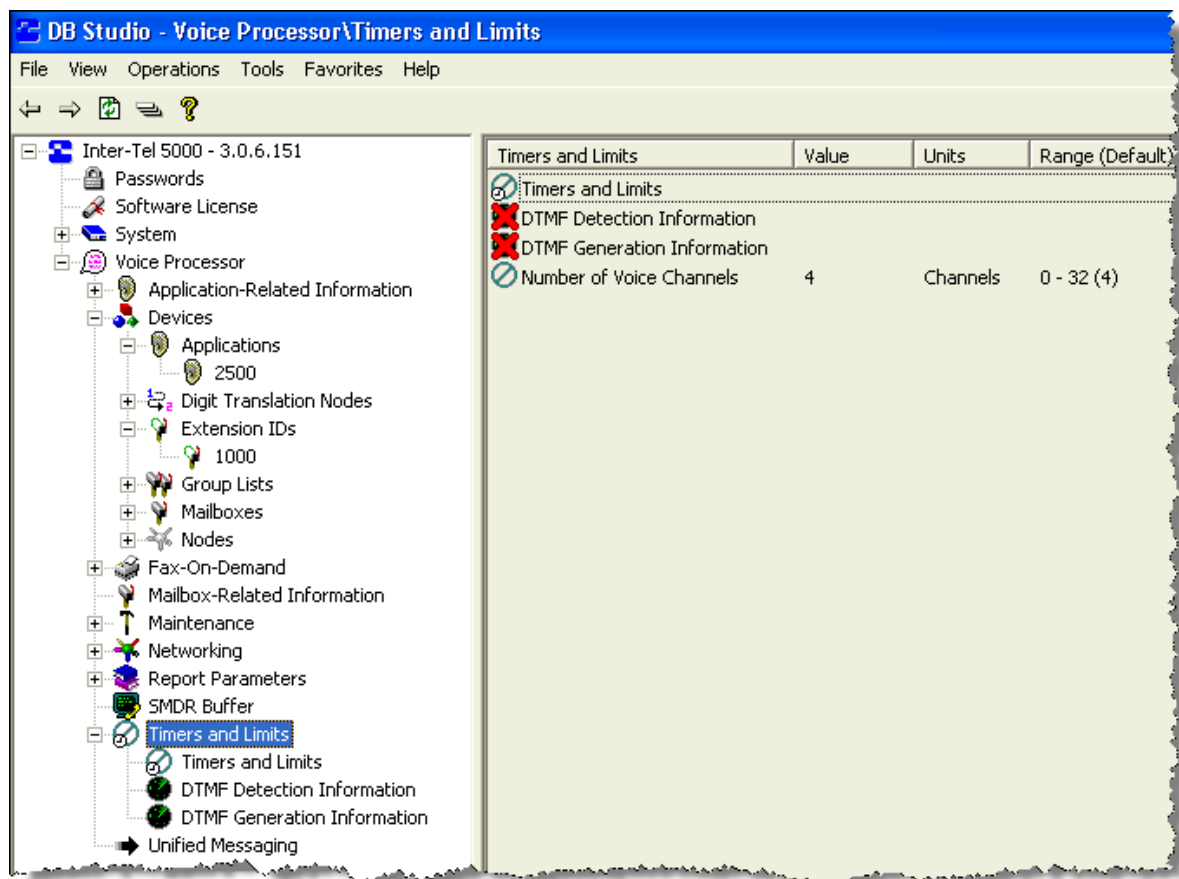
Programmable timers and limits control various Voice Processor functions. The timers and their default values, programmable ranges, and purposes are described in the following paragraphs. The default values have been selected to ensure correct operation under most circumstances. Occasionally, one or more of the timers may need to be adjusted.

The Number of Voice Channels for BVM is programmed in the Voice Processor Timers and Limits folder.

The Timers and Limits folder contains the following programming areas:

- “Timers and Limits” on [page 11-13](#)
- “DTMF Detection Information” on [page 11-57](#)
- “DTMF Generation Information” on [page 11-59](#)
- “Number of Voice Channels” on [page 11-60](#)

Figure 11-3. Voice Processor Timers and Limits



Programming BVM Timers and Limits

To view the list of current values for the Voice Processor, select **Timers and Limits**.

To program a timer or limit:

1. Select Voice Processor – **Timers and Limits**.
2. Double-click **Timers and Limits**.
3. In the **Value** column, click the current value, and then type or select the new value.
4. Click out of the field or press to **ENTER** save the change.

Table 5-36 shows the system-wide timers and limits that can be programmed for the Voice Processor.

Table 11-4. Voice Processor Timers and Limits

Timer	Default	Range	Defines
Busy Tone Cycle Detect	2 cycles	1–60 cycles	The minimum number of cycles of tone the system needs to recognize busy, Do-Not-Disturb, or reorder tones. When the voice processor does not recognize one of these tones, it will assume the call is answered. This timer is not supported in Enterprise Messaging (EM).
Call-in-Progress Dial Tone	2 sec	0–5 sec	The minimum duration of continuous dial tone that the voice processor can recognize during an active call (for example, when a caller hangs up while connected to the voice mail application). To disable dial tone detection on active calls, set this timer to 0. This timer is not supported in EM.
Call Progress Delay	6000 msec	1–60000 msec. (0.001–60 sec.)	The maximum length of time the voice processor will wait before checking call status when placing a call. It must be set long enough to prevent the voice processor from detecting dial tone on the outgoing call. This timer is not supported in EM.
Call Progress Detection	4000 hundredths	1-6000 hundredths (0.01–60 sec.)	The maximum length of time the voice processor will wait for a call to be answered before aborting the attempted call. If it detects anything other than silence during this time, the system will consider the call answered. This timer is not supported in EM.
Deleted Message Hold Duration	1 hour	0–24 hours	The amount of time that the voice processor will keep each deleted message. The duration is specified in hours and is based on the time the user deletes the message. For example, if the Deleted Message Hold Duration is set to 6 hours, and a user deletes a message at 9:22 AM, the voice processor will keep the message until 3:22 PM. A value of 0 means that the voice processor will not hold messages. (That is, as soon as the user deletes the message, it is permanently deleted and there is no way to restore it).
Dialed Pause Duration	300 hundredths	1–500 hundredths (0.01–5 sec.)	The duration of the pauses dialed by the voice processor as part of feature codes, numbers, and outgoing dialing strings. This timer is not supported in EM.

Table 11-4. Voice Processor Timers and Limits (Continued)

Timer	Default	Range	Defines
Maximum Deleted Message Space	0 MB	0–20 MB	<p>The maximum amount of space that the voice processor allocates to store deleted messages. The deleted message storage size is specified in megabytes (MB) of the hard disk. When a user deletes a message, and the deleted message queue size exceeds this number, the voice processor will purge the oldest message to make room for the new one. In this case, the voice processor will purge as many messages from storage as necessary to make room for the new one. However, if the hard disk becomes full, the voice processor will immediately purge all stored messages.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>NOTE When Voice Processing is shut down, all deleted messages are permanently deleted and cannot be restored.</p> </div>
Maximum Greeting Length	1 min	1–15 min	The maximum time allowed for all mailbox greetings and custom audiotex recordings.
Maximum Number of Deleted Messages	0 messages	0–9999 messages	The maximum number of deleted messages that the voice processor will store. If this number is exceeded, and a user deletes a message, the voice processor will remove the oldest message in storage to make room for the new one. (Entering a value of 0 means that the number is unlimited.) However, this limit is bound to the availability of hard disk space as specified by the Maximum Deleted Message Space above. That is, the Maximum Deleted Message Space limitation will take precedence over this one.
Maximum Outgoing Calls	2 calls	1–number of available ports (max 32)	The number of outgoing message notification and fax delivery calls that can be made at one time by the Message Notification/Retrieval application. Note that the number of calls that can be made are also limited by the availability of intercom voice channels and outgoing trunks.
Minimum Call Progress Silence Duration	15 hundredths	1–21 hundredths (0.01–0.21 sec)	<p>The minimum duration of a period of silence necessary for the voice processor to detect silence. That is, if a period of sound is broken by silence, and the silence is shorter than this timer, the voice processor will ignore the silence. This timer applies to outgoing remote notification calls only.</p> <p>This timer is not supported in EM.</p>
Minimum Call Progress Signal Duration	18 hundredths	1–18 hundredths (0.01–0.18 sec)	<p>The minimum duration of a period of sound necessary for the voice processor to detect sound. That is, if a period of silence is broken by a burst of sound on the line, and that sound is shorter than this timer, the voice processor will ignore the sound. This timer applies to outgoing remote notification calls only.</p> <p>This timer is not supported in EM.</p>

Chapter 11: Voice Processor System Programming

Voice Processor Timers and Limits

Table 11-4. Voice Processor Timers and Limits (Continued)

Timer	Default	Range	Defines
Notification No-Answer Detection	4 rings per prompt iteration	1–25 rings 1–5 prompt iterations (automatic)	The number of rings the voice processor waits to deliver a remote message before trying to access an Alternate Notification mail box. Automatically sets the number of times, or iterations, the Primary and Alternate Notification Cascades are tried. Sets the iterations equal to the ring Value up to 4. Ring Value settings 5–25 do not exceed 5 iterations.
Off-hook Delay	0 seconds	0–5 seconds	Length of time the voice processor should wait after coming off hook before playing the first prompt. However, the recommended minimum setting is 1 second to allow a pause before the prompts are played for outside callers, thereby assuring that no text is cut off. It is set to 0 to allow internal callers to hear the prompts immediately. This timer is not supported in EM.
Outgoing DTMF Digit Duration	60 msec	30–250 msec (0.030–0.250 sec)	Length of the DTMF tones (and inter-digit pauses) that are sent during remote notification to a pager or personal number. If this timer is changed, the PC must be reset. This timer is not supported in EM.
Pause Voice Mail	30 sec	1–240 sec	The maximum amount of time that the voice processor will pause during the playback of a message or recording. This timer is not supported in EM.
Record-A-Call Max Message Length	30 min	1–600 min	The maximum time allowed for Record-A-Call input to a mailbox. (This overrides the mailbox's maximum message length setting. However, if a Record-A-Call message exceeds the maximum message length, the mailbox will be considered full until that Record-A-Call message is deleted.)
Recording Beep Length	700 ms	100–2000 ms	The length of the tone played to indicate that recording has started.
Recording Beep Level	-20 dBm0	-63 to 0 dBm0	The level dBm0 of the tone played to indicate that recording has started.
Recording Silence Detection	5 sec	0–30 sec	Length of silence required to terminate a recording. If silence in recording exceeds this timer, the recording will automatically end. If lengthy (silent) pauses are included in any recordings, this timer should be adjusted to allow them.
Recording Silence Threshold	-38 dBm0	-40 to -20 dBm0;	Audio recorded below this level is considered silence by the system for the purposes of the recording silence detection timer.
Relay Forward/Rewind Increment	5 sec	1–60 sec	The number of seconds a message or recording will be advanced or backed up when a user skips ahead or backward during a replay.
Shortest Message Allowed	3 sec	1–5 sec	Length of the shortest message that will be accepted by the voice processor. (Messages terminated with # are always allowed, regardless of length.)
Transfer No-Answer Detection	4 rings	1–25 rings	The number of rings during which the voice processor will wait for a transferred call to be answered. Establishes the duration required for call-screening.

DTMF Detection Information

Applies to BVM only. In most installations, you should not need to change the DTMF detection information. However, if the voice processor is losing digits or if DTMF detection is causing talk-off, you may need to adjust the DTMF filter parameters. If digits are not being detected properly, there are three possible reasons:

- **The “twist” is not within the allowed range:** The Twist parameters specify the maximum acceptable difference between the high frequency energy and the low frequency energy. One frequency can be much stronger than the other, or the frequencies can be off the nominal values. If the frequencies are off, measurements made at the nominal values can show different readings because the peak will be at a different frequency. In some cases, noise or voice on the line can add to or subtract from these frequencies.
- **There is too much noise:** Noisy lines can introduce distortion to the digits. A simple inspection can identify if the lines have too much noise. If this is the case, Twist parameters should be increased and Ratio parameters should be decreased so that digits can be detected even when stronger noise and other signals exist.
- **Another signal is present that is similar to the DTMF digit:** Other signals present on the line, including some types of voice, can be detected as DTMF tones causing “talk-off.” Adjusting the DTMF Detect and DTMF Delay parameters may correct this problem. However, changing the DTMF Digit Delay or DTMF Digit Detection timer values is a trade-off between improving DTMF detection and increasing the possibility of talk off. As the values of the timers are reduced, DTMF detection is improved, but the possibility of talk off increases. As the value is increased, the possibility of talk off is reduced, but the possibility of DTMF detection problems is increased.

You can adjust DTMF filter parameters to improve performance when the DTMF detection is not performing as desired. The filter parameters have one set of values when a recording is being played (Play Mode) and another set during all other functions (Idle Mode).

NOTE

If you change the DTMF parameters, the new parameters do not take effect until the voice processor is completely idle.

When digits are lost both in Play and Idle modes, the duration of the digits and the intervals between them may be too close to the DTMF Delay and DTMF Detection values. You should decrease these values to improve the chances that the digit characteristics will remain within acceptable values during the minimum required duration. Once the minimum on and off times are set according to the pattern of the digits being dialed, the next step is to verify the twist. A spectrum analyzer can show the amplitude for the frequencies in the signal, and the values shown can be compared to the twist limits set in the driver. Rhetorex has a utility called “FFT” that will show the basic characteristics of the signal, including frequencies and amplitudes. Increasing the twist parameters for both Play and Idle modes will usually solve the problem.

When digits are lost only in Play mode, the Twist parameters should be increased and Ratio parameters should be decreased for Play mode only.

If talk-off is occurring, increasing the minimum duration of the digits should suffice. If this is not possible due to other constraints (for example., Speed Dial), Twist and Ratio parameters should be changed to make the filters less tolerant.

To program a parameter:

1. Select Voice Processor – **Timers and Limits**.
2. Double-click **DTMF Detection**.
3. Select the parameter. Parameter definitions begin on [page 11-58](#).
4. In the **Value** column, select the new parameter from the list.
5. Press **ENTER** or click another field to save the change.

Parameter definitions are as follows:

- **DTMF Digit Detect On:** Determines the minimum duration of DTMF tones that can be recognized by Voice Processing during Play Mode; for example, when a prompt or message is playing. Valid settings for this parameter are 32, 48, 64, 80, or 96 milliseconds (msec). The default is 48 msec.
- **DTMF Digit Detect Off:** Determines the minimum silence allowed between DTMF tones that can be recognized by Voice Processing during Play Mode. Valid settings for this parameter are 32 or 48 msec. The default is 48 msec.
- **DTMF Digit Delay On:** Determines the minimum duration of DTMF tones that can be recognized by Voice Processing during Idle Mode; for example, when Voice Processing is waiting for input. Valid settings for this parameter are 32, 48, 64, 80, or 96 msec. The default is 32 msec.
- **DTMF Digit Delay Off:** Determines the minimum silence allowed between DTMF tones that can be recognized by Voice Processing during Idle Mode. Valid settings for this parameter are 32 or 48 msec. The default is 48 msec.
- **DTMF Digit Low To High Twist (Play and Idle):** Reflects the difference between the DTMF digit high frequency and low frequency energy (high minus low). To allow the Voice Processor to detect a digit that consists of frequencies, the high frequency energy cannot be stronger than the low frequency energy by more than the setting of this parameter. In Play Mode the default for this parameter is 9.2dB. In Idle Mode the default is 8.2dB. Valid settings for this parameter are: No Limit, 6.7dB, 8.2dB, 9.2dB, 10.7dB, 12.7dB, 15.2dB, or 18.2dB.
- **DTMF Digit High To Low Twist (Play and Idle):** Reflects the difference between the DTMF digit low frequency and high frequency energy (low minus high). To allow the Voice Processor to detect a digit that consists of frequencies, the low frequency energy cannot be stronger than the high frequency by more than the setting of this parameter. In Play Mode the default for this parameter is 8.2dB. In Idle Mode the default is 5.2dB. Valid settings for this parameter are: No Limit, 4.2dB, 5.2dB, 6.7dB, 8.2dB, 10.2dB, 13.2dB, or 18.2dB.
- **DTMF Digit In To In Ratio (Play and Idle):** Indicates the digit energy minus the energy of the next digit. In order for the Voice Processor to detect a digit that consists of frequencies, the digit energy must be stronger than the energy of the next digit by the amount of this parameter setting. The default setting for Play Mode is 2.0dB. The default setting for Idle Mode is 8.0dB. Valid settings for this parameter are 1.0dB, 2.0dB, 3.0dB, 4.0dB, 6.0dB, 8.0dB, 9.0dB or 10.0dB.
- **DTMF Digit In To Out Ratio (Play and Idle):** Indicates the digit energy minus the noise energy. For the Voice Processor to detect a digit that consists of frequencies, the digit energy must be stronger than the noise energy by at least the amount of this parameter setting. The default setting in Play Mode is 1.0dB. In Idle Mode, the default is 4.0dB. Valid settings for this parameter are 0.5dB, 1.0dB, 2.0dB, 3.0dB, 3.5dB, 4.0dB, 4.5dB, or 5.0dB.
- **DTMF Frequency Deviation:** This is the maximum variance from the standard frequencies allowed for valid DTMF. The range is 1.5%–2.5% (.1%); the default is **1.8%**.
- **DTMF Maximum Valid Tone Dropout Time:** An otherwise valid tone may include this much silence and still be detected as valid DTMF. (Applies everywhere except during recording.) The range is 0–260 ms; the default is **15** ms.
- **DTMF Minimum Level Threshold:** This is the minimum per-frequency power for valid DTMF. The range is -14 dBm0 to -48dBm0; the default is **-25.0** dBm0.
- **DTMF Minimum Valid Tone Off Time:** This is the minimum period of silence required between successive DTMF tones. The range is 20–260 ms; the default is **40** ms.
- **DTMF Minimum Valid Tone On Time:** This is the minimum length of a valid DTMF tone. The range is 20–260 ms; the default is **40** ms.
- **DTMF Negative Twist:** This is the maximum amount of negative twist allowed for valid DTMF. The range is 1 dB–16 dB; the default is **8.0** dB.

- **DTMF Positive Twist:** This is the maximum amount of positive twist allowed for valid DTMF. The range is 1 dB–16 dB; the default is **4.0** dB.
- **Recording - DTMF Minimum Valid Tone On Time:** This is an existing field. The field name changed from “DTMF Digit Detect for Recording - On (msec.)” The range is 20–260 ms; the default is **40** ms.
- **Recording - DTMF Minimum Valid Tone Off Time:** This is an existing field. The field name changed from “DTMF Digit Detect for Recording - Off (msec.)” The range is 20–260 ms; the default is **40** ms.
- **Recording - Maximum Valid Tone Dropout Time:** An otherwise valid tone may include this much silence and still be detected as valid DTMF. (Applies only during recording.) The range is 0–260 ms; the default is **15** ms.

DTMF Generation Information

The DTMF Generation folder contains the following information:

- **DTMF High Frequency Level:** This is the power level at which the high (“column”) frequency component of DTMF tones is generated. The range is -63 to 0 dBm0; the default is -6 dBm0.
- **DTMF Low Frequency Level:** This is the power level at which the low (“row”) frequency component of DTMF tones is generated. The range is -63 to 0 dBm0; the default is -6 dBm0.
- **DTMF Tone On Time:** This is the length of generated DTMF tones. The range is 40–260 ms; the default is 80 ms.
- **DTMF Tone Off Time:** This is the length of the silence period between successively generated DTMF tones. The range is 40–260 ms; the default is 80 ms.

To program DTMF Generation parameters:

1. Select Voice Processor – **Timers and Limits**.
2. Double-click **DTMF Generation Information** – *<option>*.
3. In the **Value** column, select the option from the list.
4. Click out of the field or press **ENTER** to save the change.

Number of Voice Channels

Applies to BVM and EM voice processors only. Voice channels allow communication between the system and the applications. If a voice channel is not available in the application time slot group, callers to that application receive busy signals and the call recalls to the application attendant. At default, there are four available voice channels. The actual number of voice channels may be higher or lower depending on the number of Voice Processing circuit cards used in the external voice processing system and the port configuration of the cards.

The number of available voice channels determines the maximum number of channels that can be assigned to any single Time Slot Group. The combined total of channels assigned to Time Slot Groups may exceed the actual number of voice channels because it is unlikely that all time slot groups will use their maximum allotment at the same time.

NOTES

Although DB Programming allows you to configure 64 voice mail ports, Voice Processing using the Windows-based platform currently supports a maximum of only 32 ports. Attempting to configure 64 voice mail ports may cause serious performance issues.

This field is not programmable in remote mode when connected to an EM voice processor.

Because BVM ports are licensable, customers upgrading their port capacity are required to purchase the corresponding licenses.

To set the number of voice channels (1–64):

1. Select Voice Processor – Timers and Limits – **Number of Voice Channels**.
2. In the **Value** column, click the current value, and then type the new value.
3. Click out of the field or press to **ENTER** save the change.

When using BVM, DB Programming displays the Number of Voice Channels field as read-only. This is because the number of channels and ports allocated for BVM are synonymous. Therefore, when you change the BVM port allocation field, the Number of Voice Channels field automatically updates with the port allocation value.

However, if you are using an external voice mail system, the Number of Voice Channels field remains writable and retains its previous functionality. After the BVM port resources are changed to 0, the number of voice channels and the maximum channel allocation fields for the time slot groups are no longer dependent on the value in the Number of Voice Channels field. By breaking this dependency, the system allows the customer to convert from a BVM system to an external type of voice mail system without having to reprogram time slot groups.

The range of values in the Number of Voice Channels field is 0–16. The default value is 4. The Number of Voice Channels field is programmable for BVM in local mode but is read-only in remote mode. This field is also **not** programmable in remote mode when the Mitel 5000 platform is connected to an EM voice processing system.

Unified Messaging with EM Options

Applies to EM systems only. If the folder is selected for other voice processor types, a warning appears and all the fields appear with a red “X.”

For complete information about Unified Messaging OSE, refer to the latest version of the *Unified Messaging Open Standards Edition Administrator's Guide*, part number 835.3162.

To program the Unified Messaging fields:

1. Select Voice Processor – **Unified Messaging**.
2. Configure the following fields:
 - **Attachment Format for Inbound Faxes:** Indicates the format of fax attachments in e-mails sent for Inbound faxes. The available options are TIF or PDF. It is set to TIF by default.
 - **Enable Delivery of Incomplete/Failed Inbound Faxes:** Enables e-mail notification for fax receivers regarding failed or incomplete inbound faxes. It is set to No by default.
 - **Enable IMAP Login for EM Server:** Enables remote IMAP logins to the EM server. It is set to No by default.
 - **EM Server IMAP Connection Timeout:** Determines the maximum duration that the Em server will wait for a remote IMAP connection to be established. The range is 30–1440 minutes; the default is set to 30 minutes.
3. Click out of the field or press **ENTER** to save the change.

E-Mail Gateway

The following sections describe programming fields and procedures required to convert e-mail messages to voice mail messages with both EM and BVM systems.

For a complete explanation of the E-Mail Gateway feature, refer to the *Unified Messaging v2.3 Administrator's Guide* (part no. 835.3164), or *Unified Messaging Open Standards Edition Administrator's Guide* (part no. 835.3162). Program the E-Mail System field first, as described below.

To use the text-to-speech (TTS) functionality to convert e-mail messages to voice mail messages, the E-mail Gateway must be configured and each mailbox user must have an e-mail reader profile. This profile contains the information that EM requires to access the correct e-mail server and e-mail account.

E-Mail Gateway Programming Options

The following sections describe E-Mail Gateway options and instructions. [Table 11-5](#) shows system features that use E-Mail Gateway fields. Empty fields may be programmed depending on the SMTP server configuration.

NOTE

Remember to identify the E-Mail System first to determine the other fields that need to be programmed.

Table 11-5. *E-Mail Gateway Fields Used for System Features*

E-Mail Gateway Field	System Health Report	Forward to E-Mail	VPIM	Unified Messaging
"Administrator E-Mail Address" on page 11-63		Recommended		
"E-Mail Address" on page 11-63				
"E-Mail Real Name" on page 11-63				
"E-Mail SMTP Port" on page 11-64				
"E-Mail SMTP Server" on page 11-64	Required	Required for EM and BVM	Required for EM and BVM	Required for EM
"E-Mail System" on page 11-64	Required	Required for BVM	Required for BVM	
"E-Mail Username" on page 11-65				
"E-Mail Username" on page 11-65				

Administrator E-Mail Address

This is the e-mail address of the system administrator. The system alerts the administrator of any problems sending the e-mail. This is the address in the "From" field in the e-mail and can be different than the E-mail Address (see [page 11-63](#)) used in the "Reply To" field.

To enter the Administrator E-Mail Address:

1. Select System – E-Mail Gateway – **Administrator E-Mail Address**.
2. Click in the **Value** column, and then enter the address in the box. This field can contain up to 127 characters. Invalid characters are (; " \ | () , < > ').
3. Click out of the field or press **ENTER** to save the change.

E-Mail Address

The E-Mail Address option is the voice processing system e-mail address that is used in the "Reply To" field of an e-mail. This can be the same as the "From" field which is derived from the Administrator E-mail Address (see [page 11-62](#)). This address is only required if the E-mail System option (see [page 11-64](#)) is programmed to "SMTP."

NOTE

While this address can contain a "familiar" name, using SMTP, this should be a properly formatted E-mail address to avoid presenting a Reply-To e-mail address without a domain name and potentially being perceived as SPAM.

Below are examples of how an e-mail address is handled when the system using BVM has the Forward to E-mail feature enabled.

- The Administrator E-mail Address and E-mail Address fields are the same: When the user receives the e-mail, the "From" field and the "Reply To" field show the same e-mail address.
- The Administrator E-mail field is admin@test.com and the E-mail address field is chip@test.com: When the user receives the e-mail, the "From" field shows admin@test.com and the "Reply To" field shows chip@test.com

To enter the E-Mail Address:

1. Select System – E-Mail Gateway – **E-Mail Address**.
2. Click in the **Value** column, and then type the address in the box. This field can contain up to 127 characters. For example, this field might look like johndoe@mitel.com. Invalid characters are (; " \ | () , < > ').
3. Click out of the field or press **ENTER** to save the change.

E-Mail Real Name

The E-Mail Real Name specifies the voice processor's user name (such as VOICE MAIL). It is only programmable if the E-Mail System option is programmed to SMTP. When the voice mail computer sends an e-mail message, this name is included in the "From" field of the e-mail header.

NOTE

If a properly formatted e-mail is not specified, EM takes the domain part of the "Administrator E-Mail Address" and uses that to suffix the "real name."

To enter the E-Mail Real Name:

1. Select System – E-Mail Gateway – **E-Mail Real Name**.
2. Click in the **Value** column, and then type the address in the box. This field can contain up to 127 characters.
3. Click out of the field or press **ENTER** to save the change.

E-Mail SMTP Port

The E-mail SMTP Port is the port number for the Simple Mail Transfer Protocol (SMTP) server. It is only programmable if the E-Mail System option (see below) is programmed to "SMTP."

NOTE

This option applies to BVM only. If a Mitel 5000 platform is supported by an external voice messaging system such as EM, this option has no effect on E-mail Gateway functionality. When an EM is in use, this capability is disabled and the option marked unavailable with a red "X."

To change the E-Mail SMTP Port from the default 25:

1. Select System – E-Mail Gateway – **E-Mail SMTP Port**.
2. Click in the **Value** column, and then type the port number in the box. The range is 1–65535; the default is 25.
3. Click out of the field or press **ENTER** to save the change.

E-Mail SMTP Server

The E-Mail SMTP Server option is the address of the SMTP mail server. It is programmable only if the E-Mail System option (see the following section) is set to "SMTP." The SMTP mail server is the server that the voice mail connects to send e-mail messages over the Internet. If this field is not set, the e-mail gateway features are disabled for the entire voice mail system.

NOTE

The format should be a dotted-decimal IP address or fully qualified SMTP server name to avoid DNS complications.

To enter the SMTP Server:

1. Select System – E-Mail Gateway – **SMTP Server**.
2. Click in the **Value** column, and then type the server address in the box. The field can contain up to 127 characters.
3. Click out of the field or press **ENTER** to save the change.

E-Mail System

The E-Mail System option specifies the type of e-mail system that is used to transfer messages. The value programmed in this option must correspond to your e-mail system. This field can be programmed to NONE or SMTP. EM systems only support SMTP e-mail.

NOTE

To support VPIM networking (see [page 11-9](#)) or System Health Report (see [page 3-40](#)), you must first set the E-mail System to "SMTP."

If the E-mail System is programmed to "SMTP," you must program the following fields:

- E-Mail SMTP Server (see above)
- E-Mail Address (see [page 11-63](#))
- E-mail Username (see [page 11-65](#))
- Gateway Password (see [page 11-65](#))
- E-Mail Real Name (optional, see [page 11-63](#))

If it is programmed to "NONE," the voice processor E-Mail Gateway feature is disabled for the entire voice mail system.

To select the E-Mail System:

1. Select System – E-Mail Gateway – **E-Mail Pop Server**.
2. In the **Value** column, select either **None** or **SMTP**. The default value is NONE.
3. Click out of the field or press **ENTER** to save the change.

E-Mail Username

The E-Mail Username is the user name for the voice mail e-mail account on the SMTP Server. Before the voice mail computer can send or receive e-mail messages, it must log on to the underlying e-mail system. Depending on the SMTP configuration, this field may be required to log in to the SMTP server.

Therefore, the voice mail computer must have an account on the customer's e-mail system, and this field specifies the username for that account.

For authentication you only need to program a username and password. However, the Simple Mail Transfer Protocol (SMTP) mail software package supports three types of authentication (PLAIN, LOGIN, and CRAM-MD5) that happen automatically when it connects with the SMTP server. EM supports PLAIN and CRAM-MD5, and BVM supports PLAIN.

This package does not support Microsoft SPA (Secure Password Authentication), also known as NTLM. If the server supports CRAM-MD5, this is the most secure method supported.

To enter the E-Mail Username:

1. Select System – E-Mail Gateway – **E-Mail Pop Server**.
2. Click in the **Value** column, and then type the user name in the box. The field can contain up to 127 characters
3. Click out of the field or press **ENTER** to save the change.

Gateway Password

Optional. The Gateway Password is the password for the voice processing system e-mail account on the SMTP server. Before the voice processing system can send or receive e-mail messages, it must log on to the e-mail system. Therefore, the voice processing system must have an account on the customer's e-mail system.

NOTE

To provide system security, the e-mail system must have a password. To make the passwords difficult to guess, they should **not** consist of predictable patterns, such as one digit repeated several times.

To program the gateway password:

1. Select System – E-Mail Gateway – **Gateway Password**.
2. Right-click the **Password** field and select **Edit Password**. The Edit Gateway dialog box appears.
3. Type the current password, if one exists, then enter the new password in the **New password** box. Typed characters appear as asterisks (**). This field can contain up to 40 characters.
4. Retype the password in the **Confirm password** field.
5. Click **OK** to exit and save the password. If the entered passwords match, you return to the Password field. If not, you must re-enter the new password and verify it again.

E-Mail Gateway for Mitel CS-5600 Systems

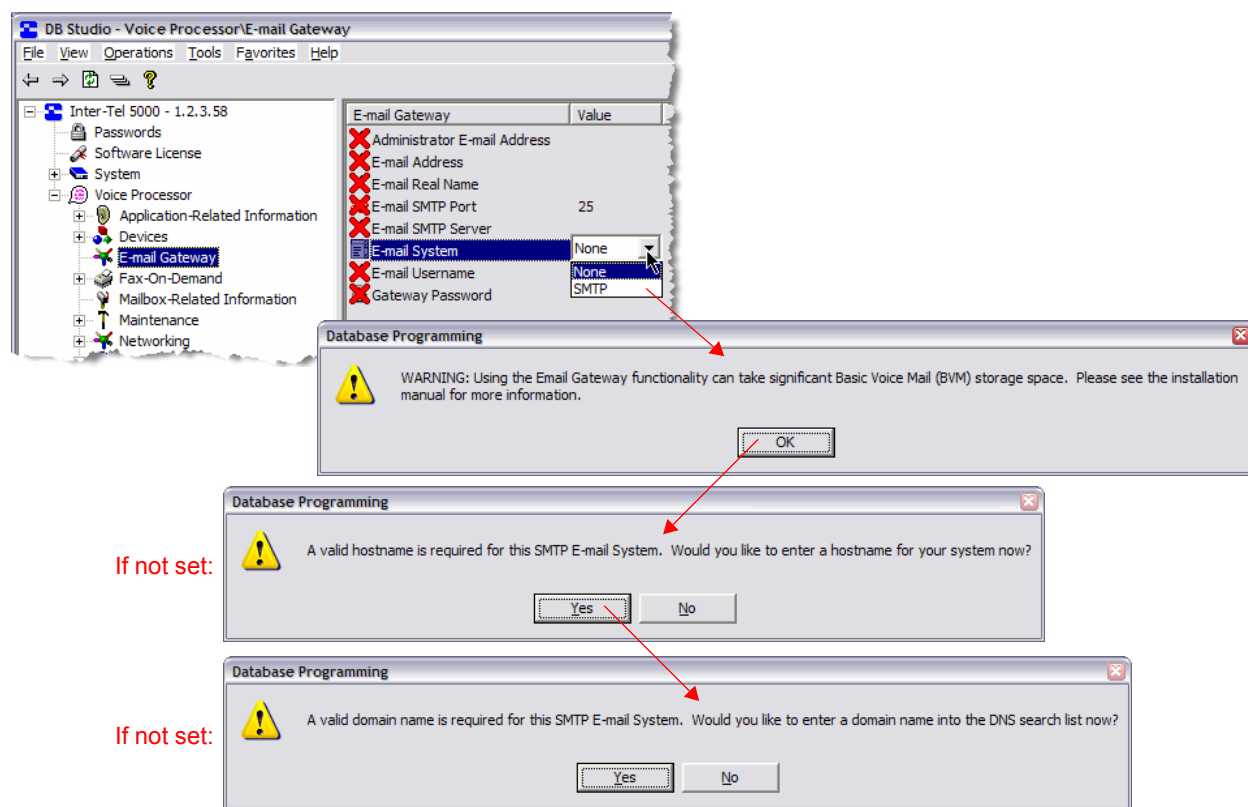
If Dynamic Host Configuration Protocol (DHCP) is disabled, when the system is connected to BVM and the SMTP option is selected for the E-mail System field, the Hostname and the DNS fields in IP Settings are automatically checked. If these fields are not configured, you are prompted to configure them. The system then navigates you to the IP Settings folder.

The fields are associated with the Processing Server on Mitel CS-5600 systems. On Mitel CS-5400 and CS-5200 systems, the fields are associated with the Base Server.

Consequently, if you select the BVM and SMTP options on a Mitel CS-5600, you are navigated to the System\IP Settings\Processing Server IP Settings folder instead of the System\IP Settings folder. On Mitel CS-5400 and CS-5200 systems, you are navigated to System\IP Settings\Base Server IP Settings.

When the system is supported by BVM, two choices exist for the E-mail System option: None and SMTP. Only SMTP supports BVM. The following example shows where this option is located.

Figure 11-4. E-Mail Gateway



NOTE

Extra storage space is required when using the E-mail Gateway functionality. If using an external voice mail system, this prompt and message does not apply. The E-mail Gateway needs to be enabled for each mailbox per endpoint, thus reducing the overall BVM storage capacity.

The BVM e-mail system requires DNS and a valid hostname. Therefore, if DHCP is disabled you cannot delete the hostname or DNS Search List without causing the BVM e-mail system to fail. If BVM is being used and SMTP e-mail is configured, the configuration is prevented and a prompt appears.

- If you click **Yes** in the prompt, you are taken to the location mentioned in the prompt where you can configure the e-mail system options.
- If you click **No**, the attempt is denied.

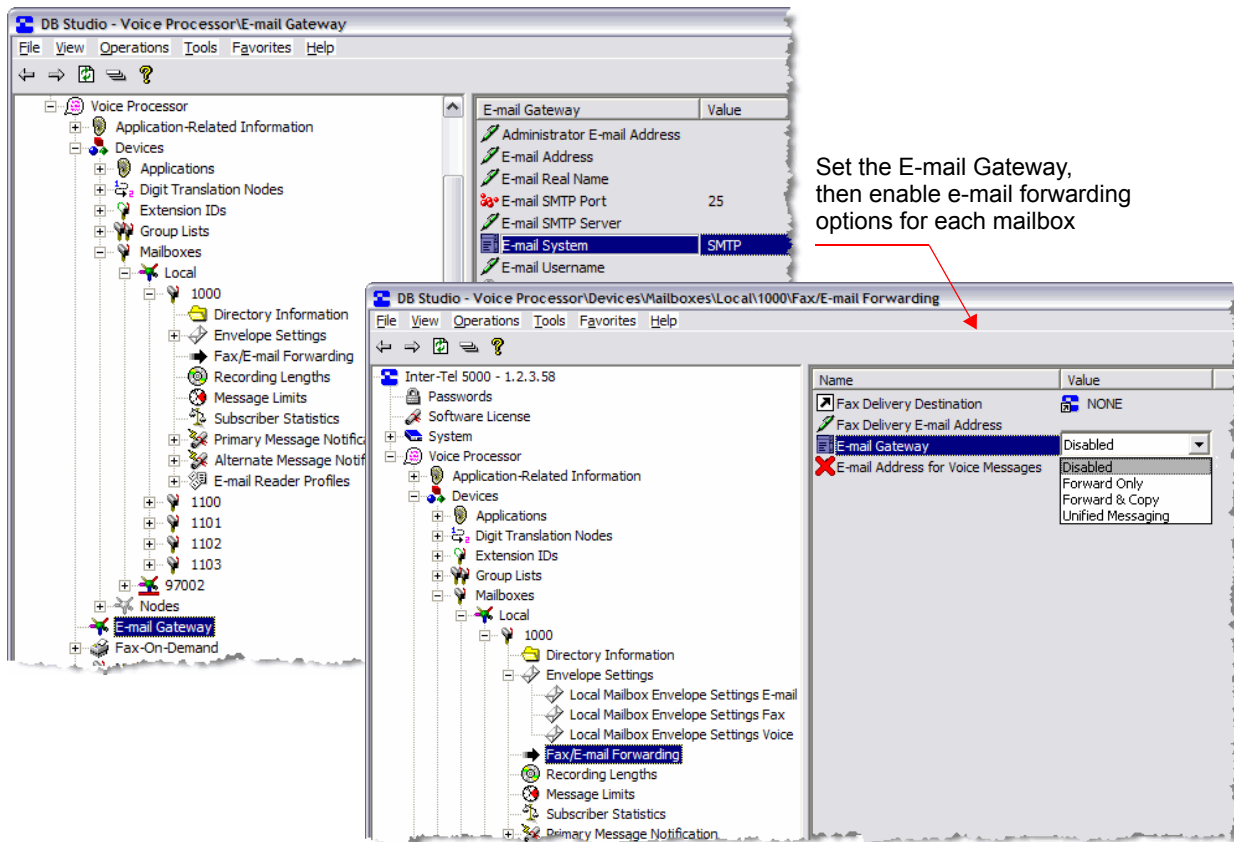
To set up the e-mail gateway for SMTP:

1. Select System – E-Mail Gateway.
2. Select the **SMTP** option for the E-mail System. Click **OK** to the warning about storage space usage with BVM. Each mailbox configured to use this option uses additional memory. At a minimum, a 512 MB Mitel memory card is recommended.

The following fields are checked from the System\IP Settings\Base Server IP Settings or Processing Server IP Settings folder: hostname, DHCP flag, and DNS Search List.

For SMTP to work with BVM, a complete hostname and domain name must be provided for the system. If DHCP is enabled, only the hostname is required. If DHCP is disabled, the DNS search list must contain a valid domain name for SMTP to work. As indicated in the example on [page 11-66](#), you will be prompted for this information. Without this information, you cannot select the SMTP option. Click **Yes** to automatically navigate to the IP Settings folder where you can set the appropriate DNS options. Also, if the hostname is configured, but DHCP is disabled and the DNS Search List is blank, you are prompted to set this information.

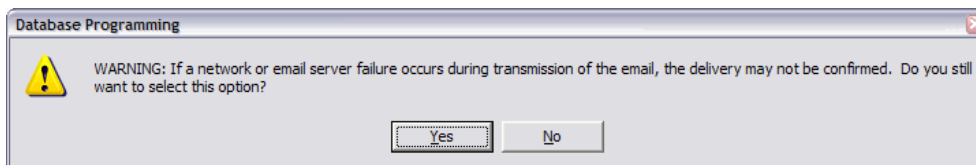
Figure 11-5. E-Mail Gateway for SMTP



3. Navigate to each mailbox for which you want to enable e-mail forwarding options, and enable the E-Mail Gateway settings from the **Unified Messaging** folder. Select from the following options.

NOTE Fax fields shown with a red “X” are not supported with BVM.

- **Forward Only:** All voice mail messages delivered to the mailbox are forwarded to the e-mail address specified in the mailbox e-mail Address field. In this configuration, voice mail messages are not saved in the mailbox. When the user deletes the e-mail message containing the voice mail message, or when e-mail delivery fails for any reason, all record of the voice mail message disappears. The following prompt appears upon selecting the Forward Only option.



- **Forward and Copy:** All voice mail messages for the mailbox are delivered to the mailbox and a copy is forwarded to the mailbox e-mail Address. If one is deleted, the other is not affected.

NOTE

If both Remote Messaging and Forward to E-Mail features are enabled, you must select the Forward and Copy option. If the Forward Only option is selected, the user does not receive Remote Messaging notifications.

Fax-On-Demand

The Fax-On-Demand feature provides fax services to callers. It is a specially programmed Call Routing Announcement application that uses digit translation to allow callers to select the documents they want to have faxed to them. Fax-On-Demand is available in external voice processing systems only.

With Fax-On-Demand, callers can use a DTMF endpoint to request one or more documents from the company's fax library. When the request is completed, the voice processor places a call to the caller's fax machine to deliver the requested documents.

To use Fax-On-Demand the following fields must be programmed:

- "Timers and Limits" below
- "Fax Documents" on [page 11-71](#)
- "Allow International Calls" on [page 11-71](#)
- "Outgoing Access" on [page 11-72](#) (trunk group)
 - Outgoing Access
 - Outgoing Access Prefix
 - Outgoing Access Termination
- "Start/Stop Time" on [page 11-72](#)
- "Days of the Week" on [page 11-73](#)
- "Fax Format" on [page 11-73](#)
 - Format - Local Fax ID
 - Format - Company Name
 - Format - Logo Document

Fax-on-Demand Timers and Limits

To view the list of current values, double-click **Timers and Limits**.

To program a timer or limit:

1. Select Voice Processor – **Fax-On-Demand**.
2. Double-click **Timers and Limits**.
3. In the **Value** column, click the current value, and then type the new setting in the box.
4. Press **ENTER** or click another field to save the change.

The following timers and limits can be programmed for the fax feature:

- **Fax Retry Timer:** When the voice processor is unable to complete a fax delivery because the line is busy or there is no answer, it will wait until this timer expires to attempt the delivery again. The range for this field is 1–255 minutes. Default is 10 minutes.
- **Fax Retransmission Timer:** When the voice processor is unable to complete a fax delivery because the connection failed (for example, the receiving fax machine had a power failure), it will wait until this timer expires to attempt the delivery again. The range for this field is 1–255 minutes. Default is 1 minute.
- **Maximum Fax Delivery Attempts:** This is the number of times the voice processor will attempt to send a fax when the number is busy, there is no answer, or there are transmission errors. If the system encounters unavailable resources (fax ports, documents, outgoing calls, or outgoing trunks) the attempt does not count toward the Maximum Fax Delivery Attempts. The allowed range for this field is 1–15 attempts. It defaults to 5 attempts.

- **Maximum Fax-On-Demand Ports:** This sets the maximum number of fax ports the system can use for performing Fax-On-Demand (either delivering outgoing faxes or importing fax documents from the system administrator mailbox). By placing a limit on the number of Fax-On-Demand ports, you can reserve fax ports for receiving incoming faxes through mailboxes and Call Routing Announcement applications. For example, if the system has eight fax ports and the Maximum Fax-On-Demand Ports field is set to six, there will always be at least two ports available for faxes received through mailboxes and Call Routing and six ports for outgoing faxes. If the Maximum Fax-On-Demand Ports field is programmed to a number that exceeds the actual fax ports available, the software will automatically adjust the limit.
- **Automatic Header Reduction:** This tells the voice processor how much of each document you fax into the system must be removed to erase the sender information at the top of the document. If the fax machine you use to enter the documents does not place sender information at the top of the document, you can set this field to 0. You can reduce the header 0–160 sixteenths of an inch (0–10 inches). This field defaults to 4-sixteenths of an inch (0.25 in.).
- **Fax Tone Wait Timer:** This is the amount of time the voice processor will wait for fax tone before sending or receiving a document. If it does not receive fax tone before this timer expires, it will hang up. If the system was sending a fax, it will attempt the call again after the Fax Retry Timer expires. The range for this field is 1–255 seconds. Default is 40 seconds. The Fax Tone Wait Timer cannot be configured for Enterprise Messaging. The system uses a value of 40 seconds.

NOTE Add the following note: EM requires a fax port license to detect fax tone.

- **Maximum Fax Selections:** This determines the number of faxes a caller can select at a time. When the caller has selected the maximum number of documents, the voice processor prompts them for their fax number. After entering the fax delivery information, the caller can then go through the process again to request more documents without hanging up and calling in again. However, each series of requests generates a separate outgoing call from the voice processor, each time the fax delivery information is entered by the caller. The allowed range for this field is 1–20 documents. It defaults to 10.
- **Maximum Fax-On-Demand Library Size:** This determines the amount of voice processor hard disk space that will be allotted for storing fax documents. The allowed range for this field is 0–255 megabytes; however, the actual maximum depends on the available disk space on the voice processor hard drive. It defaults to 0 megabytes and must be programmed to a higher value before any fax documents can be imported. If the library size is reduced while there are documents stored in the library, the reduction will not affect existing documents, even if they now exceed the new maximum. However, new documents cannot be added unless there is sufficient disk space available.
- **Current Fax-On-Demand Library Size And Percentage Of Maximum Currently Used:** This shows the amount of disk space that is currently being used by the documents in the fax library and the percentage of the Maximum Fax Library Size that has been used. These fields cannot be programmed. They are shown for reference only.

Fax Documents

To program Fax Documents:

1. Double-click **Fax Documents**, the documents currently existing in the system are shown in the list.
2. Program the number and description of a document as follows:
 - **Document Number:**
 - a.) Type a number, up to four digits, to identify the fax document in the text box.
 - b.) Press **ENTER** or click another field to save the change. This number will be used by programmers to select the destination for digit translations and by callers when selecting fax documents by number.
 - **Description:** This is the abbreviated description that is used in programming screens. It can have up to 20 characters.
 - a.) Enter the description in the text box.
 - b.) Press **ENTER** or click another field to save the change.

To see additional fields: Double-click a document to see these additional programming fields:

- **Detailed Description:** This is the description that appears on the fax cover sheet and in any fax programming reports. It can include up to 40 characters.
 - a.) Enter the description in the text box.
 - b.) Press **ENTER** or click another field to save the change. If you do not enter a detailed description for the document before exiting, a warning message appears.
- **Statistics:** This information cannot be programmed. It is shown as a reference to indicate the following:
 - **Number of Requests:** How many times the document has been requested, since statistics were last cleared (see [page 15-8](#)).
 - **Last Request:** The last date that the document was requested, since statistics were last cleared. This includes requests that could not be delivered because of transmission errors.
 - **Last Modification:** The date and time of the last modification to the document being programmed, since statistics were last cleared. Or, if the document has not been modified, it shows the time that it was imported.
 - **Pages:** The number of pages included in the document.
 - **Image File Size:** The amount of disk space occupied by this document.

Allow International Calls

This field allows you to enable or disable international fax deliveries. If it is disabled, the prompt asks the caller to enter a 10-digit number for their fax destination. If this field is enabled, the prompt gives international dialing instructions and allows international and domestic numbers. The field defaults to *disabled*.

To allow international calls:

1. Select the check box to place a check mark in it to change the setting to **Yes**.
2. Press **ENTER** or click another field to save the change. To set it back to **No**, click the check box again.

Outgoing Access

The next three fields control the outgoing access for calls placed by the Fax-On-Demand application.

Outgoing Access: This is the outgoing trunk access code that the Message Notification/Retrieval application will use to place the outgoing fax delivery call. The default value is blank. To determine the outgoing access trunk group, use one of the following methods:

Method A

1. Select the current Value, and then enter the new value in the text box.
2. Press **ENTER**. A dialog box appears displaying what is associated with the number entered.
3. Click **OK**. The new number appears in the field.

Method B

1. Right-click the existing value and select **Change Outgoing Access**. A dialog box appears prompting for the device type to include.
2. Select **CO Trunk Group**, and then click **Next**. The list of trunk groups appears. You can view them in a list by selecting the List button or view details by selecting the Details button.
3. Select the appropriate trunk group, and then click **Finish**. The selection appears in the Outgoing Access field.

Outgoing Access Prefix: This is the digit dialed by the voice processor before the outgoing access code, if needed (e.g., a forced account code). This field can include up to 18 characters. Valid characters include digits 0–9, * and #, and “P” for pause. This field is blank by default. To enter the prefix:

1. Click the **Value**, and then enter the address in the text box.
2. Press **ENTER** or click another field to save the change.

Outgoing Access Termination: This is the digit dialed by the voice processor to terminate the outgoing access code, if needed. This field can include up to 18 characters. Valid characters include digits 0–9, * and #, and “P” for pause. This field defaults to #. To enter the termination digit:

1. Click the Value, and then enter the address in the text box.
2. Press **ENTER** or click another field to save the change.

Start/Stop Time

These fields determine the time period during which faxes will be sent to callers. If a caller requests a fax after the Stop Time, the system will not send the fax until the Start Time. To provide 24-hour fax service, set both fields to the same value. Both fields default to 5:00 PM.

To set the time:

1. Select the current Value, then select the hours, minutes, or AM/PM field, and use the arrows to scroll to the desired setting.
2. Select another field or press **ENTER** to save the change.

NOTE

With a U.S. system, the Fax-On-Demand feature uses User Group 1 and the Home Area Code for toll restriction information. Ensure that these are programmed correctly for outgoing fax delivery calls. Also ensure that the Message Notification/Retrieval application has the appropriate trunk access.

Days of the Week

These fields set the days of the week during which faxes will be sent to callers. If a caller requests a fax on a disabled day, the system will wait for the next enabled day to send the fax. At default, all days of the week are enabled. You cannot disable all seven days; at least one must be selected.

To enable a specific day of the week:

1. Select the check box to place a check mark in it and change the setting to **Yes**.
2. Press **ENTER** or click another field to save the change. To set it back to **No**, select the check box again.

Fax Format

The following fields affect the format of the fax documents that are sent by the Fax-On-Demand application.

- **Local Fax ID:** The Local Fax ID appears at the top of each page sent by the voice processor. The ID should include the number of the voice processor and/or the company name. The ID can be up to 20 characters. Valid characters include upper-case letters, digits 0–9, and the plus sign (+).

To enter the Fax ID:

- a. Click the **Value** field, then enter the address in the text box.
 - b. Press **ENTER** or click another field to save the change.
- **Company Name:** The system places Company Name on the “From” line of the fax cover sheet. The company name can include up to 40 characters. Any character is allowed.

To enter the company name:

- a. Click the **Value** field, then enter the address in the text box.
- b. Press **ENTER** or click another field to save the change.

Logo Document: After you have imported your company logo, you can assign that fax document as the Logo Document for your fax cover sheets. For more information about importing fax documents, refer to the *Mitel 5000 Endpoint and Voice Mail Administrator Guide*, part number 580.8001. Any fax document in the database can be designated as the logo document. The logo can be up to 5.5 inches tall. If desired, you can choose not to have a logo on your cover sheets by selecting **None**. To indicate which fax document is the logo document, use one of the following methods:

Method A

1. Select the current Value, then enter the new value in the text box.
2. Press **ENTER**. A dialog box appears displaying what is associated with the number entered.
3. Click **OK**. The new number appears in the field.

Method B

1. Right-click the existing value and select **Change Format**, and then select **Logo Document**. A dialog box appears prompting for the device type to include.
2. Select **Fax Document** (or select **None Device**, if you do not want to use a logo document), and then click **Next**. The list of currently existing documents appears. You can view them in a list by selecting the List button or view details by selecting the Details button.
3. Select the appropriate document (or None), and then click **Finish**. The selection appears in the Logo Document field.

Subscriber Mailboxes

Introduction	12-3
Creating Mailboxes	12-3
Creating Mailboxes for Extensions with Extension IDs	12-3
Creating Associated Mailboxes	12-4
Creating Non-Associated Mailboxes	12-4
Changing Non-Associated Mailbox Extension Numbers	12-5
Deleting Mailboxes	12-5
Clearing Mailbox Messages	12-5
Copying Mailbox Settings	12-6
Network Mailboxes (Off-Node Mailboxes)	12-7
Remote Mailbox Extension	12-7
Unlisted Number and Private Mailbox Number Options	12-7
Programming Mailbox Options	12-8
Directory Information	12-9
Envelope Settings	12-10
Unified Messaging	12-11
Recording Length	12-15
Message Limits	12-15
Subscriber Statistics	12-16
E-mail Reader Profiles	12-17
Dial-0 Destinations	12-18
Programming the Day and Night Dial-0 Destination Types	12-18
Programming the Dial-0 Destination	12-18
Remote Messaging	12-19
Primary and Alternate Message Notification	12-20
Adding Cascade Levels	12-21
Deleting Cascade Levels	12-21
Programming Cascade Level Options	12-21
Mailbox Initialized	12-23
Receive Only	12-23
Allow Transfer Method Programming	12-23
Play Recording Instructions	12-23
Auto Attendant Transfer Prompt	12-24
Deliver Hangup Message (when ANI is available)	12-24
Swap “7 for Save” and “9 for Delete” Message Keys	12-25
Designate this Mailbox for Play Only	12-25
Password	12-26
Greeting	12-26

Transfer Method	12-27
Message Notification Endpoint	12-27
Time Zone	12-28
Automatic Speech Recognition (ASR) Setting	12-28
Automatic Speech Recognition (ASR) Enabled	12-28
Quota Warning	12-29
Quota Grace	12-29
Mailbox-Related Information	12-30

Introduction

This chapter provides information to create and configure subscriber mailboxes for Basic Voice Mail (BVM) and Enterprise Messaging (EM) systems.

For NuPoint Messenger system setup and mailbox configurations, refer to the following resources:

- *Mitel 5000 and NuPoint Messenger Integration Guide*, part number 580.8008
- *NuPoint Messenger Technical Documentation Help*
- *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000
- *Mitel 5000 DB Programming Help*

Program the voice processor system settings before creating and programming mailboxes. See “Voice Processor System Programming” on [page 11-1](#).

Creating Mailboxes

The following sections describe how to create and program mailboxes for nodes. A mailbox is a storage location on the voice processing computer hard disk that stores all messages that have been directed to it. Mailboxes can be either *associated* or *non-associated*:

- **Associated:** A mailbox that is directly associated to an extension number.
- **Non-Associated:** A mailbox that has an extension number that does not match the endpoint extension number. For example, a hunt group extension number can have a mailbox, but the system sends message indications to a designated hunt group endpoint, which uses a different extension number than that of the hunt group mailbox.

NOTE

If you are using non-associated mailboxes, you must disable the Validate Voice Mailbox flag. When enabled, this flag prevents users from dialing mailbox numbers that do not match valid extension numbers.

You can create associated and non-associated mailboxes on the local node. However, you cannot create non-associated mailboxes for endpoints on other system nodes. For more information, see “Mailbox-Related Information” on [page 12-30](#).

When you view system mailboxes, the nodes that are shown are determined by whether you have previously programmed Voice Processing network nodes. If nodes exist, you will see the nodes listed with the local node. You can click any of them to program the mailboxes for the selected node, as described below. If there are no voice processing networking nodes, you skip directly to the list that shows mailboxes on the local node.

Creating Mailboxes for Extensions with Extension IDs

You can create mailboxes for extensions that currently have extension IDs.

To create a mailbox for an extension that currently has an extension ID:

1. Select Voice Processor – Devices – Mailboxes – *<node>*.
2. Delete the extension ID.
3. Create the mailbox.

Creating Associated Mailboxes

You can create associated mailboxes for either local-node or off-node systems.

To create an associated mailbox:

1. Select Voice Processor – Devices – Mailboxes – **<node>**.
2. Right-click in the right pane, and then click **Create Associated Mailbox**. A window appears prompting for the device type to include.
3. Select the device type, and then click **Next**. The list of devices with details appears. To view items in a list only, click **List**.
4. Select the devices for which you want to create mailboxes (you can press SHIFT or CTRL to select more than one device), and then click **Add Items**. The selections appear in the mailbox list.
5. Click **Finish** to exit.

Creating Non-Associated Mailboxes

You can create non-associated mailboxes for local nodes. You cannot create non-associated mailboxes for endpoints on other system nodes. For more information, see “Mailbox-Related Information” on [page 12-30](#).

To create a non-associated mailbox:

1. Select Voice Processor – Devices – Mailboxes – **<node>**.
2. Right-click in the right pane, and then select **Create Non-Associated Mailbox**. The Create Mailbox Extension dialog box appears.
3. In the **Starting Extension** box, enter the starting extension for the new mailboxes.
4. In the **Number of Extensions** box, enter the number of extensions.
5. Click **OK**.
6. The new mailboxes appear in the right pane. If any mailbox extensions conflict with existing extensions, a dialog box appears, listing the mailboxes that were not created.
7. Program the description and user name as follows:
 - a. Enter a description of up to 20 characters in the **Description** box. This description is used in the mailbox directory and should be entered in the form “last name, first name” (with a comma and space separating the names).
 - b. Enter a name of up to 10 characters in the **Username** box. This is the name that appears on endpoint displays. Do **not** use slash (/), backslash (\), vertical slash (|) or tilde (~) characters in usernames. Do **not** use Control characters in descriptions or usernames.

Changing Non-Associated Mailbox Extension Numbers

You can change non-associated mailbox extension numbers.

To change a non-associated mailbox number:

1. Select Voice Processor – Devices – Mailboxes – *<node>* – *<mailbox number>*.
2. In the **Extension** column, select the number, and then type or select the new number.
3. Click out of the field or press **ENTER** to save the change.

Deleting Mailboxes

You can delete associated or non-associated mailboxes from local and remote nodes.

NOTICE

Disruption of Voice Processing Possible. Make sure a mailbox is not in use before deleting it. Deleting a mailbox while it is in use causes serious performance issues for voice processing.

To delete mailboxes:

1. Select Voice Processor – Devices – Mailboxes – *<node>*.
2. Select the mailboxes.
3. Right-click, and then select **Delete**. The mailboxes are removed from the list.

Clearing Mailbox Messages

If you have an active direct connection or remote programming session, you can clear (erase) all of the messages in a mailbox.

To clear mailbox messages:

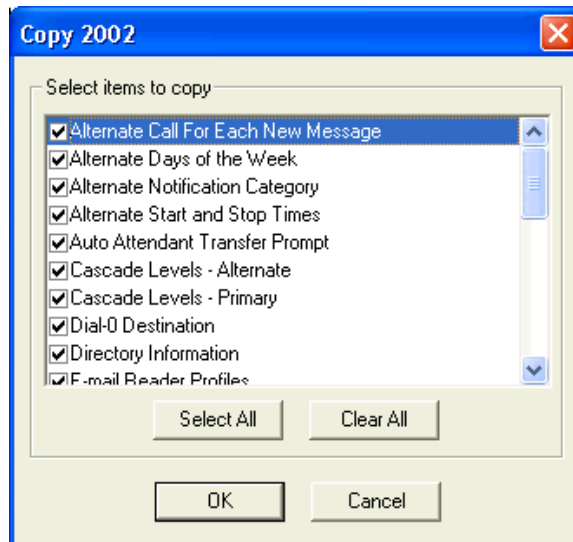
1. Select Voice Processor – Devices – Mailboxes – *<node>* – *<mailbox number>*.
2. Select the mailbox(es) you want to clear.
3. Right-click, and then select **Clear Message(s)** from the Selected Mailboxes option.

Copying Mailbox Settings

To save time, you can copy mailbox settings and paste the settings in another mailboxes.

To copy and paste mailbox settings:

1. Select Voice Processor – Devices – Mailboxes – **<node>**.
2. Right-click the mailboxes, and then select **Copy**.
3. Right-click the mailbox where you want to copy the settings, and select **Paste**. A dialog box appears, as shown below, that allows you to select the attributes you want to copy.



4. Select the options that you want paste, and then click **OK** to save your changes.

Network Mailboxes (Off-Node Mailboxes)

NOTICE

Unstable System Performance Possible. Do not create or delete more than 2000 off-node devices at a time. Batch-creating more than 2000 off-node devices may cause system instability or other problems.

Mailboxes that are programmed on the local node but are associated with mailboxes on remote voice processing nodes are referred to as “network mailboxes.” They are used by the local node to identify and locate the mailboxes located on the other nodes. They are not actual mailboxes; they are just “place holders” that tell the local node where to send messages received for that mailbox number. If the mailbox subscriber logs on to a network mailbox, the options available are the directory name, the greetings, the password, and possibly the transfer method programming prompt, if enabled. In addition, if a subscriber changes the password, directory name, or greeting selection, these changes will be automatically updated on the corresponding network mailboxes.

You can program the following options only for off-node mailboxes:

- Remote Mailbox Extension (see the following section).
- Unlisted Number (see [page 12-9](#)).
- Private Extension and Mailbox (see [page 12-9](#)).
- Allow Transfer Method Programming (see [page 12-23](#)).
- Auto Attendant Transfer Prompt (see [page 12-24](#)).
- Password (see [page 12-26](#)).
- Transfer Method (see [page 12-27](#)).

Remote Mailbox Extension

The only option available for off-node mailboxes that is different from local mailbox programming is *Remote Mailbox Extension*. The Remote Mailbox Extension contains the actual mailbox number of the mailbox on the remote node.

If there is a universal numbering plan used by all of the networked voice mail nodes, the Remote Mailbox Extension option is the same as the local mailbox number. If the numbering plan is **not** universal, the Remote Mailbox Extension option can be different than the local mailbox number. The mailbox numbers programmed in this option are not verified because the local voice processing system does not know about the mailbox numbers on the remote voice processing system until it actually attempts to deliver a message to the remote voice processing system. The default value for the Remote Mailbox Extension is the local mailbox number.

The Remote Mailbox Extension option can be changed to any number up to five digits. The remote mailbox option is not validated and it should **not** be programmed a part of a group list or network mailbox on the remote node.

Unlisted Number and Private Mailbox Number Options

A network mailbox should have the Unlisted Number and Private Mailbox Number options enabled. The Unlisted Number option keeps the network mailbox from appearing in the company directory, and the Private Mailbox Number option prevents the caller from hearing the mailbox number while using the company directory. These two fields can only be programmed from DB Programming.

Programming Mailbox Options

NOTE

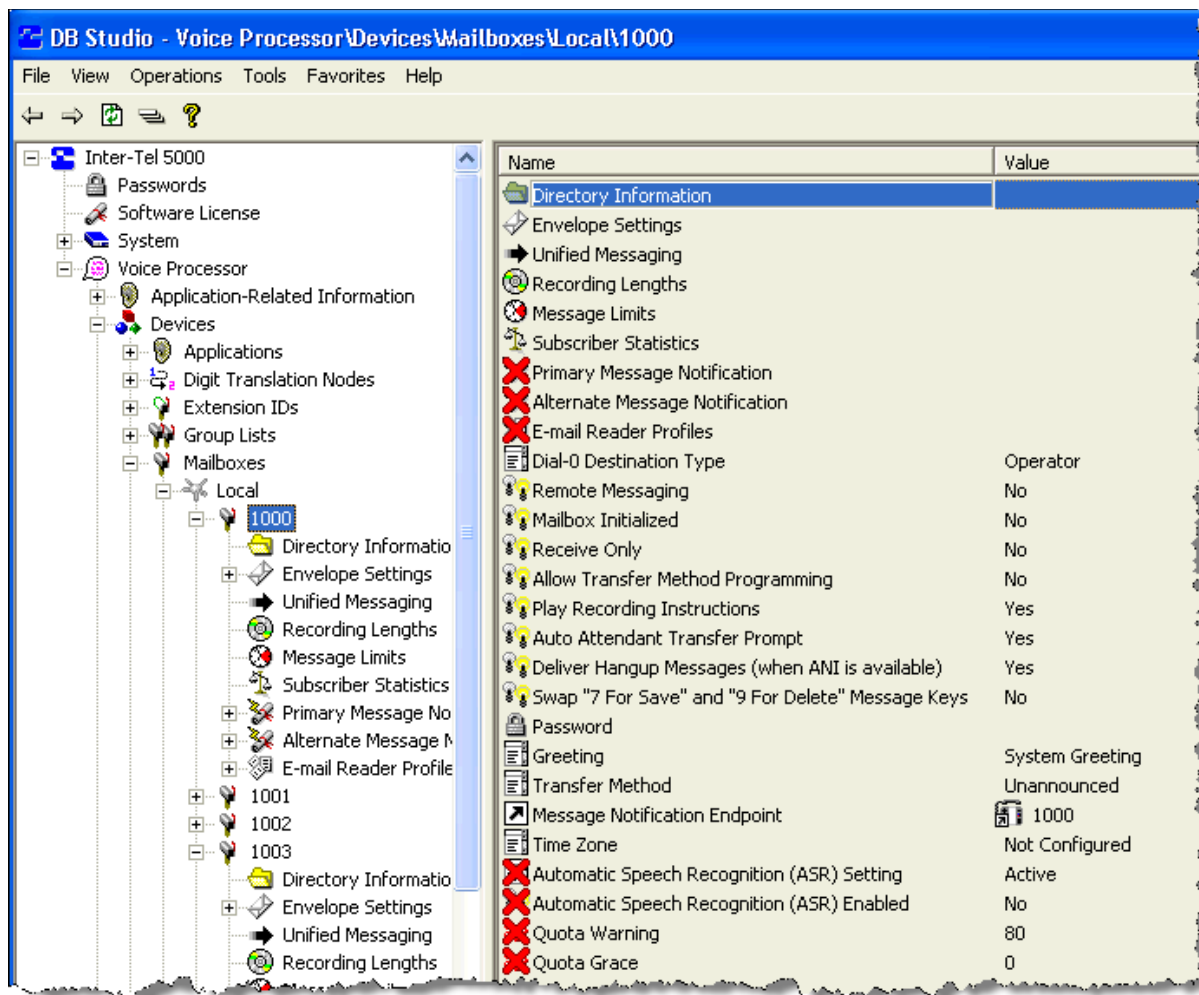
Mailboxes that are programmed on a local node but are associated with mailboxes on remote voice processing nodes are referred to as “network mailboxes.” Network mailboxes have limited programming options. See “Network Mailboxes (Off-Node Mailboxes)” on [page 12-7](#) for more information.

You can program the following mailbox options:

- “Directory Information” on [page 12-9](#)
- “Envelope Settings” on [page 12-10](#)
- “Unified Messaging” on [page 12-11](#)
- “Recording Length” on [page 12-15](#)
- “Message Limits” on [page 12-15](#)
- “Subscriber Statistics” on [page 12-16](#)
- “E-mail Reader Profiles” on [page 12-17](#)
- “Dial-0 Destinations” on [page 12-18](#)
- “Remote Messaging” on [page 12-19](#)
- “Primary and Alternate Message Notification” on [page 12-20](#)
- “Receive Only” on [page 12-23](#)
- “Allow Transfer Method Programming” on [page 12-23](#)
- “Play Recording Instructions” on [page 12-23](#)
- “Auto Attendant Transfer Prompt” on [page 12-24](#)
- “Deliver Hangup Message (when ANI is available)” on [page 12-24](#)
- “Swap “7 for Save” and “9 for Delete” Message Keys” on [page 12-25](#)
- “Designate this Mailbox for Play Only” on [page 12-25](#)
- “Password” on [page 12-26](#)
- “Greeting” on [page 12-26](#)
- “Transfer Method” on [page 12-27](#)
- “Primary and Alternate Message Notification” on [page 12-20](#)
- “Message Notification Endpoint” on [page 12-27](#)
- “Time Zone” on [page 12-28](#)
- “Automatic Speech Recognition (ASR) Setting” on [page 12-28](#)
- “Automatic Speech Recognition (ASR) Enabled” on [page 12-28](#)
- “Quota Warning” on [page 12-29](#)
- “Quota Grace” on [page 12-29](#)

Figure 12-1 on [page 12-9](#) shows the mailbox programming options in DB Programming (for associated mailboxes).

Figure 12-1. Mailbox Options



Directory Information

Mailbox Directory Information options include the following:

- **Unlisted number:** The mailbox number is not included in the mailbox directory, but callers can dial the number.
- **Private extension and mailbox numbers:** The extension *and* mailbox numbers are not included in directory, but callers can dial either number.

By default, mailbox and extension numbers are not either private or unlisted.

To set Directory Information flags:

1. Select Voice Processor – Devices – Mailboxes – *<node>* – **<extension>**.
2. Double-click **Directory Information**. The list of flags appears.
3. Select the option that you want to change.
4. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
5. Click out of the field or press **ENTER** to save the change.

Envelope Settings

E-mail, fax, and voice messages can include a “message envelope” for all message types, including those that are converted to speech. This envelope contains information such as the message duration, source, and so on. Announcement options include the following:

- **Announce Message Length:** (*Voice Only*) If enabled, the voice mail message duration is included in the message envelope.
- **Announce Message Subject:** (*E-mail Only*) If enabled, the subject line of the e-mail message is included in the envelope. If the subject line is blank, the envelope ignores this setting and does not announce the subject.
- **Announce Message Pages:** (*Fax Only*) If enabled, the total number of pages that were faxed are included in the envelope.
- **Announce Message Source:** If enabled, the envelope includes the message originator. For e-mail messages, this is the e-mail address or alias of the message sender; for voice mail messages, this is the name and number of the caller (if available); and for faxes, this is the originating fax number.
- **Announce Date and Time:** If enabled, the date and time that the message was received is included in the envelope.

You cannot program envelope options for off-node mailboxes.

NOTE

This feature is available as a programmable option to subscribers, allowing them to change the selected option.

To disable an envelope option:

1. Select Voice Processor – Devices – Mailboxes – Local – **<extension>**.
2. Double-click **Envelope Settings**.
3. Double-click the message type (**E-Mail**, **Fax**, or **Voice**).
4. Clear the check box for the option that you want to disable.

Unified Messaging

This folder is for supporting the features included with Unified Messaging (UM) OSE v2.0. For complete information about Unified Messaging OSE v2.0, refer to the *Unified Messaging Open Standards Edition Administrator's Guide*, part number 835.3162.

The Unified Messaging Level field specifies the UM level of integration. The options for this field vary depending on the Voice Processor type, as shown in [Table 12-1](#).

Table 12-1. Unified Messaging Levels for BVM and EM

Unified Messaging Level	Description	Voice Processor Type	
		BVM	EM
Disabled	Delivers a voice message to the user's mailbox just as normal. No e-mail is sent.	✓	✓
Forward Only	Delivers a voice message to the user's e-mail address when the user receives a new voice message in his or her voice mailbox. After the message is sent, the original message is deleted from the mailbox.	✓	✓
Forward and Copy	Delivers a copy of a voice message to the user's e-mail address when the user receives a new voice message in the voice mailbox. The original message can be retrieved from the mailbox.	✓	✓
Unified Messaging	Allows the user to use the Unified Messaging v2.2 functionality.		
Enhanced Forward and Copy	Provides the user with direct access into the voice mailbox from the e-mail client. This level provides full integration with the e-mail client, but does not provide synchronization between the EM server and the e-mail server. With this level, the user has configuration control over the format of the messages.		✓
Basic Integration	Provides the user with direct access into the voice mailbox from the e-mail client. This level offers limited integration with the e-mail client for voice messages because a separate IMAP inbox is required for voice messages. The user has no configuration control over the format of the messages.		✓
Enhanced Integration	Provides full integration for voice messages with the e-mail client, and provides full synchronization between the EM server and the e-mail server. The user has configuration control over the format of the message, and this level supports the Message Waiting Indication (MWI) feature.		✓

The Unified Messaging level you select determines which additional fields in the Unified Messaging folder are programmable. See [page 12-13](#) for programming instructions and field descriptions.

NOTE

For Unified Messaging OSE v2.0, the values for the option previously programmed under the Fax/E-mail Forwarding folder remain the same and the fields automatically map to their new location.

Chapter 12: Subscriber Mailboxes

Programming Mailbox Options

Table 12-2 indicates which fields in the Unified Messaging folder must be programmed for each Unified Messaging level.

Table 12-2. Programmable Fields for the Unified Messaging Folder

Programmable Fields	Unified Messaging Level					
	Disabled	Forward Only, Forward and Copy	Unified Messaging	Enhanced Forward and Copy	Basic Integration	Enhanced Integration
Unified Messaging Level	✓	✓	✓	✓	✓	✓
Enable SSL for E-mail Server Connection				✓		✓
E-mail Account Folder for Synchronization				✓		✓
E-mail Server				✓		✓
E-mail Account Password				✓		✓
E-mail Account Username				✓		✓
E-mail Address for Voice Messages		✓	✓	✓	✓	✓
Allow User to Configure Settings				✓		✓
Download Format for Mobile Web Page				✓	✓	✓
E-mail Client Message Format				✓		✓
Synchronize MWI with E-mail Client						✓
E-mail Address for Fax Delivery ¹	✓	✓	✓	✓	✓	✓
Copy Fax to Sender	✓	✓	✓	✓	✓	✓
Fax Delivery Destination ¹	✓	✓	✓	✓	✓	✓
IMAP Synchronization Method ²				✓		✓
IMAP IDLE Timeout				✓		✓
IMAP Polling Timeout				✓		✓

1. This field is disabled if the voice processor type is BVM, which does not support faxing.

2. The option selected for the IMAP Synchronization Method determines which related fields are programmable:

- *Event* (default): The IMAP IDLE Timeout field is enabled and the IMAP Polling Timeout field is disabled.
- *Polling*: The IMAP IDLE Timeout field is disabled and the IMAP Polling Timeout field is enabled.

To program Unified Messaging options:

1. Select Voice Processor – Devices – Mailboxes – *<mailbox>* – **Unified Messaging**.
2. Program the following options:
 - **Unified Messaging Level:** Specifies the level of integration for Unified Messaging. It is set to Disabled by default. Available options depend on the voice processor type. See Table 12-1 on [page 12-11](#) for option descriptions.
 - **Enable SSL for E-mail Server Connection:** Indicates whether the integration connection is made using Secure Socket Layer (SSL). It is set to Yes by default. This field appears with a red “X” unless Unified Messaging Level is set to Enhanced Forward & Copy or Enhanced Integration.
 - **E-mail Account Folder for Synchronization:** Indicates the path to the account folder (such as Inbox, Voice Mail, and so on) on the e-mail server to use for message synchronization. The folder name can be up to 127 characters. For example, to synchronize messages to the folder named “Voice Mail” in the user’s e-mail client account, type Voice Mail in the text box. To synchronize messages to the subfolder named “VM” under the “Inbox” main folder, type `Inbox/VM` in the text box. This field is set to *Inbox* by default. This field appears with a red “X” unless Unified Messaging Level is set to Enhanced Forward & Copy or Enhanced Integration.
 - **E-mail Server:** Indicates the name of the e-mail server for the account synchronization. The server name can be up to 127 characters. This field is blank by default. This field appears with a red “X” unless Unified Messaging Level is set to Enhanced Forward & Copy or Enhanced Integration.
 - **E-mail Account Password:** Indicates the password of the account to use for message synchronization. This is the user’s network password. The password can be up to 40 characters. This field is blank by default. This field appears with a red “X” unless Unified Messaging Level is set to Enhanced Forward & Copy or Enhanced Integration.
 - **E-mail Account Username:** Indicates the user name of the account to use for message synchronization. This is the user’s network username. The username can be up to 127 characters. This field is blank by default. This field appears with a red “X” unless Unified Messaging Level is set to Enhanced Forward & Copy or Enhanced Integration.
 - **E-mail Address for Voice Messages:** Specifies the e-mail address to which the voice mail messages will be forwarded. This is also the e-mail address where welcome and error e-mails are sent for the Enhanced Forward and Copy and Enhanced Integration Unified Messaging levels. The content and format of the field depends on the e-mail system being used. The address can be up to 127 characters. If you enter an invalid character (: ; “ \ | () , < > ’), an error tone occurs. For example, when using Lotus Notes, this field could be set to John Doe/Chandler/Mitel, and when using e-mail, it would be john_doe@mitel.com. This field was originally located in the Fax/E-mail Forwarding folder.
 - **Allow User to Configure Settings:** Delegates account configuration control to the individual account users. It is set to Yes by default. This field appears with a red “X” unless Unified Messaging Level is set to Enhanced Forward & Copy or Enhanced Integration.
 - **Download Format for Mobile Web Page:** Specifies which format to use when downloading voice messages from the mobile device Voice Mail Web page. Options include .MP3 or .wav file formats. The default value is MP3. This field appears with a red “X” unless Unified Messaging Level is set to Enhanced Forward & Copy, Basic Integration, or Enhanced Integration.

NOTE

Most mobile devices do not support the .wav file format. Determine which format the user’s mobile device supports and program this option accordingly.

- **E-mail Client Message Format:** Indicates whether the message that the user receives contains a URL (a link to the message), a file attachment, or both. It is set to Attachment by default. This field appears with a red "X" unless Unified Messaging Level is set to Enhanced Forward & Copy or Enhanced Integration.

NOTE

If your system uses e-mail retention software that automatically moves the e-mail notification message to another location, select File Attachment or Both for your message format. Otherwise users' voice messages may be deleted from the EM server.

- **Synchronize MWI with E-mail Client:** Synchronizes message waiting indicator (MWI) support with the e-mail client. If set to "Yes" (default), the message lamp is turned off when the e-mail message is read. This field is applicable to the Enhanced Integration Unified Messaging Level only.
- **E-mail Address for Fax Delivery:** Specifies the e-mail address of the account that will receive incoming faxes. The fax is converted to a TIFF file and sent to the e-mail address as an attached file. The address can be up to 127 characters. If you enter an invalid character (: ; " \ | () , < > '), an error tone occurs. This field appears with a red "X" if the Voice Processor type is BVM because BVM does not support faxing. This field was originally located in the Fax/E-mail Forwarding folder.
- **Copy Fax to Sender:** Enables the default operation for e-mailing a copy of a fax to a user's account as specified in the E-mail Address for Fax Delivery field (see above). The flag is enabled by default.
- **Fax Delivery Destination:** Specifies the extension of the fax machine that receives incoming faxes routed through this mailbox. This field appears with a red "X" if the Voice Processor type is BVM because BVM does not support faxing. This field was originally located in the Fax/E-mail Forwarding folder.

To program the Fax Delivery Destination extension number, use one of the following methods:

Method A

- 1.) Select the current value and enter the new value in the box.
- 2.) Press **ENTER**. A screen displays what is associated with the number you entered.
- 3.) Click **OK**. The new number appears in the field.

Method B

- 1.) Right-click on the existing extension number. An option box appears.
 - 2.) Click **Change Fax Delivery Destination**. A window appears prompting you to select the type of device to include.
 - 3.) Select the type of device and then click **Next**. The list of devices appears. (You can view them in a list only by selecting the List button.)
 - 4.) Highlight the extension number associated with the fax machine then click **Finish**. Your selection appears in Fax Delivery Destination field.
- **IMAP Synchronization Method:** Determines how the IMAP server synchronizes messages between the server and an IMAP client account. By default, it is set to Event. This allows message changes on the remote IMAP server to be automatically recognized by the synchronization client, as they occur. If the IMAP server does not support the IMAP IDLE command, select **Polling**. This forces the synchronization client to query for changes on the account on the remote server. If you do not know if the remote IMAP server supports the IDLE command, default to Event. At run time the synchronization client automatically detects if the IDLE command is supported. If not supported, the client uses the Polling method. Polling can be used as default to reduce load on the EM unit. This field appears with a red "X" unless the Unified Messaging Level is set to Enhanced Forward & Copy or Enhanced Integration.

- **IMAP IDLE Timeout:** Determines the maximum length that the IDLE command will wait for the IMAP server. The field appears with a red "X" if the Integration Synchronization Method is set to "Polling." The range is 1–30 minutes; the default value is 20 minutes. This field appears with a red "X" if the IMAP Synchronization Method is set to "Polling" as it only applies for Event or unless Unified Messaging Level is set to Enhanced Forward & Copy or Enhanced Integration.
 - **IMAP Polling Timeout:** Indicates how often the synchronization process polls for message updates. Use this when the server does not support the IDLE command. The range is 1–20 minutes; the default value is 10 minutes. The field appears with a red "X" if the IMAP Synchronization Method is set to "Polling" as it only applies for Event or unless Unified Messaging Level is set to Enhanced Forward & Copy or Enhanced Integration.
3. Click out of the field or press **Enter** to save the change.

Recording Length

You can view the number of seconds used by the mailbox directory name and the primary and alternate greetings. The information is shown for reference only. It is **not** programmable.

To view the Recording Lengths:

1. Select Voice Processor – Devices – Mailboxes – Local – **<extension>**.
2. Double-click **Recording Lengths**.

Message Limits

The message limits that can be programmed for each mailbox include the following:

- **Maximum Mailbox Message Capacity:** The mailbox can be programmed to hold up to 600 minutes of messages or have unlimited message capacity. The range is 0–600 minutes; the default value is 30 minutes. Enter 0 for unlimited capacity.
- **Maximum Non-Subscriber Message Length:** Maximum non-subscriber messages can be set to a value between one minute and the Maximum Mailbox Message Capacity setting. The range is 1 minute to the Maximum Mailbox Message Capacity value; the default value is 5 minutes.
- **Maximum Outgoing Message Length:** The length of outgoing messages by this subscriber. The range is 1–120 minutes; the default value is 5 minutes.

To change a message limit:

1. Select Voice Processor – Devices – Mailboxes – Local – **<extension>**.
2. Double-click **Message Limits**.
3. Select the Message Limit.
4. In the **Value** column, type the new number in the box. If you enter an invalid number, a warning message appears.
5. Click out of the field or press **ENTER** to save the change.

Subscriber Statistics

You can view subscriber usage statistics. The statistics reflect the period since the last date that the statistics were cleared. Statistics are cumulative and remain as such until cleared using Report Parameters. See “Enterprise Messaging Voice Processing Reports” on [page 15-6](#). The information is shown for reference only. It is **not** programmable. Statistics are as follows:

- **Last Logon Date (and Time):** Reflects the most recent date and time of the last valid logon by the subscriber. (If the System Administrator makes any change to a subscriber's personal options from the System Administrator's mailbox, no change will be made to this field.)
- **Number of New Messages:** Reflects a count of the number of messages in a subscriber's new message queue. It is the same number that is reported to the subscriber when he or she logs in to the mailbox.
- **Number of Saved Messages:** Reflects a count of the number of messages stored in the saved message queue for the mailbox. It is the same number that is reported to the subscriber when he or she logs in to the mailbox.
- **Mailbox Percent Full:** Shows the actual percentage of maximum mailbox message capacity used.
- **Number of Times Mailbox Was 80% Full:** Shows the number of times the mailbox reached 80% of its maximum message capacity.
- **Number of Times Mailbox Was Full:** Displays the number of times a mailbox reached its maximum message capacity.
- **Number of Messages Sent:** Reflects a count of the number of times a subscriber records and sends a message (to one mailbox or a group list of mailboxes), replies to a message sent by another subscriber, or forwards a message with comments.
- **Number of Messages Received:** Shows the number of messages a subscriber has received regardless of where the messages came from (subscriber, non-subscriber, or system).
- **Total Length of New and Saved Messages:** Reflects a combined total of the amount of time represented by the “Number of New Messages” and “Number of Saved Messages” fields.
- **Number of Times 3 Bad Passwords Were Entered:** Increases each time a single call includes three attempts to enter a mailbox and the caller uses an incorrect mailbox/ password combination.

To view the subscriber statistics:

1. Select Voice Processor – Devices – Mailboxes – Local – **<extension>**.
2. Double-click **Statistics**.

E-mail Reader Profiles

EM Systems Only. To use the text-to-speech (TTS) functionality to convert e-mail messages to voice mail messages, each mailbox user must have an E-Mail Reader profile. The profile contains the information that EM requires to access the correct e-mail server and e-mail account.

To create an e-mail reader profile:

1. Select Voice Processor – Devices – Mailboxes – Local – **<extension>**.
2. Double-click **E-mail Reader Profiles**.
3. Right-click in the right pane, and then select **Add to E-mail Reader Profiles List**. The Get ID dialog box appears.
4. Enter the starting ID, and then click **OK**. The ID is added to the list with a blank user name. Because you can only assign one E-Mail profile to each mailbox, you cannot change the number of IDs.
5. Double-click the ID to display the settings for that profile.
6. Complete the following options:
 - **Username:** Enter a username, up to 40 characters, for the profile. This username must match the username used to log on to the associated e-mail account.
 - **Password:** Right-click this field and select **Edit Password**. Enter a password, up to 40 characters, used to access the associated e-mail account. Confirm the password, and then click **OK**. This password must match the password used to log on to the e-mail account.

NOTE

Some networks are configured so that users are automatically logged onto their e-mail application whenever they log onto the domain. In this case, the Username and Password fields must match the user's domain account username and password.

- **Hostname:** Enter the hostname, up to 40 characters, of the E-Mail Server. The hostname is required for accessing the e-mail system and is case-sensitive.
- **Default Folder:** Enter the name of the mailbox folder, up to 40 characters, that stores the e-mail messages. By default, this is INBOX.
- **IMAP SSL:** When the this option is enabled (set to Yes), E-mail Reader uses IMAP SSL (Secure Sockets Layer) to provide an encrypted communication between the EM system and the E-mail Server. By default, it is set to Yes.
- **IMAP Port:** When the IMAP SSL option is disabled, the port which Email Reader uses to communicate with the Email Server can be configured. Email Reader uses this port number when connecting to the Email Server to retrieve email messages. By default, it is set to the standard IMAP port, 143. If IMAP SSL is enabled, the standard IMAP SSL port of 993 is used and cannot be configured. This field has a RED X when IMAP SSL is set to Yes.
- **Account E-mail Address:** Enter the e-mail address for this e-mail account. This field is used to populate the FROM address when originating e-mails. It applies to systems attached to Enterprise Messaging external VM systems. If the receiver of e-mails generated from E-mail Reader replies to the message, this E-mail address is the e-mail address to which the reply will be directed. If you enter an invalid character (: ; " \ | () , < >), an error tone occurs.

Dial-0 Destinations

The dial-0 destination is where calls are sent if callers dial 0 for the operator. Dial-0 destinations are used for Voice Mail and Automated Attendant applications.

Programming the Day and Night Dial-0 Destination Types

The following options select the type of device that is used for the day and night operator destinations:

- **None:** Operator access is denied from Voice Mail and Auto Attendant applications.
- **Extension:** The system automatically transfers the call to any system endpoint application (including a STAR application) or hunt group extension. The system software supports STAR applications as a valid Dial-0 Destination.
- **Mailbox:** The system automatically transfers the caller to the mailbox specified in the Dial-0 Destination (see the following section) when the caller dials 0.
- **Operator:** If the operator destination is set to **Operator**, the caller is transferred to the attendant.

To program the Day or Night Dial-0 Destination type:

1. Select Voice Processor – Devices – Mailboxes – Local – **<extension>**.
2. Select **Dial-0 Day** (or **Night**) **Destination Type**.
3. In the **Value** column, select the option from the list (**None**, **Extension**, **Mailbox**, or **Operator**).
4. Click out of the field or press **ENTER** to save the change.

Programming the Dial-0 Destination

If you select day or night destination types, as described in the previous section, you can select the specific device that serves as the operator destination.

To select the Dial-0 Destination:

1. Select Voice Processor – Devices – Mailboxes – Local – **<extension>**.
2. Select **Dial-0 Day** (or **Night**) **Destination Type**.
3. In the Dial-0 Destination column, right-click the existing value, and then click **Change Dial-0 Destination**. A window appears prompting for the device type to include.
4. Select the device types (you can use the SHIFT or CTRL key to select more than one item), and then click **Next**. The items with details appear. To view items in a list only, click **List**.
5. Select the desired destination, and then click **Finish**. The selection appears in the list.

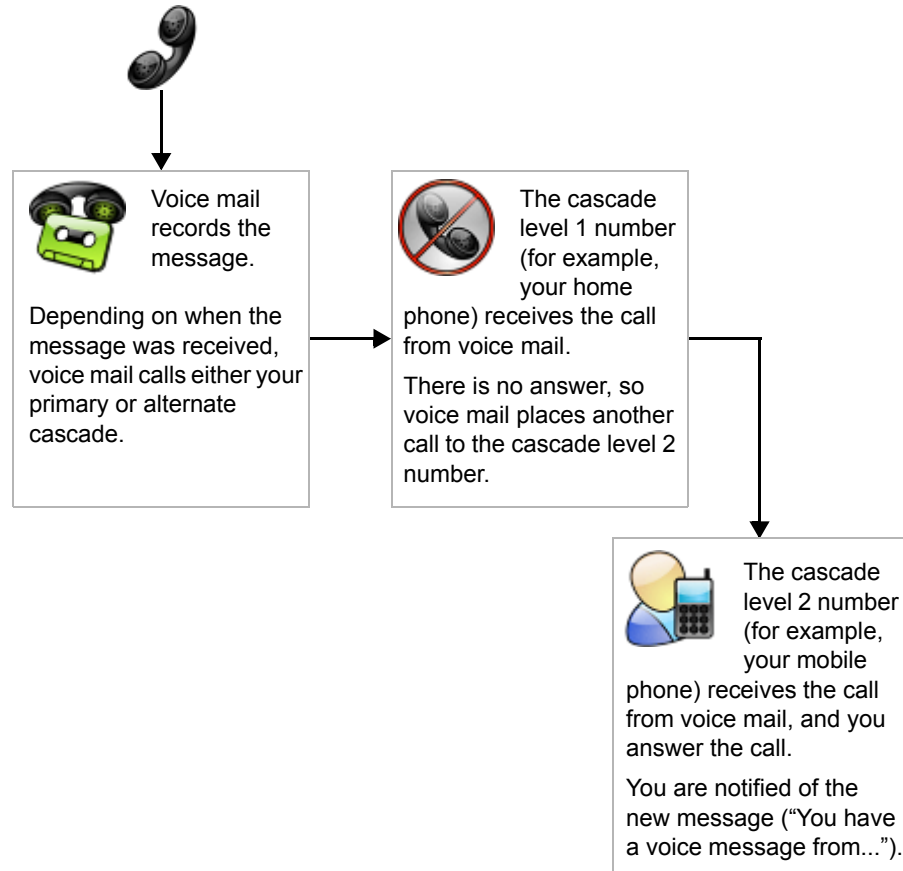
Remote Messaging

Remote Messaging places a call to subscribers when their mailboxes receive new voice messages. Using “cascade levels” of up to nine phone numbers (see [page 12-20](#)), the voice mail system calls each number until it successfully connects to a device (for example, a home phone, a mobile phone, or a pager). [Figure 12-2](#) shows an example of Remote Messaging routing.

NOTE

You cannot enable Remote Messaging unless you have programmed cascade levels (see [page 12-20](#)). If you try to enable Remote Messaging without any cascade levels, an error is displayed.

Figure 12-2. Remote Messaging Routing Example



To enable Remote Messaging:

1. Select Voice Processor – Devices – Mailboxes – Local – **<extension>** – **Remote Messaging**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Click out of the field or press **ENTER** to save the change.

Primary and Alternate Message Notification

If you enable Remote Messaging (see [page 12-19](#)), you must program either **Primary** or **Alternate Message Notification** parameters.

NOTE

If Remote Messaging is enabled, this feature is available as a programmable option to subscribers, allowing them to change the selected option.

To view or edit Primary or Alternate Message Notification Options:

Select Voice Processor – Devices – Mailboxes – Local – **<extension>** – **Primary** (or **Alternate**) **Message Notification**. The following options are shown in the right pane:

- **Cascade Levels:** Double-click **Cascade Levels** to view the list of cascades. The list appears blank if no cascade levels have been programmed. For cascade programming options, see [page 12-21](#).

NOTES

Primary and alternate cascade levels are not equipped in pairs. For example, if you add or delete a primary cascade level, a corresponding alternate cascade level is **not** automatically added or deleted.

When a Remote Message Notification call is placed, the prompt “You have received a remote message . . .” starts to play as soon as a programmable timer expires (default value is 3 seconds). Voice Processing plays the prompt five times before disconnecting the call. Playing out these prompts five times covers the (programmable) maximum number of rings and still plays at least one iteration of the prompt. User’s must press pound (#) or star (*) to stop the prompts. The programmable delay only extends the prompt replays. Users will probably hear the end of a previous prompt, but they can hear the entire prompt if they want to.

- **Notification Category:** You can set message notification to place the notification call for all messages or only when priority messages are received. The default state is “all messages.”
 - a. Select option from the list.
 - b. Press **ENTER** or click another field to save the change.
- **Call For Each New Message:** This determines whether the Voice Processor should attempt message notification every time a message is received (that meets the notification category set above), or only when a message is received and no other messages are waiting to be picked up.

To change the setting:

- a. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
 - b. Press **ENTER** or click another field to save the change.
- **Start/Stop Time:** Message notification can be enabled for any time period, up to 24 hours per day. Default is 8:00AM to 5:00PM. If start and stop times are the same, notification will be enabled 24 hours per day.

To set the time:

 - a. Select the current Value, then select the hours, minutes, or AM/PM field, and use the arrows to scroll to the desired setting.
 - b. Select another field or press **ENTER** to save the change.
 - **Days Of The Week:** Message notification can be set to place notification calls only on certain days. (This defaults to Monday through Friday.)

To enable a day:

- a. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
- b. Press **ENTER** or click another field to save the change.

Adding Cascade Levels

To add cascade levels:

1. Select Voice Processor – Devices – Mailboxes – Local – *<extension>* – **Primary** (or **Alternate**) **Message Notification**.
2. Right-click in the right pane, and then select **Add cascade level(s)**.
3. Select the starting ID and the number of levels you want to add. (For example, to add 9 levels with IDs 1–9, select 1 as the **Starting ID** and 9 as the **Number of IDs**.)
4. Click **OK**. The levels are added to the list with default values. You can then change the Notification Number for any cascade by entering the new number in its text box. You can also set the Notification flag by placing a check in the check box in this screen or in the cascade settings described below.

Deleting Cascade Levels

To delete cascade levels:

1. Select Voice Processor – Devices – Mailboxes – Local – *<extension>* – **Primary** (or **Alternate**) **Message Notification**.
2. Right-click the cascade level that you want to remove, and then select **Remove Selected Item**.

Programming Cascade Level Options

To program the cascade level options:

1. Select Voice Processor – Devices – Mailboxes – Local – *<extension>* – **Primary** (or **Alternate**) **Message Notification**.
2. Double-click **Cascade Levels**.
3. Double-click the cascade level you want to program to view the following options:
 - **Timers and Limits:** Double-click Timers and Limits to program the following. If necessary, enter a new Value, then press **ENTER** or click another field to save the change.
 - *Number Of Call Attempts:* Determines how many times the Voice Processor will attempt to complete a call to this cascade level before moving to the next level. The range is 1–1000 call attempts; the default value is 1.
 - *Number Called Busy Timer:* Defines the amount of time the Voice Processor will wait between outgoing call attempts whenever a busy signal is encountered during a remote message notification attempt to a personal number or pager. The range is 0–1440 minutes; the default value is 5.
 - *Personal Number No Answer Timer:* Defines the amount of time the Voice Processor will wait between outgoing call attempts whenever a message notification attempt to a personal number is unanswered. The range is 0–1440 minutes; the default value is 30.
 - *Pager Notification Retry Timer:* Reflects the amount of time the Voice Processor will wait between outgoing call attempts when the notification number is a pager. The range is 0–1440 minutes; the default value is 20.

- **Enable Notification:** Each cascade can be enabled or disabled individually. To change the setting, click the check box to place a mark in it and set the flag to **Yes**. (Or click an existing mark to disable it and change the flag to **No**.) Press **ENTER** or click another field to save the change.
- **Call Progress Detection:** This determines if the Voice Processor will perform call progress detection after dialing the notification number and outgoing termination fields on outside calls. If it is enabled, the system will analyze call progress tones after sending the number. If it is disabled, the system will assume the call has been answered, without analyzing tones. This should only be disabled in cases where call progress tones are not used (lighting a message lamp) or when the tones used by the destination cannot be recognized by the system (some pager destinations). To change the setting, select the check box to remove the mark in it and set the flag to **No**. (Or click it again to enable it and change the flag to **Yes**.) Press **ENTER** or click another field to save the change.
- **Notification Type:** The message notification number can be identified as a personal number (a person will answer the call) or a pager. (This defaults to "personal number.") Select the option from the list. Press **ENTER** or click another field to save the change.
- **Notification Destination Type:** This indicates whether the notification call is going to an intercom (IC) or outside (CO) destination. This can also be programmed by the mailbox Subscriber. Select the drop-down list box and scroll to the desired setting. Press **ENTER** or click another field to save the change.
- **Notification Destination:** This is the number (outside number, local extension, or off-node extension) to be notified when the mailbox receives a message. If the Notification Destination Type is IC, right-click the field and select **Change Notification Destination**. Program the destination device. If the Notification Destination Type is CO, enter the outside number in the text box. Press **ENTER** or click another field to save the change. The outside number can contain up to 24 characters including digits (0–9, #, and *) or P for pauses. This number should not include pager display numbers; they are programmed below.
- **Pager Dial String:** This digit string can contain up to 54 characters. It should include any digits that the paging company requires when the call is answered, the pager LCD number, and the pager termination code, if needed. Valid entries include: any digit 0–9, #, *, P for pause. Also, if you want to have the pager show the number of the mailbox that placed the call, you can use an M in the dial string. To show the number of waiting messages for the mailbox, use an N. For example, if the Pager String is programmed as 9619000*MN# and a pager call is placed by mailbox number 1234 which has 3 waiting messages, the pager display would show 9619000*12343 (the # is used as a call termination digit). Enter the dial string in the text box, then press **ENTER** or click another field to save the change.
- **Outgoing Access:** This is used to identify the trunk group that will be used for placing remote notification calls. To change the trunk group, right-click **Value** and select **Change Outgoing Access**. In the first window, scroll to CO Trunk Groups, then click **Next**. In the next window, select the desired trunk group, then click **Finish** to exit.
- **Outgoing Access Prefix:** This is the dial string that the system uses before an outgoing number, if any. Enter the dial string in the text box and then press **ENTER** or click another field to save the change.
- **Outgoing Termination:** This is the dial string that the system uses to terminate an outgoing number, if any. Enter the dial string in the text box, then press **ENTER** or click another field to save the change.

Mailbox Initialized

This field indicates whether the subscriber has initialized the mailbox and recorded a name in the company directory. The field is shown for reference only and is not programmable.

To view the Mailbox Initialized field:

Select Voice Processor – Devices – Mailboxes – Local – **<extension>**. The Mailbox Initialized option is shown in the right pane.

Receive Only

You can program mailboxes as “Receive Only.” Receive Only mailboxes cannot be used to send messages. By default, mailboxes do not have this option enabled.

To make the mailbox receive-only:

1. Select Voice Processor – Devices – Mailboxes – Local – **<extension>** – **Receive Only**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Click out of the field or press **ENTER** to save the change.

Allow Transfer Method Programming

This option determines whether the subscriber (or voice mail administrator) can change the Transfer Method using the voice mail Personal Options prompts. If enabled, it allows user programming. If disabled, you must change the Transfer Method in DB Programming.

1. Select Voice Processor – Devices – Mailboxes – **<node>** – **<extension>** – **Allow Transfer Method Programming**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Click out of the field or press **ENTER** to save the change.

Play Recording Instructions

If this option is enabled, the system prompt that tells the caller to leave a message after the beep plays after the primary or alternate greeting. If disabled, the beep occurs as soon as the primary or alternate greeting ends, and the system prompt does not play. By default, this option is enabled.

Use of this option is subject to the following conditions:

- If the system greeting is selected, the instructions cannot be disabled.
- If the primary greeting is selected and has not been recorded, the instructions cannot be disabled.
- If the secondary greeting is selected and has not been recorded, the instructions cannot be disabled.

To disable the instructions that play after the primary or alternate greeting:

1. Select Voice Processor – Devices – Mailboxes – Local – **<extension>** – **Play Recording Instructions**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Click out of the field or press **ENTER** to save the change.

Auto Attendant Transfer Prompt

The Auto Attendant Transfer Prompts determines whether the transfer prompt ("Please hold while your call is being transferred to...") plays after a caller has entered the extension number of the endpoint associated with this mailbox. This applies to calls transferred by Automated Attendant and Call Routing Announcement applications, including transfers to the operator's mailbox or extension ID. This option is enabled by default.

To disable the prompt:

1. Select Voice Processor – Devices – Mailboxes – *<node>* – *<extension>* – **Auto Attendant Transfer Prompt**.
2. In the **Value** column, clear the check box. The field changes to **No**. To enable the option, select the check box.
3. Click out of the field or press **ENTER** to save the change.

Deliver Hangup Message (when ANI is available)

This option determines when to leave an "indication message" if the caller hangs up. This indication message is a system-generated message that states there was an incoming call to the voice mailbox but that no voice message was left. The purpose of this indication message is to capture Caller ID (CLID) information for the call and display it on the endpoint. If the Deliver Hangup Message (when ANI is available) field is set to Yes (default), the system leaves indication messages for calls that are shorter than the Shortest Message Allowed timer (Voice Processing\Timers and Limits\Timers and Limits). If set to No, the feature is disabled, and the system does not leave an indication message.

To disable the Deliver Hangup Message (when ANI is available) option:

1. Select Voice Processor – Devices – Mailboxes – Local – *<extension>* – **Deliver Hangup Message (when ANI is available)**.
2. In the **Value** column, clear the check box. The field changes to **No**.
3. Click out of the field or press **ENTER** to save the change.

Swap “7 for Save” and “9 for Delete” Message Keys

NOTES

This feature will not be available for EM until the EM v2.0 release.

This feature is available as a programmable option to subscribers, allowing them to change the selected option.

Swap “7 for Save” and “9 for Delete” Message Keys feature applies to BVM and EM only.

You can use the Swap “7 for Save” and “9 for Delete” Message Keys to reverse the 7 and 9 digit operations in subscribers’ Message Options. By default, the 7 digit is used for SAVE and the 9 digit is used for DELETE. With the swap feature, you can use the 7 digit for DELETE and the 9 digit for SAVE, just like cell phone voice mail system functionality.

This helps users who are familiar with cell phone functionality from accidentally deleting messages by pressing 9, intending to save messages. Subscribers can program this feature for their mailboxes (see below) or you can program this feature for all subscribers in the voice processing system settings.

To swap the keys for individual mailboxes:

1. Select Voice Processor – Devices – Mailboxes – Local – *<extension>* – **Swap “7 for Save” and “9 for Delete” Message Keys**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Click out of the field or press **ENTER** to save the change.

Designate this Mailbox for Play Only

Applies to BVM non-associated mailboxes only. The BVM “play-only” mailbox option prevents the caller from leaving a message. The “play-only” mailbox is similar to an “announcement-only” application where it plays the designated greeting once, and then the call automatically disconnects after the greeting finishes playing.

This feature allows a subscriber to record a custom message without requiring administrative access to voice mail. For example, a teacher (the “subscriber”) could record a homework assignment message for students who missed class that day. The students could then retrieve the message from the mailbox, but they would not be able to leave messages in the mailbox.

Each BVM mailbox in DB Programming, now has an option to indicate if it is “play-only.” The default value is set to “No” for all mailbox types.

To enable or disable an unassociated mailbox for play only:

1. Select Voice Processor – Devices – Mailboxes – Local – *<extension>* – **Designate This Mailbox for Play-Only**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Click out of the field or press **ENTER** to save the change.

Password

You can program the passwords that subscribers use to access their mailboxes.

NOTES

To provide system security, *all* mailboxes should have a password. To make the passwords difficult to guess, they should **not** match the mailbox number or consist of one digit repeated several times. The default password should be changed the first time the user logs in. This is especially important in the voice mail administrator mailbox, which allows programming access to the voice processor. This feature is available as a programmable option to subscribers, allowing them to change the selected option.

To program a mailbox password:

1. Select Voice Processor – Devices – Mailboxes – *<node>* – **<extension>**.
2. Right-click **Password**, and then select **Edit Password**. The Edit Password dialog box appears.
3. In the **New Password** box, type the password (up to 12 digits, using digits 0–9). The digits appear as asterisks (***) in the box.
4. In the **Confirm password** box, retype the password.
5. Click **OK** to exit and save the password.

Greeting

You can enable one of the following greetings:

- **System:** The default greeting that callers hear when they access subscribers' mailboxes. The following is an example system greeting. "*<Subscriber's name>* is not available. After the tone please record your message. When finished leaving your message, hang up, or press # for more options."
- **Primary:** The "standard" greeting used by subscribers who are unavailable to take calls. Subscribers record their own primary greetings.
- **Alternate:** An alternate greeting that subscribers can use for vacations, days off, and so on.

NOTE

This feature is available as a programmable option to subscribers, allowing them to change the selected option.

To select the voice mail greeting:

1. Select Voice Processor – Devices – Mailboxes – Local – *<extension>* – **Greeting**.
2. In the **Value** column, select the greeting from the list (Primary, Alternate, or System Greeting). Even if you select Primary or Alternate greeting, the System greeting plays until the subscriber records the selected greeting.
3. Click out of the field or press **ENTER** to save the change.

Transfer Method

(Applies to associated mailboxes only.) When a call is received by an automated attendant and the caller enters an extension number, the Transfer Method determines how the call is transferred. Transfer Methods are as follows:

- **Announce-Only:** The caller is asked to state their name, and then the call is transferred to the associated extension number. When the endpoint user answers the transfer, the system plays the caller's name and completes the transfer.
- **Screened:** The caller is asked to state their name, and then the call is transferred to the associated extension number. When the endpoint user answers the transfer, the system plays the caller's name. The endpoint user has the options of replaying the name, sending the call to voice mail (if the extension has a mailbox), transferring the call to another extension, accepting the call, or rejecting the call.
- **Unannounced:** The call is transferred to the associated extension number after the system checks the endpoint to determine its status (busy, available, ringing, and so on).

NOTE

This feature is available as a programmable option to subscribers, allowing them to change the selected option.

To select a Transfer Method:

1. Select Voice Processor – Devices – Mailboxes – *<node>* – *<extension>* – **Transfer Method**.
2. In the **Value** column, select the option from the list.
3. Click out of the field or press **ENTER** to save the change.

Message Notification Endpoint

(Applies to non-associated mailboxes only.) Each mailbox has an endpoint that receives message notification whenever the mailbox receives a message. This is usually the same number as the mailbox. However, when a mailbox is shared by several endpoints or belongs to a hunt group, a specific endpoint must be designated to receive the message notification. If non-associated mailboxes are programmed, you must disable the Validate Voice Mailbox Number feature (see [page 10-23](#)) to allow subscribers to dial the non-associated mailbox number.

To designate the Message Notification endpoint:

Use one of the following methods:

Method A

- a. Select Voice Processor – Devices – Mailboxes – Local – *<non-associated mailbox extension>* – **Message Notification Endpoint**.
- b. In the **Value** column, select the current value, and then enter the new extension number in the box.
- c. Click out of the field or press **ENTER** to save the change.

Method B

- a. Right-click the existing extension number, and then select **Message Notification Endpoint**. A dialog box appears prompting for the device type to include.
- b. Select the device type, and then click **Next**. The list of devices with details appears. To view the items in a list only, click **List**.
- c. Select the appropriate endpoint, then click **Finish**. The selection appears in the Message Notification Endpoint field.

Time Zone

If the mailbox is located in a different time zone than the external voice processing system, you can set the Time Zone option to match voice processing system location. This allows the time stamp on voice mail messages to reflect the correct time for that mailbox location.

To set the time zone:

1. Select Voice Processor – Devices – Mailboxes – Local – *<extension>* – **Time Zone**.
2. In the **Value** column, select the time zone from the list.
3. Click out of the field or press **ENTER** to save the change.

Automatic Speech Recognition (ASR) Setting

The Automatic Speech Recognition (ASR) Setting determines whether the system uses the ASR Enabled value in the current folder level or in the next folder level. Depending on the folder level, you may have one or more of the following options:

- **Active:** Applies to the system, applications, and mailboxes. Indicates that the system uses the ASR Enabled setting for the current folder. If selected, any subfolders that have the ASR options automatically use the ASR Enabled setting for this folder. This is the default for all folder levels.
- **Delegated:** Applies to system and applications only. Indicates that the system uses the ASR Enabled setting for the next folder level.
- **Ignored:** Applies to applications and mailboxes only. Indicates that the system ignores the ASR Enabled setting for this folder. This folder then uses the settings programmed for the parent level. For example, mailboxes use the setting specified for the application, and applications use the setting specified for the system.
- **Ignored and Delegated:** Applies to applications only. Indicates that the system ignores the ASR Enabled value for this folder and uses the parent-level folder—that is, the Voice Processor folder. If, however, the Voice Processor folder ASR Setting field is set to Delegated, this folder uses the settings programmed for the next folder level—that is, the mailbox folder.

For a table that identifies the possible configuration combinations for the ASR Enabled and ASR Setting fields, see Table 11-1 on [page 11-23](#). For programming details, refer to *Mitel 5000 DB Programming Help*.

Automatic Speech Recognition (ASR) Enabled

The value placed in the ASR Enabled field determines whether or not ASR is enabled for the current folder, as well as any subfolders or parent folders based on the value in the ASR Setting field. If enabled, the system, application, or mailbox supports voice recognition for accessing that particular feature. If disabled, the system, application, or mailbox does not support voice recognition.

If the ASR Setting is set to Delegated, Ignored, or Ignored and Delegated, the system ignores the ASR Enabled field and displays a red “X”.

For a table that identifies the possible configuration combinations for the ASR Enabled and ASR Setting fields, see Table 11-1 on [page 11-23](#). For programming details, refer to *Mitel 5000 DB Programming Help*.

Quota Warning

Select the threshold that must be met before the system generates a warning to the subscriber. This value is set as a percentage of the Maximum Mailbox Message Capacity (under Message Limits). For example, if this value is set to 80 and the Maximum Mailbox Message Capacity value is set to 30 minutes, a warning message is issued when the number of voice mail messages totals 24 minutes (80% of 30 minutes). This warning prompt is then played each time the user accesses their mailbox. The warning prompt is no longer played after the mailbox storage total falls below the quota warning threshold. The valid range is 0–100 percent, and the default is 80. If set to 0 or 100, no warning message is issued.

To set the Quota Warning value:

1. Select Voice Processor – Devices – Mailboxes – Local – *<extension>* – **Quota Warning**.
2. In the **Value** column, select the option from the list.
3. Click out of the field or press **ENTER** to save the change.

Quota Grace

Select the amount of additional storage that the system allows once the Maximum Mailbox Message Capacity limit (under Message Limits) is met. This value is also set as a percentage of the Maximum Mailbox Message Capacity. To determine the point at which messages are denied, the system adds the quota grace value to the total capacity limit. For example, if this value is set to 80 and the Maximum Mailbox Message Capacity is set to 30 minutes, the system does not store messages once the number of voice mail messages totals 54 minutes ($30 + .8 \times 30$). When this capacity is reached, a voice mail prompt informs the user that their mailbox is currently full. The valid range is –1 to 100 percent, and the default is 0, which indicates that no grace is allowed. For unlimited messages, set this value to –1.

To set the Quota Grace value:

1. Select Voice Processor – Devices – Mailboxes – Local – *<extension>* – **Quota Grace**.
2. In the **Value** column, select the option from the list.
3. Click out of the field or press **ENTER** to save the change.

Mailbox-Related Information

You can view voice processing mailbox statistics. This information is presented for reference only and cannot be programmed. Statistics continue to accumulate until they are cleared using the Voice Processor Report Programming window. See “Application and Channel Statistics” on [page 15-6](#)) for more information.

To view mailbox statistics:

Select System – **Mailbox-Related Information**. The following statistics are shown in the right pane:

- **Number of Mailboxes:** The number of mailboxes that have been created in voice mail.
- **Number of Messages Sent:** A count of the number of times subscribers have recorded and sent messages to one mailbox or to a group list of mailboxes, replied to a message sent by another subscriber, or forwarded a message with comments.
- **Number of Messages Received:** The number of messages that subscribers have received regardless of the origination of the message—subscriber, non-subscriber, or system.
- **Number of Messages Received From Remote Nodes:** The number of messages that subscribers have received from endpoints on other nodes.
- **Number of New Messages:** The total of the number of messages in all subscribers’ new message queues.
- **Number of Saved Messages:** The total of the number of messages stored in the saved message queues for all mailboxes.
- **Total Length of New and Saved Messages:** A combined total of the amount of time represented by the “Number of New Messages” and “Number of Saved Messages” fields.
- **Average Mailbox Percent Full:** The average percentage of maximum message capacity used by all mailboxes.
- **Number of Times Mailbox Was Full:** The number of times any mailbox reached its maximum message capacity.
- **Number of Times Mailbox Was 80% Full:** The number of times any mailbox reached 80% of its maximum message capacity.
- **Number of Times 3 Bad Passwords Were Entered:** The number of times that subscribers attempted to use an incorrect password three times in row to connect to a mailbox.
- **Number of Mailboxes Currently Full:** The number of mailboxes that are currently at their maximum capacity.
- **Number of Mailboxes Currently More Than 80% Full:** The number of mailboxes that are currently over 80% of their maximum message capacity.

Voice Processing Management

Introduction	13-2
Enable Diagnostics	13-2
Saving and Restoring Voice Processing Databases	13-3
Summary of Voice Processor Save and Restore Options	13-3
Voice Processor Save and Restore	13-4
Voice Processor Save Guidelines	13-5
Save To or Restore To Location	13-5
Options	13-6
Completing the Save/Restore	13-7
Enabling or Disabling a Voice Processor	13-8
Saving a Voice Processor Database in Remote Mode	13-8
Selecting a Voice Processor Type in Local Mode	13-9
Saving or Restoring an EM Database	13-11
Saving or Restoring a CS-5600 Database on a Remote Windows Computer	13-15
Saving/Restoring Mitel CS-5600 BVM Data	13-19
Save/Restore BVM Data to a Network File Server (NFS)-Supported Computer	13-20

Introduction

This chapter describes tools that you can use for Basic Voice Mail (BVM) maintenance and how to save or restore BVM databases. For Enterprise® Messaging (EM) voice processing systems, refer to the *Enterprise Messaging Installation and Maintenance Manual*, part number 780.8006 . For NuPoint Messenger system maintenance, refer to *NuPoint Messenger Technical Documentation Help*.

Enable Diagnostics

When the Enable Diagnostics option is selected, voice processor logs all diagnostics output (including alarms) generated by the voice processor computer to a file. Using that file, you can troubleshoot problems dealing with message lamps, delayed messages, remote messaging, etc. By default, this flag is disabled.

There are five diagnostics log files: log, log.1, log.2, log.3 and log.4. Information is initially written to the log file, when this file becomes full its contents are transferred to the log.1 file. The log.1 file contents are transferred down to the log.2 file, whose contents are transferred to the log.3 file, whose contents are transferred to the log.4 file. The information contained in log.4 is discarded permanently each time log.3 is transferred.

Diagnostics may be left on at all times without affecting performance. The number and size of the log files can be changed. For a complete list of diagnostic codes, refer to the *Message Print Diagnostics Manual*, part no. 550.8018, which is supplied on the System software CD. You can also find all documentation on the [edGe Online Manuals and Guides Web site](http://www.intel.com/techpublications) (www.intel.com/techpublications).

To select the Enable Diagnostics option:

1. Select Voice Processor – Maintenance – **Enable Diagnostics**.
2. In the **Value** column, select the check box. The field changes to **Yes**. To disable the option, clear the check box.
3. Click out of the field or press **ENTER** to save the change.

Saving and Restoring Voice Processing Databases

NOTE

Saving or restoring a database causes the system to slow down. If possible, do not perform these operations during normal business hours.

Summary of Voice Processor Save and Restore Options

With Mitel CS-5200 or CS-5400 platforms, you can save or restore Basic Voice Mail (BVM) databases using the USB-A drive on the front of the Base Server chassis only. (Mitel CS-5600 BVM databases are stored on the hard drive.) If a system is equipped with Enterprise Messaging (EM), you can save or restore the database either to USB flash drive or to a local EM drive.

You can save and restore BVM and EM databases to a USB flash drive. You can save an EM database to the local drive of the attached voice processor. For CS-5600 platforms licensed to run 16-port BVM, you can save/restore BVM data to a remote computer after setting up a shared folder on the computer.

You can save/restore BVM to a remote computer running Windows 2000 or later or to a Linux/Unix Network File System (NFS) shared folder.

NOTE

Before you can save/restore BVM data to a remote Windows or Linux/Unix computer, you must set up a shared folder on the remote computer.

For detailed instructions as applicable, see “Saving or Restoring a CS-5600 Database on a Remote Windows Computer” on [page 13-15](#) or “Save/Restore BVM Data to a Network File Server (NFS)-Supported Computer” on [page 13-20](#).

[Table 13-1](#) shows the options available for saving and restoring voice processor databases.

Table 13-1. *Voice Processor Database Save/Restore Options*

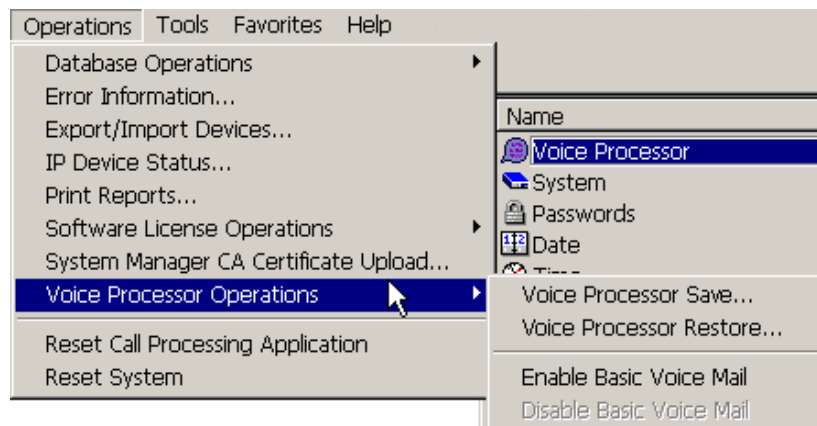
System	Version	With BVM	With EM
Mitel CS-5200	2.x or later	To USB	To USB or EM local
Mitel CS-5400	2.x or later	To USB	To USB or EM local
Mitel CS-5600	2.x or later	To USB or Remote Windows or Remote NFS	To USB or EM local

NOTE

You can use save or restore all fields except the Call Processing Server password. Also, an error message appears if you attempt to restore an incompatible system type onto a system. For example, you cannot restore a Mitel CS-5400 database onto a Mitel CS-5600 system and vice versa.

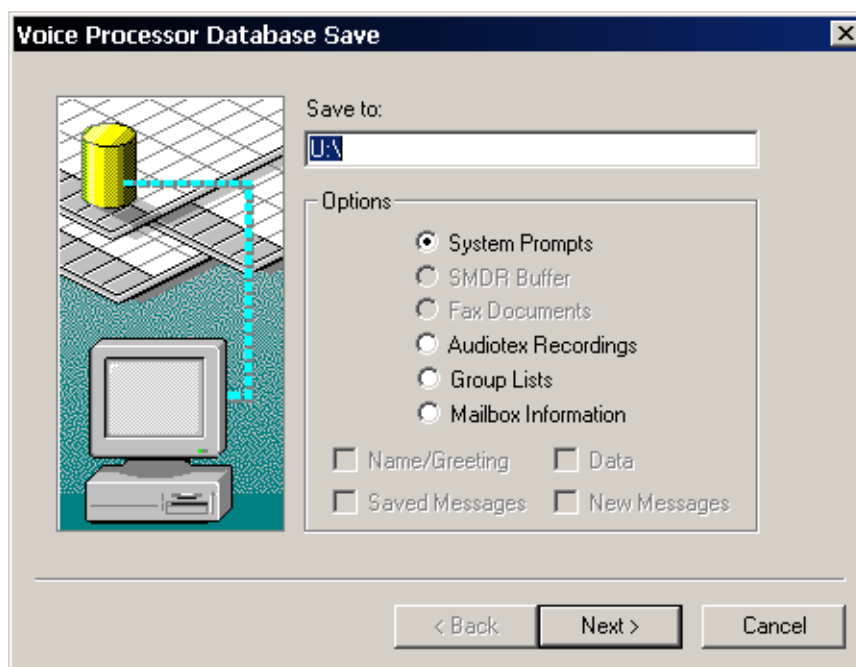
Voice Processor Save and Restore

The selective Voice Processor Save and Restore options are available under the Operations menu.



When you select either Voice Processor Save or Voice Processor Restore from the Operations – Voice Processor Operations submenu, one of the following window appears. When using Basic Voice Mail, the SMDR Buffer and Fax Document options are not available.

Figure 13-1. Voice Processor Save/Restore Dialog Boxes



Voice Processor Save Guidelines

Keep the following guidelines in mind when saving voice processor information:

- If you are using an external voice processing system, make sure the system is attached during a restore. If the external voice processing system is not attached, the system will not restore the non-associated mailbox information.
- If saving to a USB flash drive, make sure the flash drive is inserted on the Mitel 5000 Base Server *before* continuing with any voice processing database or restore operations. Create any specific directories *only while the USB flash drive is inserted into the Mitel 5000 Base Server chassis*. After performing the save operation, remove the USB flash drive, then reinsert it to verify the information in the directories you created. You will need to repeat the save operation for each subdirectory created.
- If saving external voice processing information to floppy diskettes, ensure you have enough diskettes for saving the data. Check the Disk Usage Statistics report (as shown on [page 11-18](#)) to determine the number of minutes used for the prompts and messages. Each diskette will typically hold around 5 or 6 minutes of prompts and/or messages. To calculate the number of diskettes needed, divide the number of minutes used (shown in the statistics) by 5. If applicable, use a mapped drive or CD-ROM drive instead of floppy disks.

Save To or Restore To Location

If saving or restoring to a USB flash drive (Basic Voice Mail only), `U:\` appears in the Save To/Restore From field. If using an external voice processing PC, set the Save to and Restore from fields accordingly. For example, `A:\<path>` if using floppies or `D:\` if using CD-ROM or other drive where the voice data was saved to or will be restored from.

NOTES

Always use the option to save voice data if you are defaulting the database or changing the flash card, as this does a complete save of the system and voice information. When you then do a restore, all messages are restored as saved and new respectively.

If you simply save the voice data then default the database or change the flash card, or remove the messages through the database or the endpoint, the restored voice data will be restored as new.

Selecting the desired drive places a dot in the option button. Place a diskette in the correct drive on the voice processor computer before selecting **Next**. If you are using the USB flash drive for BVM, make sure the drive is inserted into the Mitel 5000 system before specifying the save to or restore from options.

NOTICE

Possible Database Loss and VM System Inoperability. When an external voice processing system performs a save operation, it erases files and/or directories from the UNC_path. Therefore, be careful when specifying the save/restore path. For example, do not specify `C:\` as the save/restore path because the external voice processing system would delete the entire C drive.

Options

Select information you want to save or restore from the following list. If you select Mailbox Information, you will also need to select the types of information by clicking the appropriate check boxes. Restoring Voice Processor data will not allow you to create new mailboxes or group lists. You can only restore data to mailboxes and groups lists that already exist in the System database.

NOTE

When using a USB flash drive to back up Basic Voice Mail, and you want to back up specific voice data, create subdirectories on the flash drive while it is in the Mitel 5000 Base Server. For example, to back up prompts, create a subdirectory at the root level of the flash drive such as U:\prompts. Specify this as the Save to location in the dialog box shown in Figure 13-1 “Voice Processor Save/Restore Dialog Boxes” on [page 13-4](#). Repeat the save to process for each subdirectory.

- **System Prompts:** The system prompts (default and customized) will be saved or restored. Restored information will overwrite the current prompts, if any.
- **Fax Documents:** All fax documents in the database will be saved or restored. Restored documents will overwrite existing documents of the same number, if any.
- **Audiotex Recordings:** All audiotex recordings will be saved or restored. Restored recordings will overwrite the current recordings of the same number, if any.
- **Group Lists:** All group lists and group list directory information in the database will be saved or restored. Restored information will overwrite existing information for group lists of the same number, if any.
- **Mailbox Information:** You can select the mailboxes information to be included. Depending on the items checked, the following will be saved or restored:
 - **Name/Greeting:** Name and greetings recorded by the Subscribers, including primary and alternate greetings and directory names for extension IDs.
 - **Saved Messages:** Messages that have been saved by the Subscribers.
 - **Data:** User statistics for each mailbox and extension ID.
 - **New Messages:** New and undelivered messages that have not been heard by the Subscribers.

NOTES

Restored mailbox information overwrites existing information in the database. If any certified messages are restored, the “certified” flag will be cleared so that the sender does not receive duplicate receipt messages. If a message being restored is already in the mailbox, the message will not be copied from the disk. It will not create a duplicate copy of the message.

Restored messages appear labeled as “New” after the restore has completed.

Completing the Save/Restore

Selecting Recordings, Group Lists, or Mailboxes: If you are saving recordings, group lists, or mailbox information, you must select the items you want to save. When you click **Next**, a window appears that allows you to select the items that you want to save. You can select several consecutive items by selecting one, holding down **SHIFT** and then selecting the last. Or you can select individual items by holding down **CTRL** while clicking on the desired items. When you have finished, click **Next** again.

Next/Back: When you click **Next**, the selected information is displayed for reference. If it is not correct, select **Back** and correct the information. If it is correct, click **Finish** to continue.

Finish: When you click **Finish**, the information will be saved or restored to the selected drive. The following windows may appear:

- A restore operation begins with a warning that the database is about to be overwritten with the new data. You are given the choice of allowing the overwrite (select **Yes**) or canceling the restore process (select **No**).

If using a USB flash drive to back up Basic Voice Mail, and you want to back up specific voice data, create subdirectories on the flash drive while it is in the Mitel 5000 Base Server. For example, to back up prompts, create a subdirectory at the root level of the flash drive such as U:\prompts. Specify this as the Save to location in the dialog box in Figure 13-1 “Voice Processor Save/Restore Dialog Boxes” on [page 13-4](#). Perform the save operation for each subdirectory.

If using diskettes with an external voice processing system, use a separate disk for each type of save (System Prompts, SMDR Buffer, and Fax Documents). Each time you perform a save operation, **all files** on the disk are erased and replaced with the new saved information.

- During a save or restore process, a window appears that shows the percentage of the database that has been copied. To cancel the save or restore operation, select **Cancel**.

NOTE

Canceling a restore operation will cause the system to default the Voice Processor database.

- If restoring mailbox information, group lists, or audiotex messages, place the **last** disk of the saved information in the drive. This disk has the file that tells the system which information was saved and has the requested information included in the saved data. The system checks to see if the requested information is contained on the disks. If not, you will see an error message. If the information is available, you will be instructed to insert the appropriate disk(s) to complete the restore operation. Only the information you checked in the Save/Restore windows will be restored to the system, even if other information is present on the disks.

The Voice Processor applications and/or mailboxes will not be usable while they are being saved or restored and callers will receive reorder tones. This is necessary to prevent users from making new recordings and causing database errors. *If a mailbox is busy when you attempt to restore it*, you will receive a warning message with the following three options:

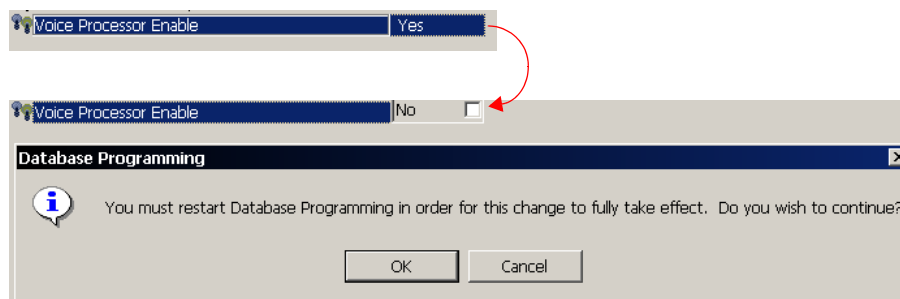
- **Abort the Save/Restore operation:** This terminates the entire save or restore operation, even if you were performing the operation for more than one mailbox.
- **Cancel the operation for that mailbox:** This terminates the save or restore operation for the busy mailbox.
- **Try again:** If you are saving or restoring multiple mailboxes, it places the busy mailbox at the end of the list and retries it later. If only one mailbox is being restored, it immediately tries again. If the mailbox is still busy when retried, you receive the three options again.

Enabling or Disabling a Voice Processor

You can enable or disable the voice processing application.

To disable voice processing:

1. Back up the Voice Mail database. You need a USB flash drive for this operation if backing up Basic Voice Mail. See “Voice Processor Save and Restore” on [page 13-4](#).
2. Launch Session Manager and start the DB Programming session.
3. Select the **System** folder, and then click **Voice Processor Enable**.
4. Click the **Yes** value, and then click in the check box to remove the check mark. Click outside the area to implement the change. Click **OK** to the prompt that appears. DB Programming restarts.



The Voice Processor Enable database field is autoenabled by Call Processing. For example, if the Voice Processor Enable flag is set to No, and the user successfully connects an external voice processing system or enables Basic Voice Mail, Call Processing auto-enables the flag. However, if DB Programming is currently programming the switch, the auto-enable flag does **not** get automatically enabled.

NOTE

In its default state, this flag is turned ON. If you do not have an external voice processing system connected to the Mitel 5000 Base Server, make sure to turn this flag OFF before attempting to import or export information over the network.

Saving a Voice Processor Database in Remote Mode

You can save BVM or EM databases in remote mode. For proper configuration, DB Programming requires that the voice processor type is identified. After the voice processor is physically connected, the system senses which type it is.

A voice processor connected to a Mitel 5000 platform auto-enables when the system boots up. To avoid the risk of overwriting an established database with default values, Mitel recommends connecting the voice processor first, then connecting with a remote mode session of DB Programming, and then saving.

To save a voice processor database in remote mode:

1. Connect the PS-1 or EM equipment to the system in accordance with installation instructions. Refer to the applicable installation manual.
2. In remote mode, launch Session Manager and start a DB Programming session.
3. From the DB Studio menu bar, select Operations – Database Operations – **Database Save**. Identify the location where you want to store the system database, then select the Save Voice Data to: check box and identify the location where you want to save the voice processor database.
4. Click **Start**. System and voice processor databases are saved to the locations indicated.

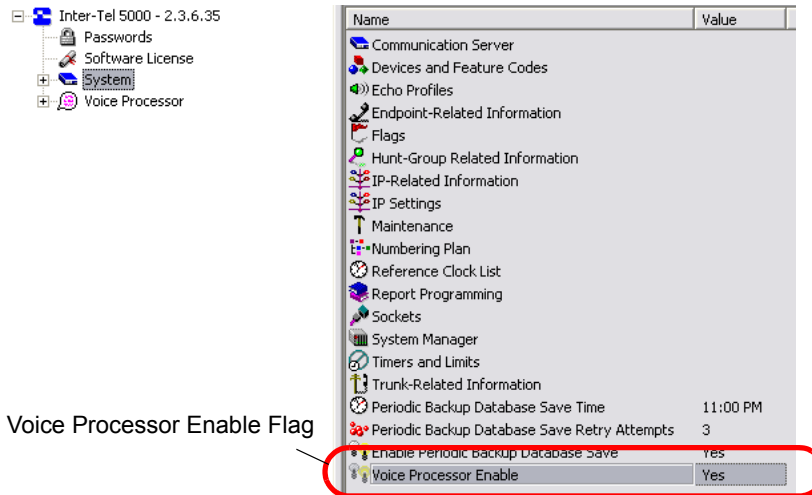
Selecting a Voice Processor Type in Local Mode

When you enable a voice processor in local mode, you may be prompted to choose a voice processor type. The Select a Voice Processor Type dialog appears *only* if you have saved the database from a remote session that did **not** have the voice processor physically connected. For the recommended process, see “Saving a Voice Processor Database in Remote Mode” on [page 13-8](#).

The Select a Voice Processor Type dialog allows you to identify a known type of voice processor that has not been enabled in the system configuration. It does *not*, however, allow you to change a voice processor type after the database has been created.

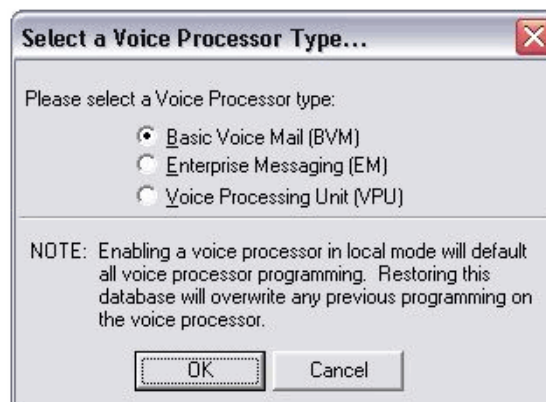
To enable a voice processor in local mode:

1. Launch Session Manager and start a session of Database (DB) Programming.
2. From the left pane of the DB Studio main screen, select the System folder. Contents of the System folder appear in the right pane.
3. Click the value of the Voice Processor Enable feature to **Yes**.

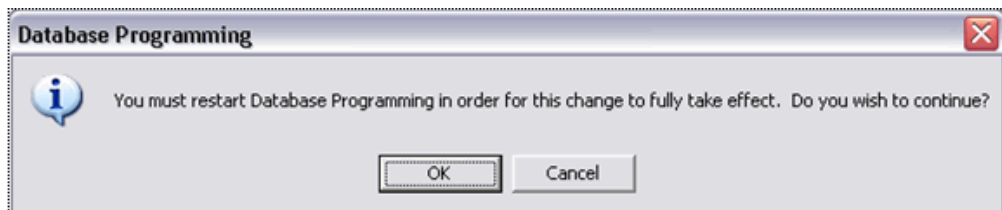


NOTE

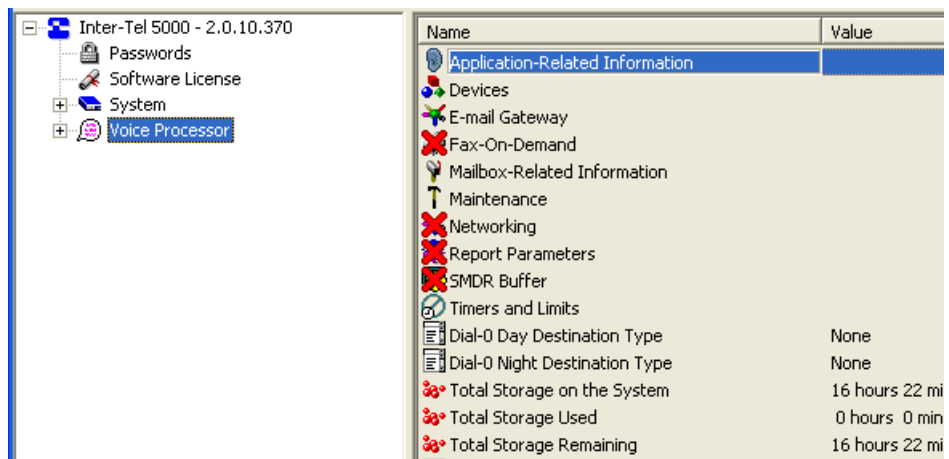
The “Select a Voice Processor Type” dialog appears only if you have, from a remote session, saved the database of a system that does **not** have a voice processor unit physically connected. Once the voice processing unit is connected, the applicable function enabled, and a database saved in a remote session, the Select a Voice Processor Type dialog does **not** display again.



4. Select the option button for the voice processor type you know is connected to the system.
5. Click **OK** to continue programming the selected voice processor. If you select **Cancel**, the Voice Processor Enable field in the System folder toggles to **No**. If you select a voice processor type, or if one already exists in the database, you must restart the system in order for the changes to take effect. The following message window appears.



6. Click **OK**. The voice processor type is updated in DB Programming and the session closes. Clicking **Cancel** toggles the Voice Processor Enable value in the System folder to **No**, cancels any Select a Voice Processor Type selection made, and displays the DB Studio window.
7. Restart a local DB Programming session.
8. Once enabled, the voice processor can be configured and programmed in accordance with customer requirements. The following illustration shows a sample of the Voice Processor folder contents.



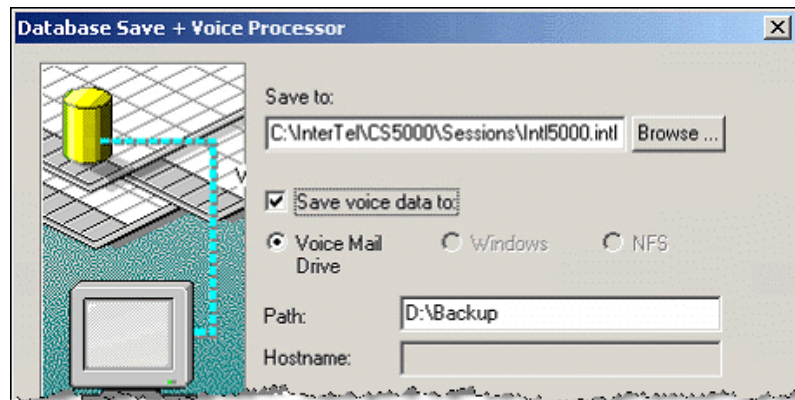
Saving or Restoring an EM Database

The following instructions explain how to save or restore voice processor data on a Mitel CS-5600 system supporting an EM voice processing unit. For detailed instructions about saving and restoring voice data on a Mitel CS-5200 or CS-5400 supporting BVM or EM, refer to *Mitel 5000 DB Programming Help*.

Save/restore options appear in the dialog box on the first page of the Voice Processor Save/Restore wizard.

From the dialog box similar to the one in the following example, you may select only Voice Mail Drive. Because you are not connected to a Mitel CS-5600 with BVM, the Windows and NFS options are dimmed and *not* selectable.

Figure 13-2. Database Save — Voice Processor



In the Path box, enter the drive letter and path to the location of the local EM unit. The Hostname field does not apply when saving or restoring EM data.

If a Mitel CS-5600 with BVM is connected and you are saving to or restoring from a Windows or NFS computer, the Hostname field is enabled. The Hostname field is dimmed and unselectable when you select a USB location.

The Hostname field and the path to it are filtered by DB Programming to ensure that only valid characters are entered. For the Hostname, a valid number or letter must be entered as the starting character. The remaining characters can be any valid character for a hostname.

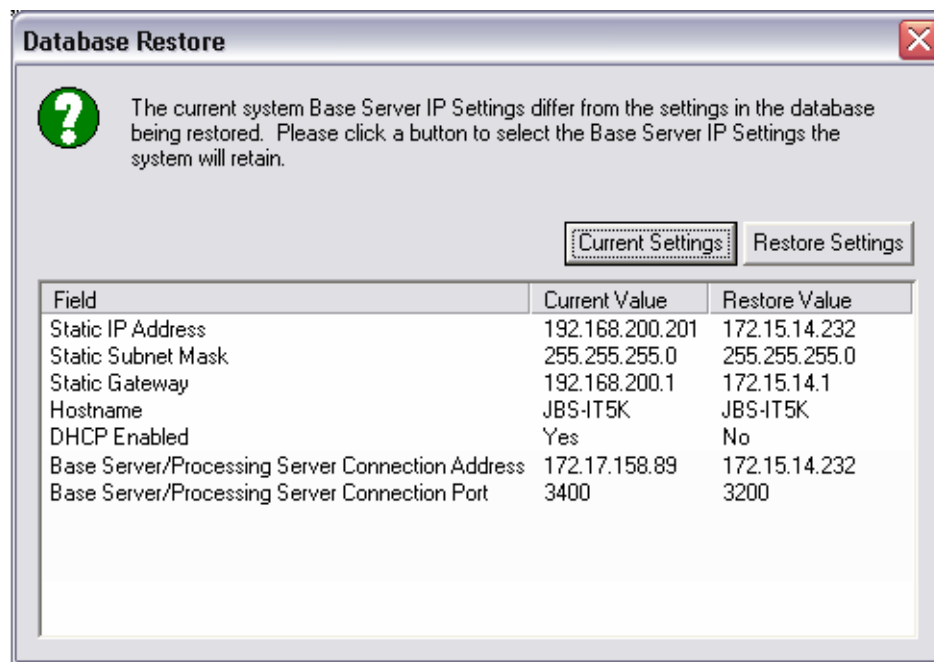
Table 13-2 shows valid characters for both path and Hostname entries.

Table 13-2. Valid Characters for Path and Hostname Entries

Field	Default	Range
Hostname	Blank	0–63 characters Valid characters for first character: 0–9, a–z, A–Z Valid characters for remaining characters: 0–9, a–z, A–Z, '-', and '.'
Path (Character validation applies to all system types.)	For external Voice Mail drive selection, E:\ For Basic Voice Mail drive selection, U:\	1–65 characters All characters are considered valid except the following: * . () , ` ; ? < > \ " & \$ ^ % # In Windows and NFS, the path should start with a single backslash (\). Two backslash characters to start the path should work as well, but three invalidate the path.

Remember the following when restoring a database:

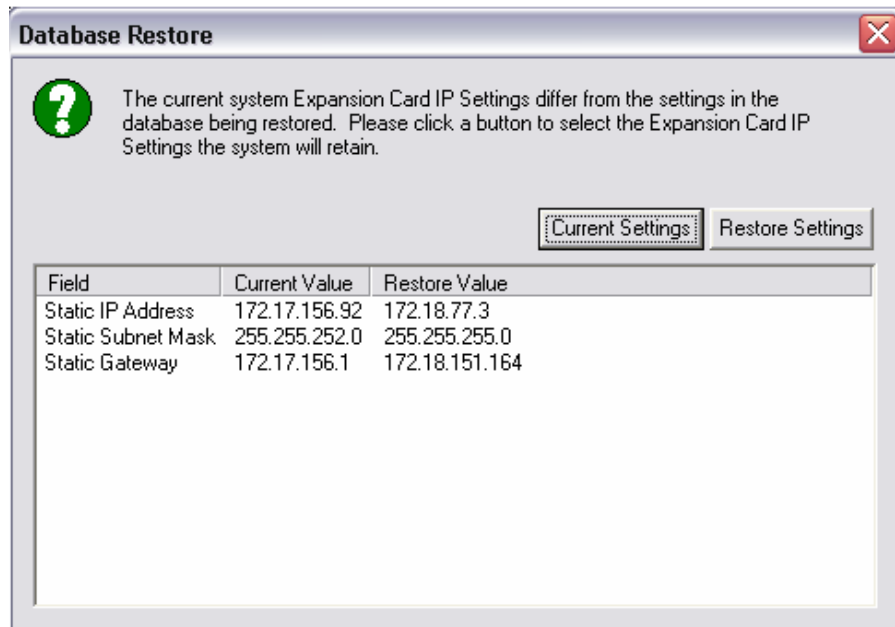
- If you attempt to restore an incompatible system type onto a system, an error message appears. For instance, you cannot restore a Mitel CS-5400 database onto a Mitel CS-5600 system and vice versa.
- Restoring a database with more IP Devices than is supported in the system is *not* allowed. If this illegal operation is attempted during a Database Restore procedure, a warning message appears, and the restore is canceled.
- When restoring a database, if the IP settings on the Base Server or Processing Server differ from the settings in the database to be restored, a dialog similar to the following one below appears. Previously, the SSH Server Enabled and Web Server Enabled fields were available on this dialog so that the current values for these fields could be preserved. The option to preserve the current value for these fields is no longer included in the dialog. Only fields pertaining to the system identity on the network are provided.



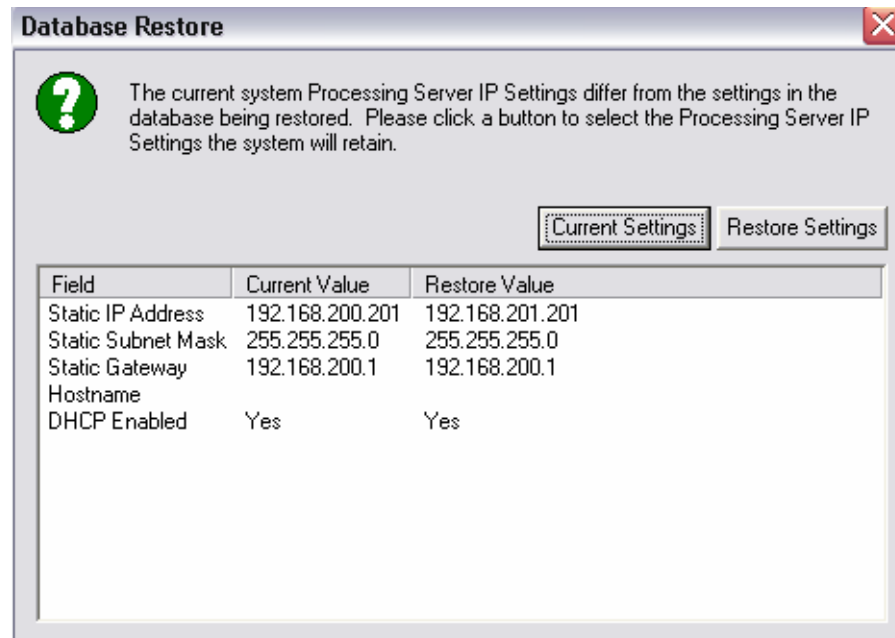
To keep the current IP settings, click **Current Settings**. The settings in the Current Value column are copied over to the database.

To restore the IP settings, click **Restore Settings**. The settings in the Restore Value column are copied over to the database.

- For Mitel CS-5400 or CS-5600 systems, if the current settings for the Processor Expansion Card (PEC-1) differ than the settings in the database to restore, the following dialog box appears, allowing you to specify which settings you want for the Expansion card of your system.



- For Mitel CS-5600 systems, the following dialog box displays if the system PS-1 settings differ from the database to be restored.



To save or restore Mitel CS-5600 voice data to an EM local drive:

1. *In remote mode and connected to a Mitel CS-5600 PS-1 supporting an EM unit.* From the DB Programming menu bar, select Operations – Database Operations – **Database Save...** (or **Database Restore**). A dialog box similar to the previous one appears.
2. Select the **Save voice data to:** or **Restore Voice Processor voice data:** option. The **Voice Mail Drive** option is automatically selected. Because the Windows and NFS options are *not* supported for EM, they are dimmed and cannot be selected.
3. In the **Path** box, type the path. If you are saving to or restoring from a voice mail drive, **E:** appears in the Path: box. If using an external voice processor computer, browse to the applicable destination drive and folder sequence where the voice data was saved to or is restored from. Valid characters appear in [Table 13-2](#). If you do not specify a path, the following message window appears.



4. Click **Start**.

Saving or Restoring a CS-5600 Database on a Remote Windows Computer

To save or restore BVM data from the Mitel CS-5600 PS-1 to a computer running Windows 2000 or later, the destination computer must have a “Guest” account enabled and must be allowed to share folders.

Depending on the Windows operating system and how the computer is configured, the procedure may differ from the one shown in the following example. However, the setup procedure needs to be done only once for the destination computer. The following procedure uses examples from Windows 2000 user interfaces and can be performed only by a user with administrative privileges.

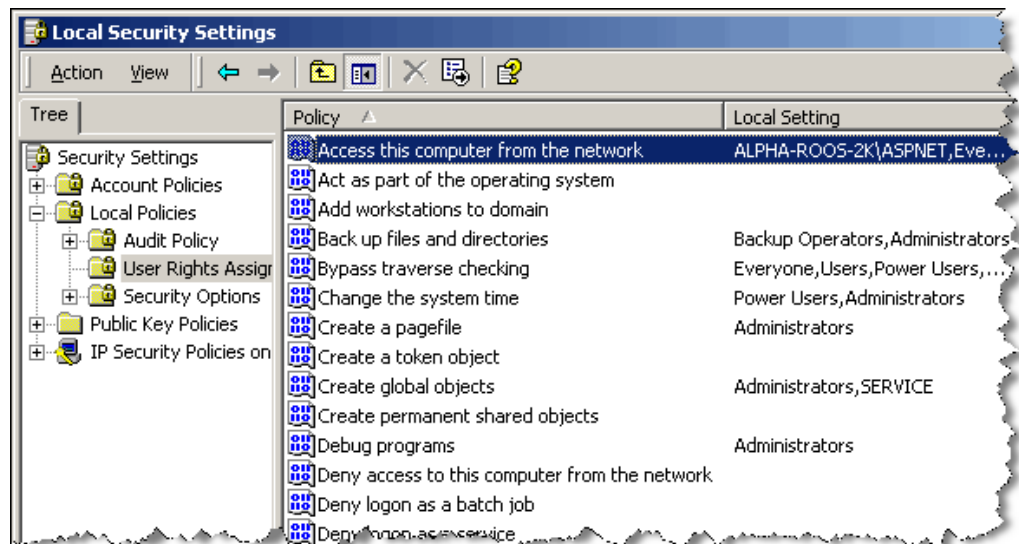
NOTICE

Security Concern. Using a shared folder on a remote computer for saving and restoring BVM data may introduce an undesirable network security risk. Before setting up a shared folder on a remote computer for this purpose, Mitel recommends that you obtain permission from the network administrator.

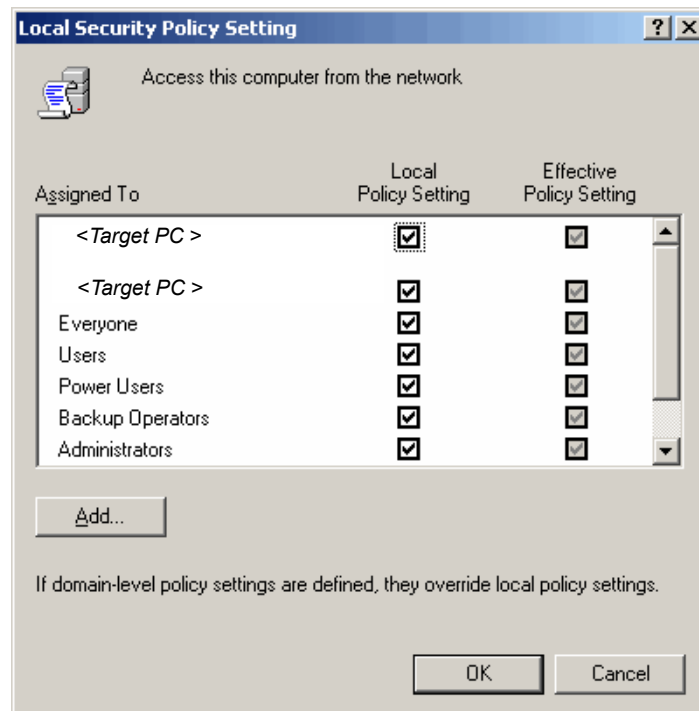
The shared folder should be considered a temporary location for the purposes of the backup only. Once the backup has completed, you should move the data to a secured folder.

To identify active policy settings on Windows 2000 computer:

1. From the Windows task bar, select Start – Control Panel – **Users and Passwords**.
2. In the Tree tab in the left pane of the Local Security Policy Settings window, select Security Settings – Local Policies – **User Rights Assignment**. The Local Security Settings window displays.
3. In the Policy column, double-click the policy titled, “Access this computer from the network.”



The Local Security Policy Setting window appears, showing a summary of active local policy settings.



4. Verify that Guest appears on the list and is checked. If missing, add Guest to the Local Security Policy Setting list.

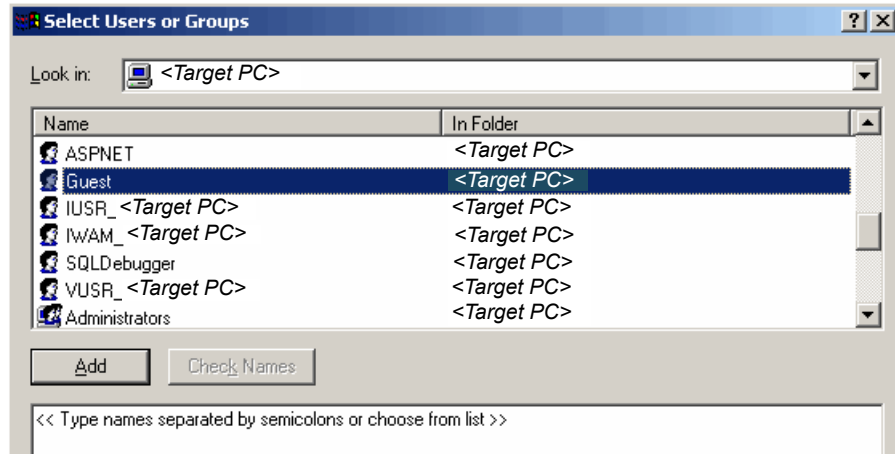
To add Guest to the Local Security Policy list:

1. In the Local Security Policy Setting window (see the preceding procedure), click **Add**. The Select Users or Groups window displays.

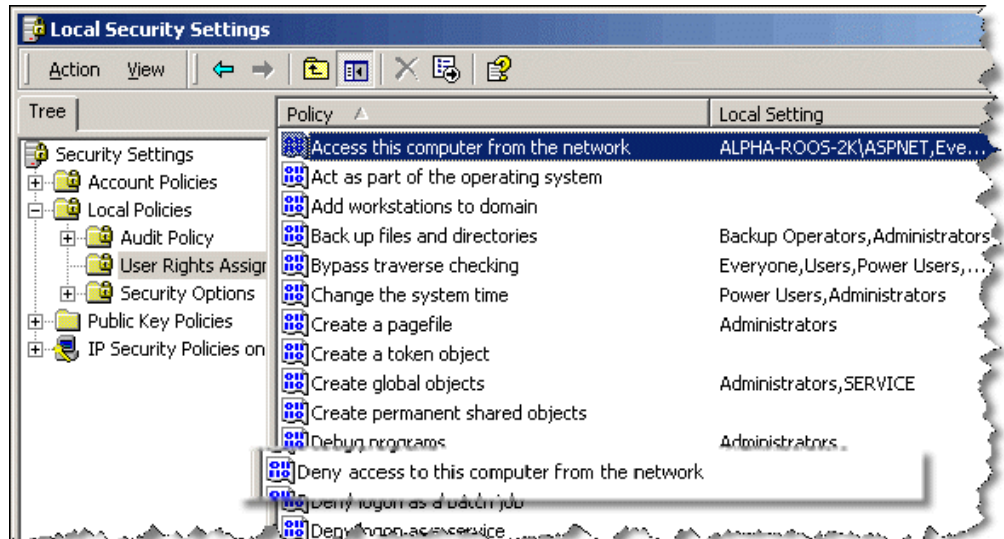
NOTE

Be aware that a user group exists in Windows that is named Guests, with an “s” at the end. Be careful not to confuse this similar name with the singular user name, Guest.

2. In the list box find the account for Guest in the Name column. The value in the In Folder column must be the name of the destination computer. Make sure the name of the destination computer appears in the **Look in** list.



3. Select Guest.
4. Click **Add**, and then click **OK**.
5. Make sure that Guest does not appear on the Local Security Settings policy titled, “Deny access to this computer from the network.”



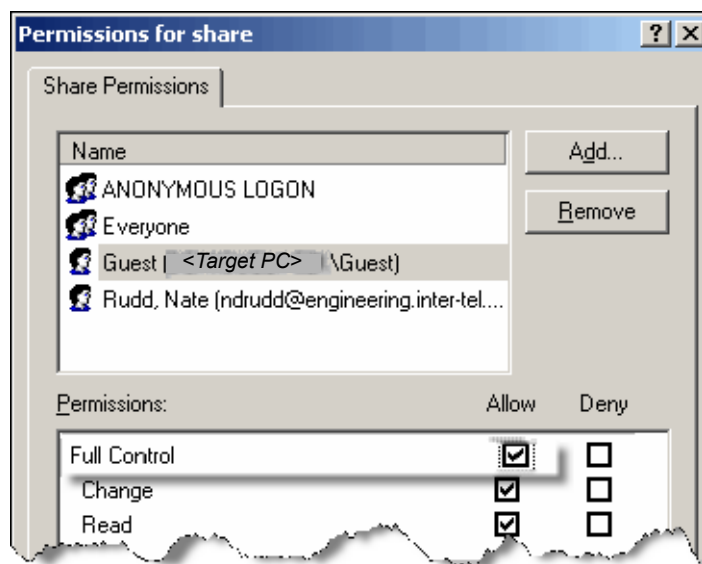
From Windows Explorer, create and name an empty folder into which you will save the system BVM database and from which you will restore the database to the PS-1. In the following example, the name of the folder is “share.”

To add a shared folder on a Windows 2000 computer:

1. From Windows Explorer, right-click the empty folder you created in the preceding step and click **Properties**. The “share Properties” window displays.
2. If Guest does not appear on the user list, under the Sharing tab, click **Permissions**, and then click **Add**. To enable the Guest account to access the shared folder, make sure the Location is set to the name of the destination, or target, computer and type “Guest” in the box.



3. Click **OK**. This action returns you to the “Permissions for share” window.
4. On the Share Permissions tab under Name, select the Guest user with the destination, or target remote computer identified in parentheses. In the Permissions: list box, check Full Control in the Allow column, and then click **OK**.



Repeat the preceding procedure on the Security tab in folder Properties—right-click the folder and then click **Properties**. When the Security tab settings have been made, the destination folder is ready to be saved to or restored from. In the preceding example, the folder would be accessed by Voice Processor save/restore by providing the hostname <Target computer Name> and the path /share.

Saving/Restoring Mitel CS-5600 BVM Data

If a PS-1 is connected to Mitel CS-5600 Base Server and appropriately licensed for BVM, the Windows and NFS options appear in the Database Save – Voice Processor window.

To save/restore a BVM database to a remote computer Running Windows:

1. Set up an empty shared folder on the remote/destination computer. See the preceding procedure, “Saving or Restoring a CS-5600 Database on a Remote Windows Computer” on [page 13-15](#).
2. From the remote/destination computer with the shared folder you created in step 1, start a session of Mitel 5000 Session Manager.
3. From the DB Programming menu bar, select Operations – Voice Processor Operations – **Voice Processor Save** or **Voice Processor Restore**, as appropriate.
4. Select the **Save to** check box.
5. Select the applicable destination, and then click **Next**.
6. In the **Path** box, type the path on the remote/destination computer to the shared folder created in step 1.
7. In the **Hostname** box, either enter the path and name of the remote/destination computer on the network or enter the IP address of the destination computer.
8. Click **Start**.

Save/Restore BVM Data to a Network File Server (NFS)-Supported Computer

This procedure typically applies when using a computer running a Linux operating system, although it would also apply to a Unix-driven computer. Settings may vary because of the many distributions of Linux. You must have root privileges to set up the system for saving or restoring BVM data.

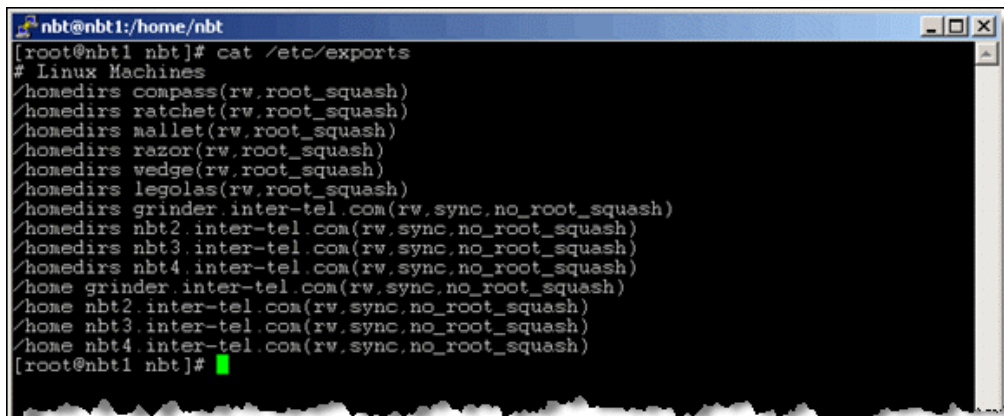
For online assistance to configure NFS, go to <http://nfs.sourceforge.net/nfs-howto/>.

The `nfsd` process must be running and the folder you want to save must be exported to the IP address of the PS-1. In the Red Hat/Fedora flavors of Linux, you can find the export table listed in the file `/etc/exports`.

NOTICE

Security Concern. Using a shared folder on a remote computer for saving and restoring BVM data may introduce an undesirable network security risk. Before setting up a shared folder on a remote computer for this purpose, Mitel recommends that you obtain concurrence from the customer's LAN administrator.

Figure 13-3. NFSD Process



```
nbt@nbt1:/home/nbt
[root@nbt1 nbt]# cat /etc/exports
# Linux Machines
/home dirs compass(rw,root_squash)
/home dirs ratchet(rw,root_squash)
/home dirs mallet(rw,root_squash)
/home dirs razor(rw,root_squash)
/home dirs wedge(rw,root_squash)
/home dirs legolas(rw,root_squash)
/home dirs grinder.inter-tel.com(rw,sync,no_root_squash)
/home dirs nbt2.inter-tel.com(rw,sync,no_root_squash)
/home dirs nbt3.inter-tel.com(rw,sync,no_root_squash)
/home dirs nbt4.inter-tel.com(rw,sync,no_root_squash)
/home grinder.inter-tel.com(rw,sync,no_root_squash)
/home nbt2.inter-tel.com(rw,sync,no_root_squash)
/home nbt3.inter-tel.com(rw,sync,no_root_squash)
/home nbt4.inter-tel.com(rw,sync,no_root_squash)
[root@nbt1 nbt]#
```

To set up an NFS server to Save/Restore voice processing data:

1. Add the absolute path (starting from `/`) to the folder you want to export and then the IP address or name of the PS-1 server you are exporting to. Example: If the IP address of the PS-1 is 155.166.1.1 and you want to share a folder named `/vp_data`, you would add the following line to the exports file:

```
/vp_data 155.166.1.1(rw,sync,no_root_squash)
```

2. After editing this file, execute the command `exportfs` and restart the `nfsd` process.

To save/restore a BVM database to a remote computer Running Linux/Unix NFS:

1. Set up an empty shared folder on the remote/destination computer. See the preceding procedure.
2. From the remote/destination computer with the shared folder you created in [step 1](#), start an `nfsd` process.
3. From the DB Studio menu bar, select Operations – Voice Processor Operations – **Voice Processor Save** or **Voice Processor Restore**, as appropriate.
4. Select the **Save voice data to** check box.
5. Select the NFS option, and then click **Start**.

Database Utilities

Introduction	14-2
MOH Converter Utility	14-3
DB Test and Repair Utility	14-7
Database Test and Repair Menus	14-8
DB Test Toolbar Icons	14-8
DB Test Guidelines	14-9
Database Test Options	14-9
DB Test Common Error Results	14-10
DB Tests	14-10
Associated Mailboxes Test	14-11
Boards Test (Mitel 5000 Modules)	14-12
Cleanup Test	14-13
Devices Test	14-13
Dynamic Enumerations Test	14-15
Enumerations Test	14-16
Extension Conflicts Test	14-16
Hardware Addresses Test	14-17
Miscellaneous Test	14-18
Referential Integrity	14-19
Repairs for the Referential Integrity Test	14-20
Static Records Test	14-20
Upload Utility	14-21
Database Converter Utility	14-23
Conversion Notes	14-23
Mitel 5000 Database Conversions	14-24

Introduction

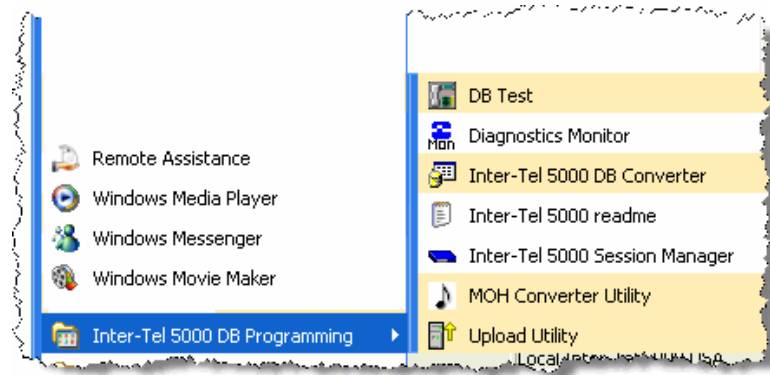
Database utilities help to maintain database integrity when you install, convert, and maintain system databases. The following are the Mitel 5000 system utilities:

- “MOH Converter Utility” on [page 14-3](#)
- “DB Test and Repair Utility” on [page 14-7](#)
- “Database Converter Utility” on [page 14-23](#)
- “Upload Utility” on [page 14-21](#)
- “Diagnostics Monitor” (for more information, refer to the *Mitel 5000 Reference Manual*, part number 580.8007)

To view database utilities:

From the Microsoft® Windows® Start menu, select All Programs – Inter-Tel 5000 DB Programming – *<utility>*, as shown in [Figure 14-1](#).

Figure 14-1. Database Utility Menu



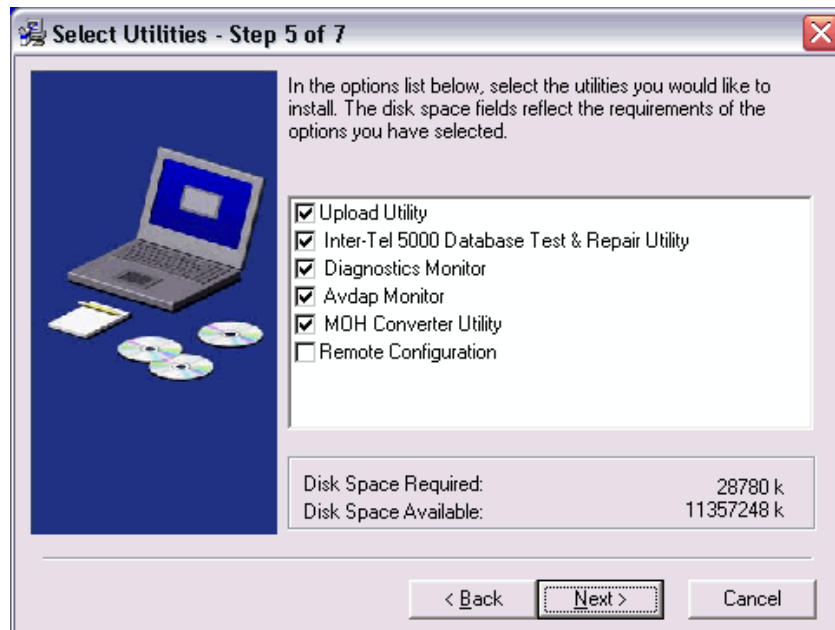
MOH Converter Utility

The MOH Converter Utility converts audio files to the proper format (.n64u) for use for the File-Based MOH feature. You have the option to install the MOH Converter Utility when you install DB Programming. See [Figure 14-2](#).

NOTE

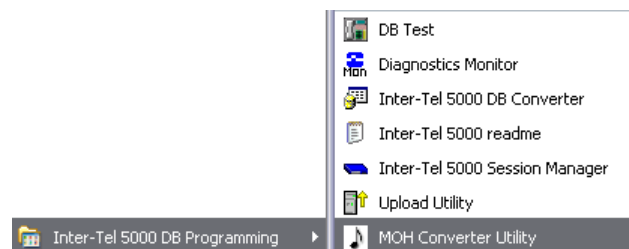
The power of all signal energy other than live voice cannot exceed -9dBm when averaged over a 3 second interval. With our default loss plan, worst case, this means that the File-Based MOH file cannot exceed -12 dBm0 when averaged over a 3 second interval. If any gain on the system (for example, the transmit gain on a loop start trunk) is increased, this maximum level must be decreased by the same amount.

Figure 14-2. DB Programming Installation Wizard



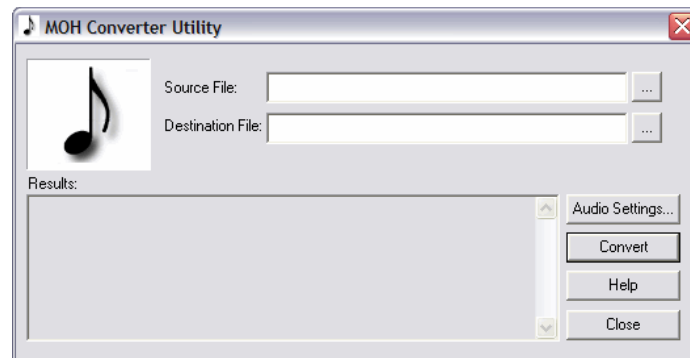
You can access the MOH Converter Utility from the same menu where you access Session Manager. See [Figure 14-3](#).

Figure 14-3. Database Utilities Menu

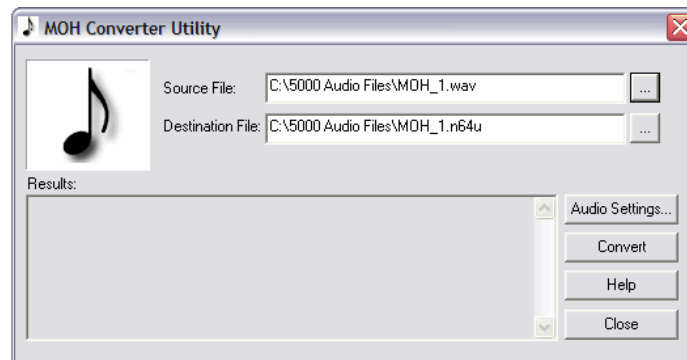


To convert an audio file to G.711 (.n64u) file format:

1. Click the **MOH Converter Utility** option from the DB Programming menu. The MOH Converter Utility dialog box appears.



2. Type the complete path and file name in the **Source File** text box, or click **Browse** to locate the file. The path and file name from the Source File text box is automatically populated in the Destination File text box with the **.n64u** extension.
3. Type a new file name with a **.n64u** extension in the **Destination File** text box, or keep the name that is automatically generated as stated in [step 2](#), in the Destination File text box.

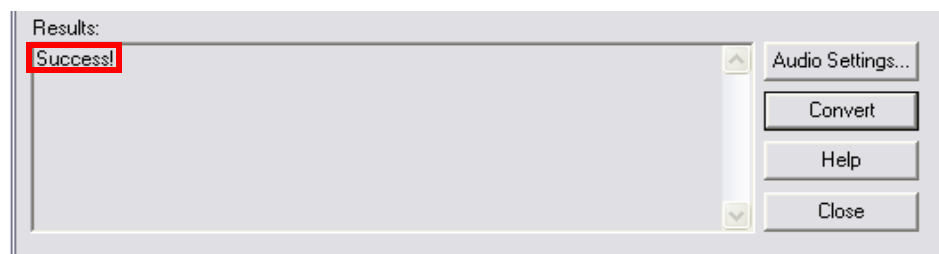


4. Click **Convert**.
5. Check the **Results** dialog box, and then do one of the following:

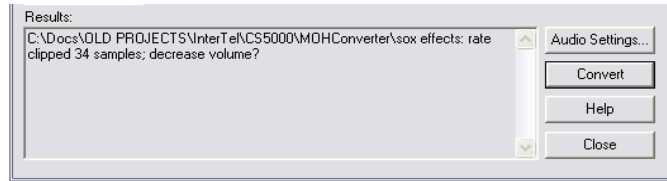
NOTE

The output from the Results dialog box is generated by SoX, not by Mitel. If the information in the Results dialog box is not clear, refer to the SoX text files located in the MOH Converter folder where DB Programming and the MOH Converter is installed, for more information. You may also go to <http://sourceforge.net/projects/sox> for more information.

*If the conversion was successful and there were no issues, the **Results** text box displays Success!. Proceed to [step 6](#).*



If the conversion was successful, but there was an issue, the **Results** text box displays output explaining issues or problems with the audio file. Try changing the volume level of the MOH file (see [step 1](#) below). The following shows an example of a clipped audio file.

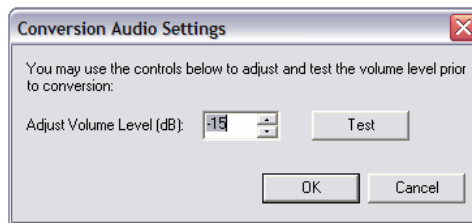


6. Click **Close**. The file is ready to upload to the Mitel 5000 (see “File-Based Music-On-Hold (MOH)” on [page 10-9](#)).

If necessary, you can change the volume level of the MOH file using the Audio Settings dialog box.

To change the volume level for the audio file:

1. Click **Audio Settings** from the MOH Converter Utility dialog box. The Conversion Audio Settings Dialog Box opens.



2. Type a numerical value or scroll to the value in the Adjust Volume Level (dB) list. The options are -30 dB to 0 dB with increments of 3dB while using the list box. The default value is -15 dB (after the conversion process normalizes the file at 0 dB).
3. Click **Test**. The file starts playing and the button text changes to “Stop Test.” A SoX command executes and applies the Adjust Volume Level to the source file.
4. Click **Stop Test** when you are done listening to the test file. The file stops playing and the button text changes to “Test.”

NOTE

If you click OK, the file stops playing and any changed settings are saved. If you click Cancel, the file stops playing and any changes settings are not saved.

5. Click **OK** to save any changed settings, close the Conversion Settings dialog box, and then return to the MOH Converter Utility dialog box.
6. Follow the instructions to convert the file (see [page 14-4](#)).

All of the SoX commands and results are saved to a log file, named MOHConverter.log. This log file is located in the MOH Converter folder where you installed the MOH Converter Utility and Database (DB) Programming. The MOH Converter log file is created and appended for each MOH Converter Utility session. The log file contains the commands and results for both the audio test and the conversion.

To check the log file:

1. Locate the MOHConverter.log file (where the MOH Converter Utility and DB Programming is installed).
2. Open the log file in an application such as Notepad.
3. Review the commands and results that appear in the log. For example, this is an excerpt for a specific MOH Converter Utility session:

```
***** MOH Converter Utility Started [09-09-2008 12:22] *****
---Begin Audio Test---
Test Command to Adjust Volume: "C:\5K_DB_UTILITIES\MOH_Converter
Utility\sox" "C:\piano.wav" -r 8000 -c 1 "C:\5K_DB_UTILITIES\MOH_Converter
Utility\MitelMOHConverterTest.wav" norm -15
Test Command to Play Test File: "C:\5K_DB_UTILITIES\MOH_Converter
Utility\play" "C:\5K_DB_UTILITIES\MOH_Converter
Utility\MitelMOHConverterTest.wav"

Test Results:
C:\5K_DB_UTILITIES\MOH_Converter Utility\MitelMOHConverterTest.wav:
    Encoding: Signed PCM
    Channels: 1 @ 16-bit
    Samplerate: 8000Hz
    Replaygain: off
    Duration: 03:23.21

0.00% 00:00.00 [03:23.21] of 03:23.21 out:0 [ | ] clip:0
1.01% 00:02.05 [03:21.16] of 03:23.21 out:16.4k [ ==|== ] clip:0
1.51% 00:03.07 [03:20.14] of 03:23.21 out:24.6k [ =|= ] clip:0
2.02% 00:04.10 [03:19.11] of 03:23.21 out:32.8k [ -==|== ] clip:0

---Test Ended---

---Begin Audio Test---
Test Command to Adjust Volume: "C:\5K_DB_UTILITIES\MOH_Converter
Utility\sox" "C:\piano.wav" -r 8000 -c 1 "C:\5K_DB_UTILITIES\MOH_Converter
Utility\MitelMOHConverterTest.wav" norm -9
Test Command to Play Test File: "C:\5K_DB_UTILITIES\MOH_Converter
Utility\play" "C:\5K_DB_UTILITIES\MOH_Converter
Utility\MitelMOHConverterTest.wav"

Test Results:
C:\5K_DB_UTILITIES\MOH_Converter Utility\MitelMOHConverterTest.wav:
    Encoding: Signed PCM
    Channels: 1 @ 16-bit
    Samplerate: 8000Hz
    Replaygain: off
    Duration: 03:23.21

0.00% 00:00.00 [03:23.21] of 03:23.21 out:0 [ | ] clip:0
1.01% 00:02.05 [03:21.16] of 03:23.21 out:16.4k [ ----|---- ] clip:0
1.51% 00:03.07 [03:20.14] of 03:23.21 out:24.6k [ -==|== ] clip:0
2.02% 00:04.10 [03:19.11] of 03:23.21 out:32.8k [ ----|---- ] clip:0
2.52% 00:05.12 [03:18.09] of 03:23.21 out:41.0k [ -==|== ] clip:0

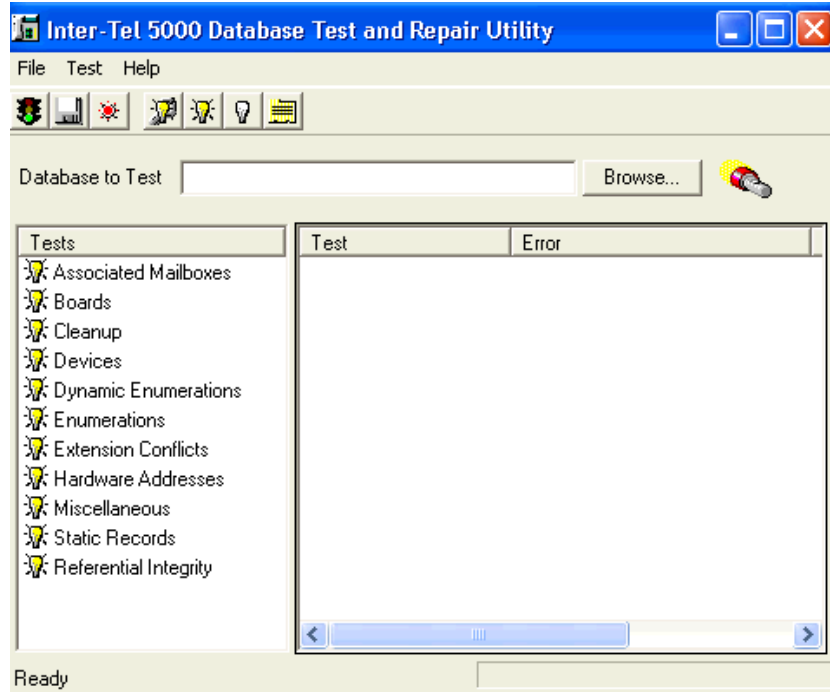
---Test Ended---

Converting C:\piano.wav to C:\piano.n64u
Conversion Command: "C:\5K_DB_UTILITIES\MOH_Converter Utility\sox"
"C:\piano.wav" -t raw -r 8000 -U -c 1 "C:\piano.n64u" norm -9
Result: Success!
***** utility closed *****
```

DB Test and Repair Utility

The Database Test and Repair utility (DB Test) tests and can usually repair corrupted databases. The utility has several individual tests, and you can use each test to either test only or test and repair. [Figure 14-4](#) shows the DB Test dialog box.

Figure 14-4. *DB Test Dialog Box*



Database Test and Repair Menus

The Database Test and Repair Utility window provides File, Test, and Help menus, which are detailed in the following tables.

The File menu contains the options shown in [Table 5-4](#).

Table 14-1. Database Test and Repair Utility File Menu Options

Menu Option	Action
Start Testing	Runs the enabled tests. Repairs errors if repairs are enabled.
Save Results	Saves the errors/warnings to a file.
Options	Enables user to program utility options.
Exit	Closes the program.

The Test menu contains the options shown in [Table 5-5](#). You can also view these options by right-clicking in the objects in the Tests list in the left pane of the window.








Table 14-2. Database Test and Repair Utility Test Menu Options

Menu Option	Action
Enable/Repair	Enables the selected test for test and repair.
Enable	Enables the selected test for testing only.
Disable	Disables the selected test.
Enable/Repair All	Enables all tests for test and repair.
Enable All	Enables all tests for testing only.
Disable All	Disables all tests.
Properties	Displays the test properties — a test description.

DB Test Toolbar Icons

The toolbar provides icon shortcuts to the drop-down menu options summarized in [Table 5-6](#).

Table 14-3. Database Test and Repair Toolbar Icon Shortcuts

Icon	Menu Option	Action
 Stoplight	Start Testing	Runs the enabled tests. Repairs errors if repairs are enabled.
 Floppy disk	Save Results	Saves the errors/warnings to a file.
 Red dot	Options	Enables user to program utility options.
 Lit light bulb with wrench	Enable/Repair	Enables the selected test for test and repair.
 Lit light bulb	Enable	Enables the selected test for testing only.
 Unlit light bulb	Disable	Disables the selected test
 Paper	Properties	Displays a description of the test.

DB Test Guidelines

Remember the following when running a DB Test:

- The DB Test utility can find and repair most, but not all, database corruptions. Frequently found corruptions are described in “Associated Mailboxes Test” on [page 14-11](#). If the Repair function is enabled and the repair status is “Not Repaired,” the program was unable to fix the problem. In this case, contact Mitel Technical Support for assistance.
- A repair may cause another corruption. If this happens and the required test has not been run, DB Test notifies you that you must run another test to repair the new corruption. If DB Test detects an error but cannot repair it, contact Mitel Technical Support for assistance.
- When DB Test deletes records to repair a database, further corruption can happen. However, you can correct the additional corruption by running the appropriate test. For example, if a test deletes “device 1000” because of corruption, all references to device 1000 would still exist in the database. The Referential Integrity test can clean up these references. Therefore, once the repairs are made, the utility may warn you that other tests/repairs need to be run in order for total clean up to occur. If the proper test automatically runs after the deletion occurs, then no warning is necessary because the test has already run. However, you may notice additional error messages as the new corruption is repaired.
- DB Test ensures that no more resources are reserved than the system can support. If resources are reserved beyond the maximum number a system can support, DB Test reports the error and corrects it by resetting the excess reserved fields to 0.
- DB Test recognizes T1M-2 and T1M as valid modules for Mitel 5000 system (expansion bays 1–3). DB Test also tests the port types of the T1M-2 and T1M modules and flags any configuration type other than T1, T1/PRI, E1/PRI, or None. When you click DB Test option on the DB Programming menu, the Database Test and Repair Utility window appears.

Database Test Options

The following are DB Test options:

- **Log File:** Enter the path where the log file is stored.
- **Browse:** Browse to locate the log file.
- **Repair System Tables:** Select this check box to repair system tables.
- **Compact Database:** Select this check box if compaction should occur after testing or repairing the database. Because this reduces the size of the resulting database, Mitel recommends that you do this to optimize disk space.
- **Display Warnings:** Select this check this box to display warnings and errors in the output window.
- **Max. Errors:** This is the maximum number of errors you allow the test to find before stopping the test. The default is 100000.

To view DB Test options:

From the **File** menu, select **Options**.

DB Test Common Error Results

Table 14-4 shows common errors found when using DB Test.

Table 14-4. Database Test and Repair Utility Common Errors

Test	Error
Hardware Address	Hardware Address Ext ____ refers to an unrecognized module [0.0.0 Type 262] A device has a hardware address of 0.0.0. DB Test removes the device and cleanup references to it.
Referential Integrity	[Applications] / [transfer_recall_destination_device_id] contains a reference to a device of the wrong type [DevID:1, Type 0] [Endpoints] / [transfer_recall_destination_device_id] contains a reference to a device of the wrong type [DevID:1, Type 0] The Transfer Recall Destination field is not pointing to a valid device. DB Test changes this field to point to the current device.
Boards (Modules)	The module in bay ____ has an incorrect number of records in [DSPs]. DB Test creates the necessary records.
Static Records	<BoardsInformation> contains an invalid number of records [0 instead of 16] DB Test creates the necessary records.
Referential Integrity	[Report...] / [report_id] contains an invalid reference to [Reports] / [report_id][0] DB Test removes these unneeded records.
Referential Integrity	[PrimaryRateBoards] / [board_id] contains a reference to a module of the wrong type [BoardID:<module ID>, Type:253] DB Test removes this unnecessary record.
Static Records	[MessagePrintFreezeOnStrings] contains an invalid number of records [0 instead of 6] DB Test creates the necessary records.
Devices	Ext ____ has no records in [CallRoutingAnnouncements] DB Test creates the necessary records.
Boards (Modules)	The module in bay ____ has no records in T1CallType DB Test creates the necessary records.
Dynamic Enumerations	[Keysets] / [attached_device_baud_rate_id] contains an invalid enumeration value [4]

DB Tests

DB Tests include the following:

- “Associated Mailboxes Test” on [page 14-11](#)
- “Boards Test (Mitel 5000 Modules)” on [page 14-12](#)
- “Cleanup Test” on [page 14-13](#)
- “Devices Test” on [page 14-13](#)
- “Dynamic Enumerations Test” on [page 14-15](#)
- “Enumerations Test” on [page 14-16](#)
- “Extension Conflicts Test” on [page 14-16](#)
- “Hardware Addresses Test” on [page 14-17](#)
- “Miscellaneous Test” on [page 14-18](#)
- “Referential Integrity” on [page 14-19](#)
- “Static Records Test” on [page 14-20](#)

Associated Mailboxes Test

Each mailbox in the database has a flag to indicate if it is associated with another device. This test searches for two cases. The first case is when the mailbox-associated flag is enabled, but there is no valid corresponding device with the same extension to be associated. The second case is when the mailbox-associated flag is disabled, but there is a valid corresponding device with the same extension to be associated. For a summary of possible error messages, see [Table 14-5](#).

Table 14-5. DB Test and Repair Error Messages for Associated Mailboxes

Error Message	Indication
Mailbox x<extension> is not associated, but has multiple corresponding devices	In this case, mailbox x1000 has an associated flag disabled. It has more than one valid corresponding device with the same extension and is repaired. It is not valid for a mailbox to be associated to more than one device. The Repair Status is Not Repaired. To repair this case, run the Extension Conflicts test. This test repairs the multiple devices sharing one extension. Then, rerun the Associated Mailboxes test.
Mailbox x<extension> is not associated, but has a corresponding device	In this case, mailbox x1000 has an associated flag disabled. However, it has a valid corresponding device with the same extension. This corruption is repaired by enabling the associated flag. The Repair Status will be Set Associated Flag to true.
Mailbox x<extension> is associated, but has no corresponding device	In this case, mailbox x1000 has an associated flag enabled. However, it does not have a valid corresponding device with the same extension. This corruption is repaired by disabling the associated flag. The Repair Status will be Set Associated Flag to false .
You have exceeded the maximum number of mailbox licenses	The database is currently programmed for the maximum number of licenses allowed. You cannot add any more mailboxes. For additional licenses, contact your Mitel service provider.

Boards Test (Mitel 5000 Modules)

This test confirms that each board, or module, has the proper entries in all corresponding tables. For a summary of possible error messages, see [Table 14-6](#).

NOTE

The term “board” refers to Mitel 5000 expansion modules. The term “slot” refers to one of the bays in the Mitel 5000 Base Server.

Table 14-6. *DB Test and Repair Error Messages for Modules*

Error Message	Indication
The board in slot <slot number> has no records in <table name>	In this case, the module/board is required to have records in its table. However, none exist. This corruption is repaired by adding default records to the table. The Repair Status either indicates Record Added if one record was added or Records Added if more than one record was added.
The board in slot <slot number> has an incorrect number of records in <table name>	In this case, the module/board does not have the proper number of records in its table. This corruption is repaired by adding default records to the table. The Repair Status indicates Records Added.
The board in slot <slot number> has an incorrect record sequence in <table name>	In this case, the module/board has the proper number of records in the table. However, the sequence numbers are incorrect. For example, the records should be numbered 1–10. However, they are numbered 0–9. This corruption is repaired by deleting the record that has an out-of-bounds sequence number and adding a default record for the each missing sequence number. In the given example, record 0 would be deleted and record 10 would be added. The Repair Status indicates Added/Deleted Records, Deleted Records, or Records Added depending on the action that was taken.

Cleanup Test

The Cleanup test detects and removes objects that are not in use, which includes the following:

- Hunt groups. See “Hunt Groups” on [page 8-32](#).
- Facility groups. See “Programming ARS Facility Groups” on [page 5-13](#)
- Route groups. See “Programming ARS Route Groups” on [page 5-16](#).
- CO trunk groups. See “CO Trunk Groups” on [page 8-7](#).
- Page zones. See “Page Zones” on [page 10-15](#).
- Standard account codes. See “Account Codes” on [page 7-69](#).
- Forced account codes. See “Programming Forced Account Code Options” on [page 7-70](#).
- System Speed Dial. See “System Speed Dial” on [page 7-75](#).

Devices Test

This test confirms that each device has the proper entries in all corresponding tables. For a summary of possible error messages, see [Table 14-7](#).

Table 14-7. DB Test and Repair Error Messages for Devices

Error Message	Indication
Invalid table <i><table name></i>	This message is only a warning. It indicates that the utility was looking for a table, but could not find it in the database. This discrepancy can happen if a new table is added in a later version of a major release. If the test is being run on the earlier version, this warning appears. For example, if Table A was added in v1.1, running this test on databases prior to v1.1 produces a warning that Table A cannot be found.
Invalid column <i><table name>:<column name></i>	This message is only a warning. It indicates that the utility was looking for a column, but could not find it in the database. This discrepancy can happen if a new column is added in a later version of a major release. If the test is being run on the earlier version, this warning appears. For example, if Column A was added in v1.1, running this test on databases prior to v1.1 produces a warning that Column A cannot be found.
Ext <i><extension number></i> has no records in <i><table name></i>	This corruption indicates that the given device has no records in the table indicated. This corruption can be repaired in more than one way. If the table that is missing the records is critical, then the device is non-recoverable and is deleted completely. In this case, the Repair Status indicates Deleted Device. If the table that is missing the records is not critical, the corruption is repaired by adding default records to the table. The Repair Status either indicates Record Added if one record was added or Records Added if more than record was added.

Table 14-7. *DB Test and Repair Error Messages for Devices (Continued)*

Error Message	Indication
Ext %s has an incorrect number of records in %s	In this case, the device does not have the proper number of records in a table. This corruption is repaired by adding default records to the table. The Repair Status indicates Records Added.
Ext %s has an incorrect record sequence in %s	In this case, the device has the proper number of records in the table. However, the sequence numbers are incorrect. For example, the records should be numbered 1–10. However, they are numbered 0–9. This corruption is repaired by deleting the record that has an out-of-bounds sequence number and adding a default record for each missing sequence number. In the given example, record 0 is deleted and record 10 is added. The Repair Status indicates Added/Deleted Records, Deleted Records, or Records Added depending on the action that was taken.

Dynamic Enumerations Test

This test confirms that all dynamic enumeration fields contain valid values. A dynamic enumeration field is an enumeration field that depends on another field. If the master field is set to A, the field can contain one set of values. If the master field is set to B, the field can contain a different set of values. For a summary of possible error messages, see [Table 14-8](#).

Table 14-8. DB Test and Repair Error Messages for Dynamic Enumerations

Error Message	Indication
Invalid table <i><table name></i>	This is only a warning. It indicates that it was looking for a table, but could not find it in the database. This can happen if a new table is added in a later version of a major release. If the test is being run on the older version, this warning will appear. For example, if Table A was added in v1.1, running this test on databases previous to v1.1 will produce a warning that Table A could not be found.
Invalid column <i><table name>:<column name></i>	This is only a warning. It indicates that it was looking for a column, but could not find it in the database. This can happen if a new column is added in a later version of a major release. If the test is being run on the older version, this warning will appear. For example, if Column A was added in v1.1, running this test on databases previous to v1.1 will produce a warning that Column A could not be found.
<i><table name>/<column name></i> contains an invalid enumeration value [<i><invalid value></i>]	The table has an incorrect value in the indicated column. This corruption is repaired by changing the field to a correct value. The Repair Status will be Value Set to <i><value></i> where <i><value></i> is the new contents for the field.

Enumerations Test

Each enumeration field has a set of values that are valid. An error is detected if the field has a value that is out of this range. For a summary of possible error messages, see [Table 14-9](#).

Table 14-9. DB Test and Repair Error Messages for Enumerations

Error Message	Indication
Invalid table <table name>	This is only a warning. It indicates that it was looking for a table named, but could not find it in the database. This can happen if a new table is added in a later version of a major release. If the test is being run on the older version, this warning will appear. For example, if Table A was added in v1.1, running this test on databases previous to v1.1 will produce a warning that Table A could not be found.
Invalid column <table name>:<column name>	This is only a warning. It indicates that it was looking for a column named, but could not find it in the database. This can happen if a new column is added in a later version of a major release. If the test is being run on the older version, this warning will appear. For example, if Column A was added in v1.1, running this test on databases previous to v1.1 will produce a warning that Column A could not be found.
<table name>/<column name> contains an invalid enumeration value [<invalid value>]	The table has an incorrect value in the indicated column. This corruption is repaired by changing the field to a correct value. The Repair Status will be Value Set to <value> where <value> is the new contents for the field.

Extension Conflicts Test

This test checks for extension conflicts. For a summary of possible error messages, see [Table 14-10](#).

Table 14-10. DB Test and Repair Error Messages for Extension Conflicts

Error Message	Indication
Found blank extension, device type <device type>	In this case, a device was found with a blank extension. The extension is changed to P#XXX where XXX can be from 000 to 999. The Repair Status will be Set to Extension <new extension>.
Found conflict with extension <extension number>, device types <device type 1>, <device type 2>	Two devices have the same extension number, and the two device types are not compatible. This corruption is repaired by changing the extension number of the second device <device type 2> to P#XXX where XXX can be from 000 to 999. The Repair Status will be Set to Extension <new extension>. Only 1000 extension conflicts can be resolved at a time because there are only 1000 possible extensions in the P#XXX framework. Therefore, starting at the 1001 extension, the Repair Status shows Not Repaired. Once an extension is set to P#XXX, you can go into DB Programming and change the extension to a valid number.

Hardware Addresses Test

This test confirms that each hardware address is valid. For a summary of possible error messages, see [Table 14-11](#).

Table 14-11. DB Test and Repair Error Messages for Hardware Addresses

Error Message	Indication
Ext <extension number> refers to an invalid bay[<bay number>.<port>.<circuit> Type:<module type>]	In this case, the device is on a module that is in a bay that it should not be. Repairs are made by deleting the device. The Repair Status will be Deleted Device.
Ext <extension number> refers to an invalid port [<slot number>.<port>.<circuit> Type:<module type>]	In this case, the device has an invalid port number. Repairs are made by deleting the device. The Repair Status will be Deleted Device.
Ext <extension number> refers to an invalid circuit [<slot number>.<port>.<circuit> Type:<module type>]	In this case, the device has an invalid circuit number. Repairs are made by deleting the device. The Repair Status will be Deleted Device.
Ext <extension number> refers to an unrecognized module [<slot number>.<port>.<circuit> Type:<module type>]	In this case, the device is on a module with an invalid type. Repairs are made by deleting the device. The Repair Status will be Deleted Device.
Ext <extension number> refers to an invalid module type [<slot number>.<port>.<circuit> Type:<module type>]	In this case, the device is on a module that it should not be. For example, a loop start device cannot be on a single line module. Repairs are made by deleting the device. The Repair Status will be Deleted Device.

Miscellaneous Test

This test checks for miscellaneous business rules. For a summary of possible error messages, see [Table 14-12](#).

Table 14-12. *DB Test and Repair Error Messages for Miscellaneous*

Error Message	Indication
Endpoint <extension> is its own attendant	This error message indicates that the endpoint is programmed to serve as its own attendant. The DB Test will set the attendant to none and the Repair Status will show [Set to None Device]. This test ensures that all static records are present in the database.
Invalid Expansion Card Static Subnet Mask Setting	<p>The Miscellaneous Test recognizes when a database has static subnet masks or gateways programmed that are not the same for the Processor Module, Expansion Card, and Processing Server (checks fields accordingly based on system type).</p> <p>This is reported as an error, and the repair method is to copy the subnet mask and gateway from the Processor Module to the Expansion Card (for a 5400 or 5600 system) and the Processing Server (for a 5600 system). This allows them to be on the same subnet/gateway.</p> <p>This test is also performed for the DHCP flag, SSH port and enable, Web Server listening port and enable, and listening port fields of the Processing Server. If they do not match the Processor Module's fields and the system is a 5600, DB Test reports the error and repairs it, if Repair is enabled. The repair is to copy the value for each field from the Processor Module to the Processing Server.</p> <p>The Default keymap is also validated in the Static Records test. If any entries of the Default keymap are missing, DB Test reports the error and repairs it, if Repair is enabled.</p>
Invalid Expansion Card Static Gateway Settings	
Invalid Processing Server Static Subnet Mark Setting	
Invalid Processing Server Static Gateway Setting	
Invalid Processing Server Web Server Port Setting	

Referential Integrity

This test confirms that the relationships between tables in the database are valid. For a summary of possible error messages, see [Table 14-13](#).

Table 14-13. DB Test and Repair Error Messages for Referential Integrity

Error Message	Indication
Invalid table <i><table name></i> or Invalid source table <i><table name></i>	This is only a warning. It indicates that it was looking for a table, but could not find it in the database. This can happen if a new table is added in a later version of a major release. If the test is being run on the older version, this warning will appear. For example, if Table A was added in version 1.1, running this test on databases previous to version 1.1 will produce a warning that Table A could not be found.
Invalid column <i><table name>:<column name></i> or Invalid source column <i><table name>:<column name></i>	This is only a warning. It indicates that it was looking for a column, but could not find it in the database. This can happen if a new column is added in a later version of a major release. If the test is being run on the older version, this warning will appear. For example, if Column A was added in version 1.1, running this test on databases previous to version 1.1 will produce a warning that Column A could not be found.
<i><table name>/<column_name></i> contains an invalid reference to <i><source table name>/<source column name></i> [<i><invalid reference></i>]	The indicated value contains an invalid reference to another table or column.
<i><table name>/<column name></i> contains a reference to a device of the wrong type [DevID: <i><device ID></i> , Type: <i><device type></i>]	The indicated value contains a reference to a device that is not the proper type. For example, if the System Administrator Mailbox field contains a reference to an endpoint it is invalid, because the System Administrator Mailbox can only be a mailbox.
<i><table name>/<column name></i> contains a reference to a module of the wrong type [BoardID: <i><module ID></i> , Type: <i><module type></i>]	The indicated value contains a reference to a module that is not the proper type. For example, LSM-2 records are connected to a module record for a SLM-4 module.

Repairs for the Referential Integrity Test

Repairs for Referential Integrity are different depending on the field that has the corruption. The possibilities are as follows:

- If a lack of a valid reference makes the record no longer useful, a repair is made by deleting the record. The Repair Status will be Record Deleted.
- If a reference is referring back to a device or object that is not valid or not present, several repairs can be made. They are as follows:
 - **Set to Extension <extension number> [<device ID>]**: In this case, the repair was made by replacing the bad reference with a device of the same extension, but of the proper type.
 - **Set to None Device**: In this case, the repair was made by replacing the bad reference with None.
 - **Set to Current Device**: In this case, the repair was made by replacing the bad reference with the current device.
 - **Set to First Available**: In this case, the repair was made by replacing the bad reference with the first device/object found.
- It is possible for the repair to be complicated, and therefore not attempted. In this case, the Repair Status will be Not Repaired.

Static Records Test

This test ensures that all static records are present in the database. For a summary of possible error messages, see [Table 14-14](#).

Table 14-14. DB Test and Repair Error Messages for Static Records

Error Message	Indication
<Table name> contains an invalid number of records [<current number> instead of <desired number>]	The table should have the “desired number” of records. However, it has the “current number” records. This corruption is repaired by deleting unneeded records and adding records that are missing. The Repair Status will be: Added/Deleted Records, Added Records, or Deleted Records.
<Table name> is missing <specific record>	This corruption occurs when a specific record is missing. Only some of these corruptions will be repaired. The Repair Status can be: Rebuilt Table, Created None Device, Created Voice Processing Local Node, Created Unused Trunk Group, or Not Repaired.

Upload Utility

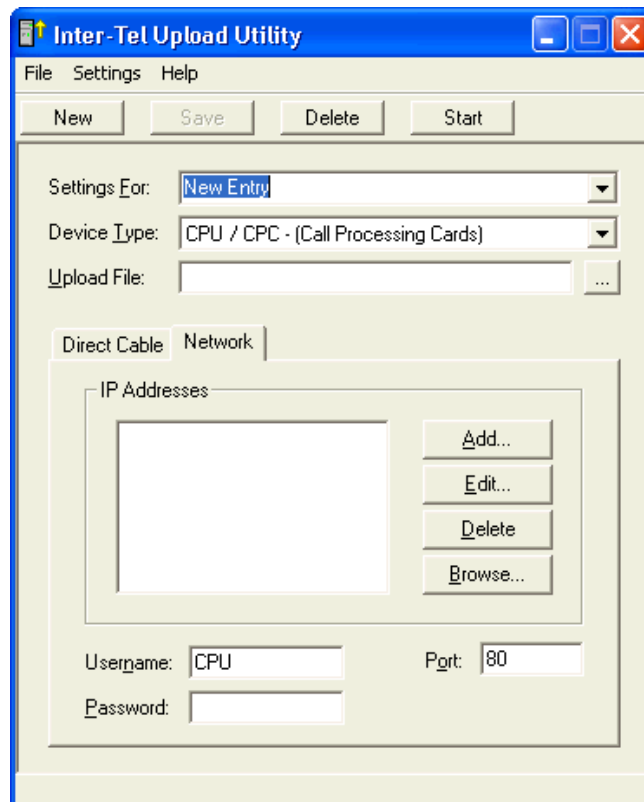
The Upload utility applies to Inter-Tel Model 8660 and IP PhonePlus endpoints only. For more information, refer to the “Installation” chapter in the Mitel 5000 Installation and Maintenance Manual, part number 580.8000.

You can use the Upload Utility, which supports network connections, to load different versions of software on IP devices. Mitel recommends using the Upload Utility for uploading firmware to the Inter-Tel Model 8660 and Inter-Tel IP PhonePlus endpoints.

You can upgrade multiple IP devices at the same time. You can also save the settings so that you do not have to configure information for every upload. For example, you can create an entry for all hard IP endpoints, such as the Model 8660, in your network.

To upload firmware to IP devices using a network connection:

1. Select Start – Programs – Inter-Tel DB Programming – **Upload Utility**.



2. From the **File** menu, select **Start** or **New** to create an entry.
3. Complete the following fields:
 - **Settings For:** Type a description, up to 40 characters, to identify the connection type. For example, if you are creating a setting for the IP devices on node 2, you could type **Node 2 IP Devices**.
 - **Device Type:** Select **IPP+/IP SLA - (IP Phones)** for IP devices. The Username field is automatically populated (IPT or IPC, respectively) in the Network tab.
4. Select the Network tab.

5. Click **Browse**. The Upload Utility queries the network for a list of Mitel Device IP addresses on the network. This information is then displayed in the Browse IP Address screen and includes the following:
 - **IP Address**: The IP address of the module or device found on the network.
 - **Hostname**: The hostname assigned to the module or device.
 - **Description**: The description used to identify the module or device in DB Programming. For IP endpoints, this is the endpoint description.
6. Select the IP address of the desired device, and then click **Add** (you can use the SHIFT and CTRL key to select more than one item). To add all IP addresses or hostnames, click **Add** without selecting any items. The selected IP addresses are added to the list box in the main screen.
7. Click **Save** to save the settings. At the prompt, click **Yes** to confirm the save.
8. In the **Upload File** box, type the filename to upload or click the ellipsis (...) button to select a file from the dialog box. The source file names differ based on the device. In general, the file names for IP devices are as follows:
 - **ipp8660.bin** for the Model 8660 endpoint
 - **ip_sla.hex** for the IP SLA

The IP resource files include the version.

9. Enter the password. The case-sensitive default is **iptpassw**.
10. If necessary, enter the port number that corresponds to the Web listening port number assigned to the IP device. The Port value must match the Web listening port number; otherwise, the upload will fail. The default port value is 80.
11. Click **Start** or select **Start** from the File menu. If you entered the correct IP addresses, username, and password, the upload process begins, and an Upload Progress dialog box appears.

The IP address or hostname of the affected devices and the status of the upload are indicated. The following options are available:

- **Close**: Closes the dialog box.
 - **Retry**: Allows you to attempt the upload again for failed operations. To retry the upload, select the IP address or hostname of the devices that did not get upgraded, then click **Retry**. To attempt the upload again for all devices that did not get upgraded, do not select any IP addresses or hostnames before clicking **Retry**.
 - **Save Log**: Saves the log information to a text file (.txt).
 - **Cancel**: Terminates the upload operation.
12. Click **Close** when the upload is complete. When the device accepts the file, the device indicates this change of state. The IP SLA flashes the online LED and the SL Status LED once per second while it erases and programs its flash memory

Database Converter Utility

You can use the DB Converter utility to upgrade database parameters from an existing version to a later version of software. You *cannot* downgrade to a previous version database. You can also convert an Inter-Tel Axxess v5.3 or later database to a Mitel v2.2 database and then convert to later Mitel 5000 software versions, if applicable.

This guide provides information for converting Mitel 5000 v2.4 databases to Mitel 5000 v3.0. For information about converting databases from earlier Mitel 5000 software versions, or for information to convert an Inter-Tel Axxess database to a Mitel 5000 database, refer to the following resources:

- The *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000 (and supporting documentation) for the applicable software release number
- *Mitel 5000 DB Programming Help*

Conversion Notes

The following are conversion notes:

With Mitel 5000 v2.4 and later:

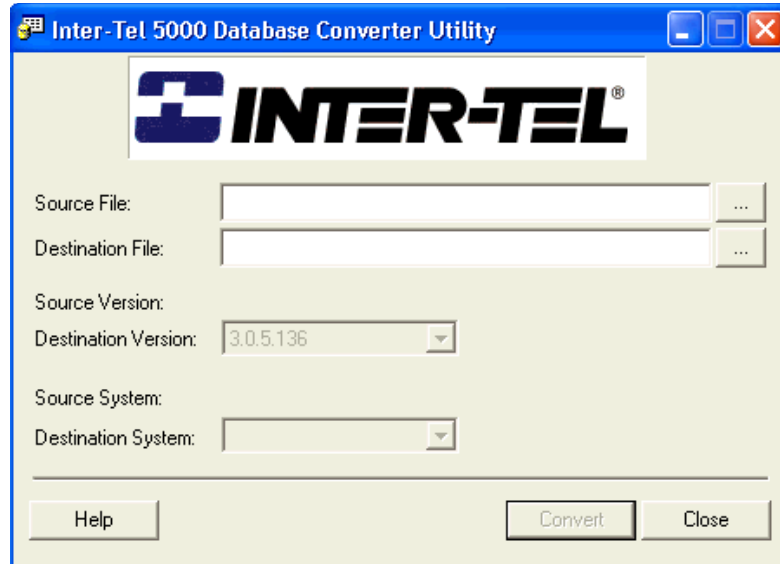
- The DB Converter updates the keymap-related programming of databases when converting from v2.3 or earlier to v2.4 or later. The conversion includes the following updates:
 - The ID numbers of existing keymaps are incremented by 1 (for example, Keymap #3 in v2.3 becomes Keymap #4 in v2.4). This is because the system assigns “Keymap #1” from the previous version to “Default Keymap” in the new version.
 - Additional programmable keys, 36–45, have been added to all endpoints and keymaps programmed in the database.
 - The Default keymap has been added to the databases. No existing endpoints reference this keymap, but any new endpoints programmed for v2.4 or later are automatically assigned to the Default Keymap.
- The DB Converter also performs IP Settings checks. If a database has static subnet masks or gateways programmed that are not the same for the Processor Module, Expansion Card, and Processing Server (checks fields accordingly based on system type), the converter copies the subnet mask and gateway from the Processor Module to the Expansion Card (for a Mitel 5400 or Mitel 5600 system) and the Processing Server (for a Mitel 5600 system). That way, they will all be on the same subnet/gateway. This conversion is also performed for the SSH port and enable, Web Server listening port and enable, listening port, and the DHCP flag of the Processing Server. If they do not match the Processor Module fields and the system is a Mitel 5600 system, the converter copies the value for each field from the Processor Module to the Processing Server.

Mitel 5000 Database Conversions

You can convert Mitel 5000 databases to later versions.

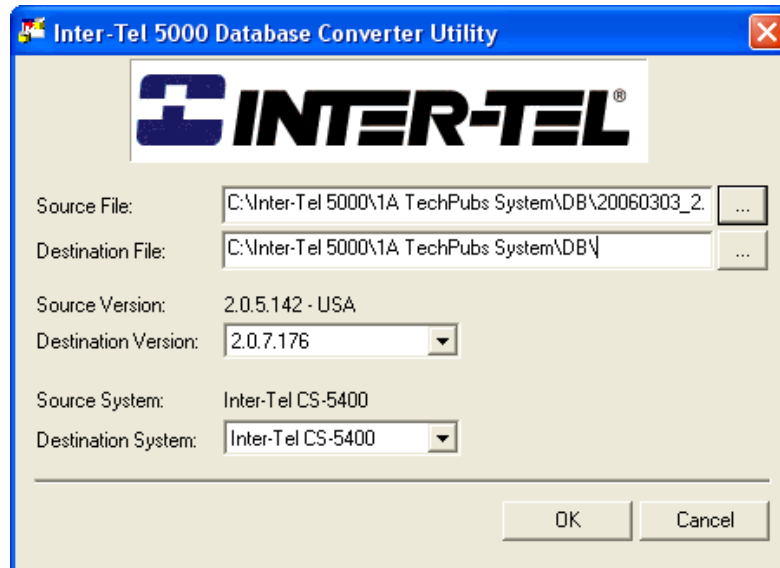
To convert a database from one version to another:

1. Upgrade the system software to the version you want running on the system after completing the upgrade process. For more information system upgrades, refer to the "Installation" chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000)
2. To open the Database Conversion Utility, select Start – All Programs – Inter-Tel 5000 DB Programming – **Inter-Tel 5000 DB Converter**. The following dialog box appears.

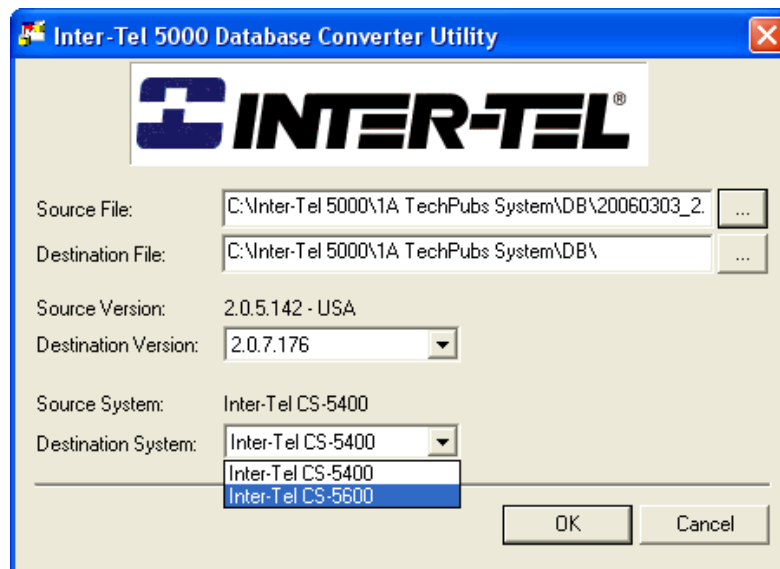


3. Click the **ellipsis** button at the right of the Source File box.
4. The database source files available for conversion display. You can browse to a different folder if necessary.
5. Select the existing database version that you want to upgrade. The selected file name appears in the File name box.

6. Click **Open**. The Database Converter Utility dialog box appears. The selected and opened source file appears in the Source File: box, and the Source Version appears below the Destination File: box. In the following illustration the source version is 2.0.5.142 - USA.



7. Click the **ellipsis** button at the right of the Destination File box.
8. If necessary, browse to search in the appropriate folder, and then select the .intl database file downloaded in step 5.
9. Select the target version from the Destination Version list.
10. Select the target system from the Destination System list.
11. Click **OK**. The source database version is converted to the target database version and system.



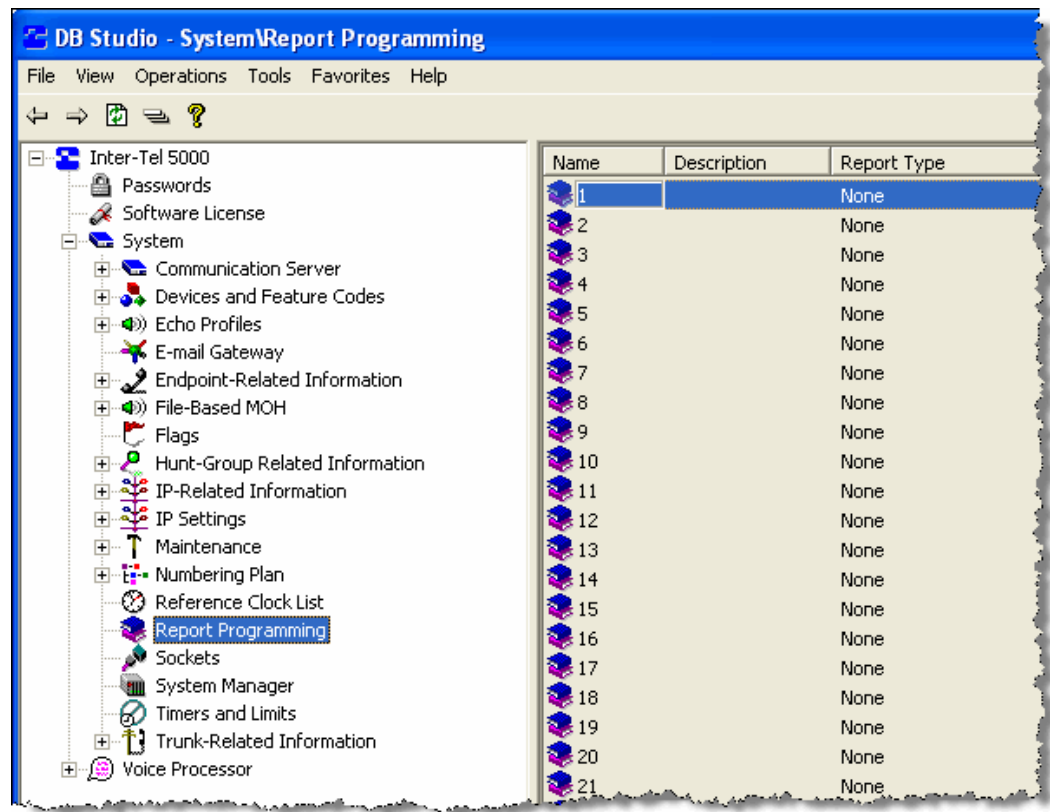
System and Enterprise Messaging Reports

Introduction	15-2
System Reports	15-3
System Report Types	15-3
Programming a System Report	15-4
Printing System Reports	15-5
Enterprise Messaging Voice Processing Reports	15-6
Report Parameters	15-6
Report Options	15-6
Application and Channel Statistics	15-6
Directory Listing Reports	15-7
Group List Report	15-7
Fax Delivery Reports	15-7
Fax Document Usage Report	15-7
Directory Sort Order	15-7
Using Automatic Report Generation	15-8
Report Selection	15-8
Statistics To Clear	15-8
Print Day	15-9
Print Time	15-9
Using Manual Report Generation	15-10
Report Selection	15-10
Statistics To Clear	15-10
Printing Reports	15-11

Introduction

You can use DB Programming to generate customized system and Enterprise® Messaging (EM) voice processing reports. [Figure 15-1](#) shows the system Report Programming area. The language used to create the report, American English for U.S. installations and British English for European installations, depends on the country selected in Session Manager.

Figure 15-1. Report Programming Location in DB Programming



System Reports

This section describes system reports. For voice processing reports, see “Enterprise Messaging Voice Processing Reports” on [page 15-6](#).

System Report Types

The following are available report types and their options:

- **ARS Facility Group Report:** Lists the facility groups and their dial rules and/or trunk groups/nodes.
- **ARS Route Group Report:** Include dial patterns and/or facility groups.
- **Call Routing Report:** Shows the call routing tables.
- **Class of Service Report:** Includes the day/night lists of endpoints and the dial patterns for each class of service.
- **CO Trunk Groups Report:** Includes day/night answer access, day/night outgoing access, day/night emergency outgoing access, day/night ring in, toll restriction, and/or trunk lists.
- **Detailed Endpoint Report:** Lists selected endpoints with account codes, mailboxes, flags, port, endpoint-related information, programmable buttons, special purpose endpoint status, system forwarding, toll restriction, and/or voice mail information.
- **Endpoint Flags Report:** Lists enabled flags for selected endpoints.
- **General Endpoint Report:** Shows endpoint information including attendant, class of service, equipment, and/or special purpose endpoint status.
- **Hunt Group Report:** Lists hunt groups with their agent/member lists, supervisors, and/or timers.
- **Individual Trunk Reports:** Lists selected trunks with their answer supervision setting, connect trunk-to-trunk call on polarity reversal, disconnect timer, DTMF signaling information, hybrid balance setting, language, loop current dial tone detection, number of digits to receive, base number, service type, start type, and/or trunk group.
- **Keymaps Report:** Shows IP and digital endpoints, DSS keymap groups, and map diagrams are listed with their button assignments and/or endpoint lists.
- **Off-Node Devices Report:** Lists off-node applications, modems, IP connections, hunt groups, paging ports, paging zones, endpoints, and/or single line endpoints.
- **Phone List Report:** Lists selected endpoints, hunt groups, and page zones.
- **System Speed Dial Report:** Lists selected System Speed Dial numbers.
- **System Timers Report:** Lists selected system timers.
- **T1/E1/PRI Report:** Shows information for T1M and T1M-2 modules, including error statistics, error thresholds, flags, primary rate timers, and/or reference clock information. Note that you cannot select a certain port only to be in a report—it is always by module.
- **User Group Report (U.S. only):** Lists selected user groups with day/night lists of endpoints, allowed area and office codes, restricted area and office codes, and/or extended area codes.

Programming a System Report

To program a report:

1. Select System – **Report Programming** – *<report number>*.
2. In the **Report Type** column, select the report type from the list.



CAUTION

Changing the report type clears all information for the selected report.

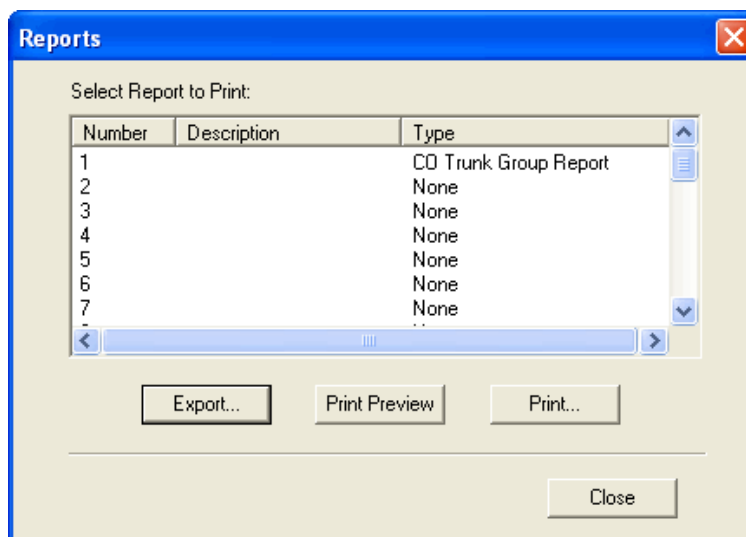
3. Click out of the field or press **ENTER** to save the change.
4. *Optional.* In the **Description** column, type a title for the report.
5. To program the report contents and options, double-click the report. The options shown depend on the report type. The following are report types:
 - **Modules:** Depending on the report type selected, the “modules” included in the report can be endpoints, hunt groups, trunks, call routing tables, ARS route groups, and so on. Double-click the module to select the devices to include in the report.
 - **Options:** Select **Options** to view available options for each report type. Select the check box to enable the option, and then click out of the field or press **ENTER** to save your change.
 - **Group Page Breaks:** Select this check box if you want to have each group (module, map group, hunt group, and so on) on a separate page of the report. Click out of the field or press **ENTER** to save your change.
6. To print the report, see [page 15-5](#).

Printing System Reports

The Print Reports option is not enabled until after a report is generated.

To print reports or export them to files:

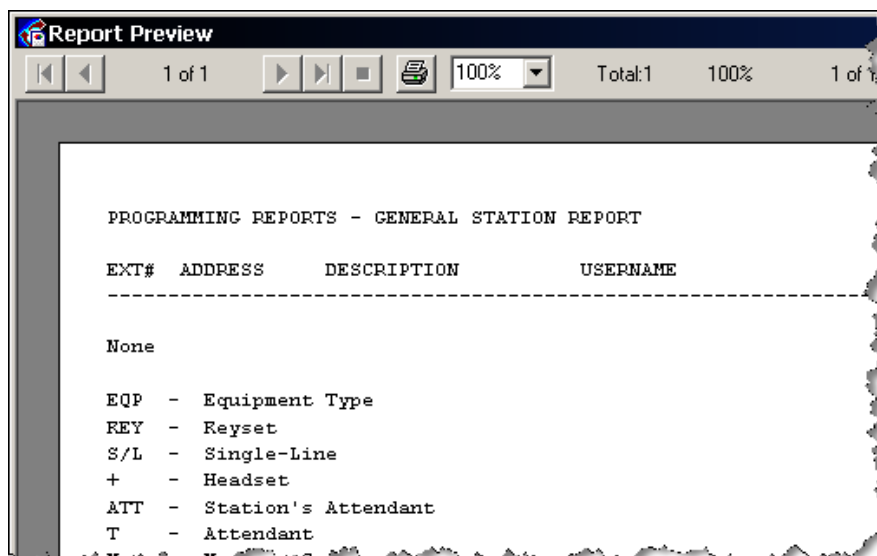
1. From the DB Programming menu bar, select Operations – **Print Reports**. The following dialog box appears.



2. In the **Select Report to Print** box, select the report.
3. Do one of the following:
 - Click **Print** to print the report.
 - Click **Export** to export the report as a .txt file.

To view the report before printing it:

1. Select **Print Preview**. A screen appears, as shown below, that shows the report exactly as it will print.
2. Page through the report using the arrow buttons at the top of the screen and change the view size. To print from this screen, select the printer icon.



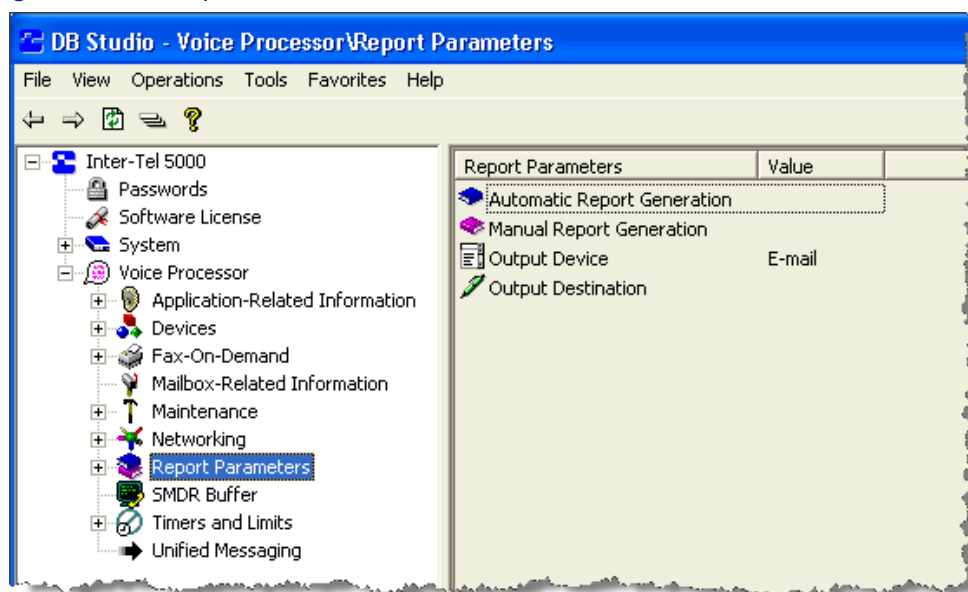
Enterprise Messaging Voice Processing Reports

You can use DB Programming to generate reports for Enterprise® Messaging (EM) systems only. You cannot generate reports for Basic Voice Mail (BVM) or NuPoint Messenger systems.

Report Parameters

The voice processing system can print reports from an external voice processing system to a printer or to a file for storage. The reports include Application and Channel Statistics, Directory Listings (by last name, first name, or extension), and Group List reporting. EM report parameters are shown in Figure 15-2.

Figure 15-2. EM Report Parameters



Report Options

Report selection options include the following:

Application and Channel Statistics

The following information appears individually for each application and as a summary for all applications.

- **Description and extension number of the application:** Shows the programmed name for the application. (Call Routing Announcement applications are all listed together by extension.) The applications are listed in the following order: Message Notification/Retrieval, Voice Mail, Auto Attendant, and Call Routing Announcement. (Auto Attendant Recall applications are reported within the Auto Attendant information.)
- **Incoming calls:** Shows the total number of calls received by that extension number. This is shown as a combined total for Call Routing Announcement applications.
- **Outgoing calls:** Shows the Message Notification/Retrieval application. These are the remote message notification calls placed by the Voice Mail application.
- **Connect minutes:** Shows the total time spent on incoming and outgoing calls (if any) combined. This is shown as a combined total for Call Routing Announcement applications.

- **Minutes per call:** Shows a combined total of the average amount of time spent on each call in minutes and seconds for Call Routing Announcement applications.
- **Transfers to Operator:** Shows the number of times a caller (within Voice Mail or Auto Attendant) presses the dial pad button 0 for operator access.
- **Voice Mail messages left:** Appears in the summary section only. It shows how many voice mail messages were left in all mailboxes combined.
- **Channel statistics:** Includes activity data of all applications. It shows, in 30-minute segments, the total number of minutes and seconds that all of the voice processing voice channels were busy simultaneously. The detailed segments begin at 07:00 AM and conclude at 06:00 PM. The “Off Peak Hours” segment shows statistics for the remaining time period (6:00 PM to 7:00 AM). This section ends with a grand total of busy channel occurrences for each of the days being reported.

If the number of voice channels programmed in DB Programming is greater than the number of actual channels available, the statistics reported will be based on the number available and **not** the programmed number.

Directory Listing Reports

You can sort directory listings by first name, last name, or extension/mailbox number (directory number). The listings show the mailbox description or extension ID, the mailbox/extension number, the message notification endpoint for mailboxes, and mailbox information. The mailbox information shows whether the mailbox is marked Private and/or Unlisted. (An X appears in the Mailbox field to indicate a mailbox that is neither Private nor Unlisted and a blank indicates that it is an extension ID.)

Group List Report

The Group List report provides a printed copy of the system group lists. The report identifies the group list number, the list description, and the mailboxes included in the group list.

Fax Delivery Reports

The Fax Delivery Report includes information for up to 200 fax delivery attempts. Each entry contains the date and time of the delivery attempt, the date and time the fax was requested, the delivery status (Successful, Busy, Call Failed, or Transmission Error), the fax number, and the list of requested documents. The Fax Delivery Report displays an asterisk (*) immediately to the left of the delivery status in the Fax Delivery Report for an entry representing a fax delivery that failed and was removed from the delivery queue. Fax deliveries can fail for many reasons, but the most common problem is that the fax number entered was not a fax machine, but was a company's main number or answering service. Review the Fax Delivery Report on a regular basis to check for delivery failures.

Fax Document Usage Report

This report lists all documents in the fax library by document number. Each entry shows the document number, description, how many times it was delivered to callers, the last request date, and the last revision date and time. If the document has not been revised, it shows the import date and time.

Directory Sort Order

(Available only if Directory Listing Reports are selected.) You can use the Directory Sort Order lists to select a sorting order from the following options: First Name, Last Name, or Directory Number.

Using Automatic Report Generation

You can use Automatic Report Generation to:

Set the day and time the system for automatic report printouts.

- Enable automatic report printouts.
- Clear system statistics.
- List the reports to print.
- Sort the Directory Listing report.

To enable automatic report generation:

1. Select Voice Processing – Report Parameters – **Automatic Report Generation**.
2. Select **Enable**.
3. In the **Value** column, select the check box to select the option. The field changes to **Yes**. To deselect the option, clear the check box.
4. Click out of the field or press **ENTER** to save the change.

Report Selection

You can select the report types that you want to generate.

To select report types:

1. Select Voice Processing – Report Parameters – **Automatic Report Generation**.
2. Double-click **Report Generation**. The report types appear in the right pane.
3. In the **Value** column, select the check box. The field changes to **Yes**. To deselect the option, clear the check box.
4. Click out of the field or press **ENTER** to save the change.

Statistics To Clear

You can select the following statistics to be cleared after a report is printed:

- **Application and channel**: Clears the information that is listed in the Application and-channel Statistics report only.
- **Fax Delivery and Document Usage**: Clears all statistics for the Fax Delivery report and the request count and last request date for the Fax Document Usage report.
- **Mailbox**: Clears all mailbox statistics.

To mark a statistic to be cleared:

1. Select Voice Processing – Report Parameters – **Automatic Report Generation**.
2. Select **Statistics to clear**.
3. In the **Value** column, select the check box. The field changes to **Yes**. To deselect the option, clear the check box.
4. Click out of the field or press **ENTER** to save the change.

Print Day

You can select the day in which the system prints the automatic reports.

To select the day to print automatic reports:

1. Select Voice Processing – Report Parameters – **Automatic Report Generation**.
2. Select **Print Day**.
3. In the **Value** column, select the day from the list.
4. Click out of the field or press **ENTER** to save the change.

Print Time

You can select the time of day in which the system prints the automatic reports.

To select the time of day for printing automatic reports:

1. Select Voice Processing – Report Parameters – **Automatic Report Generation**.
2. Select **Print Time**.
3. In the **Value** column, type or select the time (AM or PM).
4. Click out of the field or press **ENTER** to save the change.

Using Manual Report Generation

Manual Report Generation lists report types that you can print and the option to sort the Directory Listing report. You can also clear statistics after printing the reports.

Report Selection

Double-click **Report Selection** to view the list of available report types.

To enable a report:

1. Select Voice Processing – Report Parameters – **Manual Report Generation**.
2. Double-click **Report Generation**. The report types appear in the right pane.
3. In the **Value** column, select the check box. The field changes to **Yes**. To deselect the option, clear the check box.
4. Click out of the field or press **ENTER** to save the change.

Statistics To Clear

You can select the following statistics to be cleared after a report is printed. See [page 15-8](#) for descriptions.

To mark a statistic to be cleared:

1. Select Voice Processing – Report Parameters – **Manual Report Generation**.
2. Select **Statistics to clear**.
3. In the **Value** column, select the check box. The field changes to **Yes**. To deselect the option, clear the check box.
4. Click out of the field or press **ENTER** to save the change.

Printing Reports

To print the selected reports:

1. Select Voice Processing – Report Parameters – **Manual Report Generation**.
2. Right-click **Report Selection**, and then select **Print Selected Reports**.
3. From the list, select the output device. For a BVM system, the options are FILE or LPT1. For an EM system, the options are FILE or EMAIL.
 - If “LTP1” is selected, a printer must be attached to the parallel port on the voice mail server.
 - If “File” is selected, you must program the Output Destination field.
4. Click out of the field or press **ENTER** to save the change.

The following applies only if output device is “FILE” or “E-mail.”

- If the Output Device is File,
 - a. In the **File** box, type the name of the file (for example, C:\avdap\reports.txt).
 - b. Click out of the field or press **ENTER** to save the change. The system validates that the specified drive output is defined, but does **not** validate that the path exists on the voice processing computer. Instead, the database manager verifies that the file syntax is correct (for example, check for valid characters). If only the file name is entered, the system saves the report using the file name under the Avdap directory.
- If the Output Device is Email,
 - a. Type the e-mail address (for example, johndoe@abc.com) in the box.
 - b. Click out of the field or press **ENTER** to save the change.
- If the e-mail address is invalid or if the destination mailbox is full, the system generates a voice mail message indicating that the report could not be delivered. This message is left in the designated system administrator voice mailbox.

System Diagnostics

Introduction	16-3
Digital Trunk Diagnostics	16-3
Database Test and Repair Utility	16-3
Busy Out Manager	16-4
Database Change Log	16-6
General Guidelines	16-6
How to Read the Database Change Log	16-7
General	16-7
Header and Footer	16-7
Field Changes	16-8
Other Changes	16-9
Tools Menu	16-12
Operations Menu	16-13
View Menu	16-18
Audio Diagnostics	16-19
Audio Direction	16-21
Record-A-Call	16-22
Data Collection	16-22
Using the Audio Diagnostics Feature	16-22
Responding to the Audio Diagnostics Feature	16-23
Network Group Diagnostics	16-24
Oversubscription/IP Resource Sharing Statistics	16-24
IP Resource Sharing Log File	16-25
Hybrid Balance Test	16-26
Improved Hybrid Balance Line Settings	16-26
Hybrid Balance Test Options	16-27
Running a Hybrid Balance Test	16-27
Running a Hybrid Balance Test on Single Trunk	16-27
Running A Hybrid Balance Test for All Trunks	16-28
Viewing Hybrid Balance Test Results in Message Print	16-29
Viewing Hybrid Balance Results	16-31
Manually Changing the Hybrid Balance Setting	16-32

Alarms	16-33
Alarm Types	16-33
Network Alarms	16-34
Displaying Alarms	16-34
Alarm Queue	16-35
Clearing an Alarm	16-36
Responding to a Major Alarm	16-36
Diagnostics Through DB Programming	16-37
Automatic Diagnostics Delivery	16-37
System Device Information	16-37
Associated Devices and References	16-38
Periodic Diagnostics	16-40
System Software Performance Statistics	16-40
Database Operations	16-41
Error Information	16-41
IP Device Status	16-42
Voice Processing Diagnostics	16-42
Other Diagnostic Features	16-43
Administrator Endpoint Support	16-43
Diagnostics Feature Codes	16-43
Online Monitor Command Line	16-46
System Diagnostics Commands	16-46
Application Diagnostics Commands	16-47
LCD Panel Diagnostic Options	16-47
Resource Manager CPH Diagnostics Flag	16-48
Call Processing History (CPH) Freeze File Compression	16-48
History Queues/Log Files – Clearing	16-48
Traceroute	16-48
External Diagnostic Resources	16-49
Administrative Web Session	16-49
System Manager	16-49
Raw Commands	16-49

Introduction

System diagnostics are provided to assist trained personnel in monitoring and maintaining the functional health of the system. This chapter provides fundamental instruction for interpreting the output data from the utilities.

Depending on the problem and the data that has been collected during troubleshooting, technical support personnel may require additional information to perform their analysis. In many instances, diagnostic utility information and instruction is provided by the product specialist and may not be covered in this chapter. Some diagnostics should be performed only when directed by authorized technical support personnel.

This section provides information about diagnostic applications available throughout the system and associated software components. In the following sections, the applications are organized and grouped by their location in the system or a component within the system. The information that is provided for each application includes:

- Where the application is located in the system.
- Instructions on how to implement the application.
- The purpose of the application; for example, identification of the information captured.
- How to use the information from the application for troubleshooting.

Digital Trunk Diagnostics

For digital trunk diagnostics information, refer to the “System Diagnostics” chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

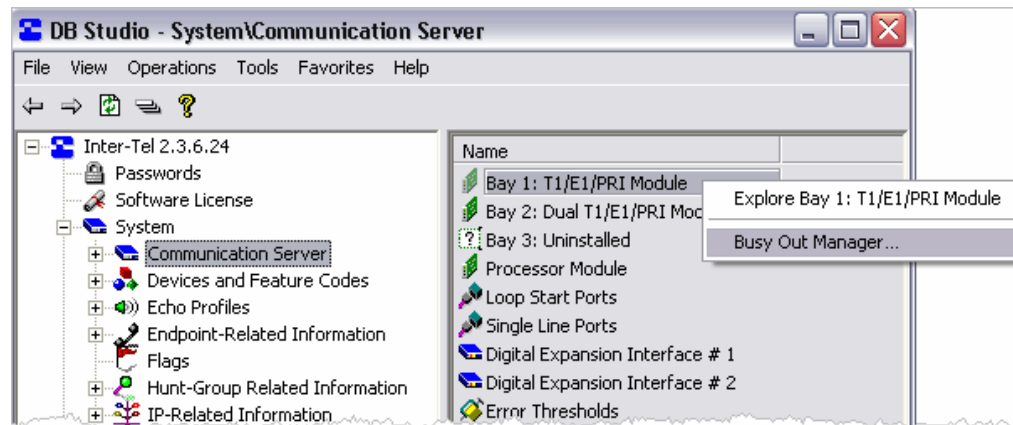
Database Test and Repair Utility

The Database Test and Repair utility tests databases for corruption and referential integrity. For more information, see “DB Test and Repair Utility” on [page 14-7](#).

Busy Out Manager

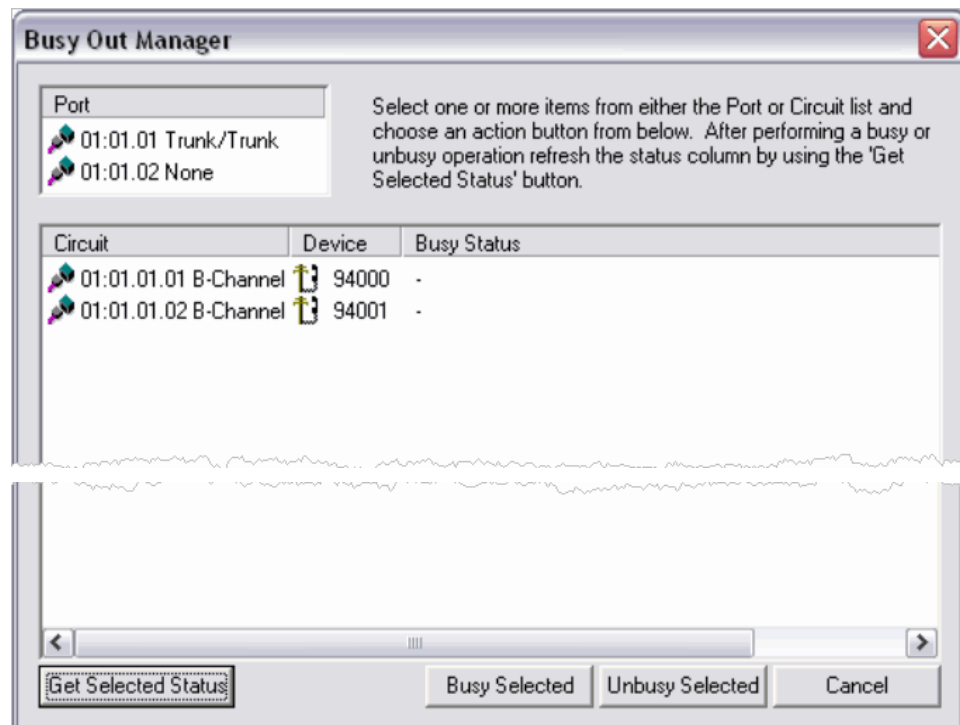
A context menu item appears for Dual T1/E1/PRI, T1/E1/PRI, and Basic Rate modules that allows you to open the Busy Out Manager. You must be in the Communication Server view in Remote Mode to access the Busy Out Manager.

Figure 16-1. *Busy Out Manager*



The Busy Out Manager allows you to select ports or circuits from a list and specify Busy Out commands for the selected items. The Busy Out Manager displays all ports on the selected module as well as what type of port is configured (a "None" device will be shown if the port has not been configured). Selecting a port displays the devices/circuits programmed for that particular port (devices/circuits that have not been configured will *not* show up as a None device).

Figure 16-2. *Busy Out Manager Programming*



When you first open the Busy Out Manager for a particular module, the status of the devices/circuits are unknown (shown as a '-') as they have not been retrieved yet. Anytime you want to see the "current" status of a particular item, you must select one or more items from either the ports view or devices/circuits view, and then click the **Get Selected Status**. If you choose to retrieve the status at the port level, the command may take a few seconds as it is retrieving status for every device/circuit programmed for the selected port(s).

You can similarly perform busy out operations on item selections from either the ports view or the device/circuits view.

To busy out items, do one of the following:

- Select one or more ports.
- Select one or more devices/circuits, and then click **Busy Selected**.

For example, if you want to busy out the entire board, select all of the ports in the port list, and then click **Busy Selected**.

NOTE

Performing a "Busy Selected" action does not display the current status. The status for the devices/circuits instead displays "Pending Status Update," at which point you must retrieve the status.

In the same way that you can perform busy out operations you can perform unbusy operations. Following the same steps as above, however, instead of clicking **Busy Selected** you would click **Unbusy Selected**.

There are several different statuses that may be shown in the Busy Out Manager. The display string and their meaning can be found in the table below.

Table 16-1. *Busy Out Statuses*

Status	Meaning
-	The status of the device/circuit is unknown. To get the status, select the device/circuit, and then click Get Selected Status .
Not Scheduled For Busy Out	The device is operable. It may be idle or active, but it is not currently busied out or scheduled for busy out.
Busy	The device/circuit has been set to busy by the Busy Out Manager.
Pending Busy	The device has been scheduled to be busied out, but is currently in use.
Pending Status Update	The user has actioned an item for Busy/Unbusy. You need to retrieve the status.

Database Change Log

The Database Change log provides details on user changes to DB Programming. The log details recent user changes to facilitate diagnostics. The Database Change log is written and maintained by the Mitel 5000. It is stored on the Mitel 5000 and is accessible through the Administrative Web Session (AWS) interface. For more information, refer to AWS Help.

The naming convention for the log filename is `cp_database_log_<date and time>.txt`, where date and time indicates when the file was created. The maximum file size allowed is 200 KB. Like other system logs, after the first log file reaches the maximum size, the system creates a new log file. After the second log file reaches the maximum size, the system deletes the oldest backup log file, and then logs to a new log file. The Mitel 5000 maintains two backup log files.

General Guidelines

The following list provides some general information about the Database Change log:

- All entries include the path to the folder or menu option from which the change was made, the name of the field that was changed, and the new value (if applicable).
- Numbers are translated to text whenever possible.
- The Database Change log file does not include DB Programming changes that occur behind the scenes. Some examples are:
 - You put an endpoint in Class of Service 2. Behind the scenes, DB Programming assigns the endpoint to User Group 1.
 - You delete a SIP Voice Mail. Behind the scenes, DB Programming deletes all mailboxes, group lists, and applications under that SIP Voice Mail.
 - You unequip endpoint 1003, which was the attendant for endpoint 1004. Behind the scenes, DB Programming sets the attendant for 1004 to NONE.
 - You delete a trunk group. Behind the scenes, DB Programming puts all trunks that were in that group into the unused trunk group. Then DB Programming goes through and replaces all links to that trunk group with the appropriate replacement (usually NONE).
- Changes are included for Remote sessions only. Local session changes are not included, other than the indication of when you perform a Database Restore. See [page 16-14](#) for an example.
- Changes made to DB Programming outside of the DB Programming application are not included in this log. Examples of changes that are not included:
 - Administrator endpoint programming
 - Automatic exports from other nodes
 - Equip off-node device event
 - Automatic DB Backup Save/Restore attempts
 - System OAI
 - User endpoint programming
 - Date/Time updates

How to Read the Database Change Log

Database Change Log entries are categorized as follows:

- “General” below
- “Header and Footer” below
- “Field Changes” on [page 16-8](#)
- “Other Changes” on [page 16-9](#)
- “Tools Menu” on [page 16-12](#)
- “Operations Menu” on [page 16-13](#)
- “View Menu” on [page 16-18](#)

General

This section details some general information about the Database Change Log:

- Every log entry begins with the date and military time:

```
[2008-01-30 11:20:11 DBP] <text>
```

- The “DBP” service name that is included after the timestamp does not appear if the log file is stored on the DB Programming computer (instead of the Mitel 5000).
- All changes are logged regardless if they are in On-Line Monitor (OLM) mode or not. OLM-only field changes are designated as “OLM.”

```
[YYYY-MM-DD-HH:MM:SS DBP] [Folder] Changed <Field> to <New Value> - OLM
```

Header and Footer

This section contains information about the header and footer of the Database Change Log.

- The following text appears for each session that is initiated:

```
[2008-01-30 11:19:48 DBP] CP SESSION ESTABLISHED - Database
Programming Client Address: 192.168.1.37
[2008-01-30 11:20:11 DBP] User Information: jsmith on smith2-0xp
[2008-01-30 11:20:11 DBP] Database Programming Version: 3.0.1.5
[2008-01-30 11:20:12 DBP] Call Processing Version: 3.0.1.13
[2008-01-30 11:20:12 DBP] Voice Processor Type: Basic
[2008-01-30 11:20:12 DBP] Voice Processor Version: 3.0.1.13
```

The version numbers for each component clearly show when you perform an upgrade. You can also search by a specific component version.

- The following text appears for each session that is terminated:

```
[2008-01-30 11:15:27 DBP] SESSION TERMINATING WITH <status>
[2008-01-30 11:15:27 DBP] CP SESSION TERMINATED - Database
Programming Client Address: 192.168.1.37
```

- The termination status includes the following:
 - **SUCCESS**: The session terminated with success.
 - **WARNING** - <text>: The session completed, but warning text appears.
 - **FAILURE** - <text>: An error caused the session to terminate. Error text appears.

If the session terminates in such a way that DB Programming does not post a termination entry to the log, only the CP SESSION TERMINATION message appears.

Field Changes

This section details the field changes in the Database Change Log. Many database changes are made through editing a field. When you edit a control and complete the edit, the change is saved to the database. These changes are always associated with a field in a folder hierarchy.

Each field change includes the following entry:

```
[YYYY-MM-DD-HH:MM:SS DBP] [Folder] Changed <Field> to <New Value>
- OLM
```

Some examples are:

```
[2008-01-28 12:58:22 DBP] [Passwords\2] Set Description to John
[2008-01-28 12:58:35 DBP] [Passwords\2] Set Password to #####
[2008-01-28 12:58:59 DBP] [System Forwarding Paths\2] Set
Description to test2
[2008-01-28 12:59:18 DBP] [System Forwarding Paths\2] Set
Forwarding Point 3 to 1001
[2008-01-30 13:22:23 DBP] [System Information\Meta Database] Set
Echo Profiles to 26 - OLM
```

- Where *[Folder]* is the path to the folder in which the field resides. This is limited to two levels up, except in the following situations:
 - “Inter-Tel 5000” appears only for items that are changed at the highest level.
 - “System” appears for only items that are changed at the System level.
 - If the second level up is a number or shows “local,” one more level appears.
 - The folder path will always go up high enough to show the affected extension.
- Where *<Field>* is the column header or field name.
- Where *<New Value>* is the new value.
- “OLM” appears for OLM-only fields.

Other Changes

This section details other changes in DB Programming:

- **Device Additions and Deletions:**
 - The device type and extension(s) always appear.
 - The hardware address appears when it is available.
 - Items added in a batch are grouped on one line only when they do not have hardware addresses. A batch item with a hardware address appears on its own line.
 - Some examples are:

```
[2008-01-30 13:24:18 DBP] [Endpoints] Added 1001
[2008-01-30 13:24:18 DBP] [1001] Set MAC Address to
00:10:36:00:10:01
[2008-01-30 13:24:43 DBP] [Endpoints] Added 1002,1003,1004
[2008-01-30 13:24:43 DBP] [1002] Set MAC Address to
00:10:36:02:FF:FF
[2008-01-30 13:24:43 DBP] [1003] Set MAC Address to
00:10:36:03:FF:FF
[2008-01-30 13:24:44 DBP] [1004] Set MAC Address to
00:10:36:04:FF:FF
[2008-01-30 13:25:05 DBP] [Trunks] Added 94000
[2008-01-30 13:25:17 DBP] [Trunks] Added 94001
[2008-01-30 13:25:17 DBP] [94001] Set Endpoint Name to E1
[2008-01-30 13:25:17 DBP] [94001] Set Gateway Name to G1
[2008-01-30 13:25:48 DBP] [Bay 1: Loop Start Module - 2\01.01]
Added 94002 (Loop Start)
[2008-01-30 13:25:49 DBP] [Bay 1: Loop Start Module - 2\02.01]
Added 94003 (Loop Start)
[2008-01-30 13:26:30 DBP] [01:02.01 T1\T1 Circuits\01.01] Added
1005 (Single Line)
[2008-01-30 13:26:38 DBP] [01:02.01 T1\T1 Circuits\01.02] Added
94004 (Ground Start)
[2008-01-30 13:26:44 DBP] [01:02.01 T1\T1 Circuits\01.03] Added
94005 (DID)
[2008-01-30 13:26:49 DBP] [01:02.01 T1\T1 Circuits\01.04] Added
94006 (E&M)
[2008-01-30 13:27:24 DBP] [01:03.01 E1/PRI\E1 Circuits\01.01]
Added 94007 (B-Channel)
[2008-01-30 13:27:25 DBP] [01:03.01 E1/PRI\E1 Circuits\01.02]
Added 94008 (B-Channel)
[2008-01-30 13:27:27 DBP] [01:03.01 E1/PRI\E1 Circuits\01.03]
Added 94009 (B-Channel)
[2008-01-30 13:27:28 DBP] [01:03.01 E1/PRI\E1 Circuits\01.04]
Added 94010 (B-Channel)
[2008-01-30 13:27:42 DBP] [Hunt Groups] Added 2000
[2008-01-30 13:27:53 DBP] [Page Zones] Added 9600,9601,9602
```

- **List Additions and Deletions and Drag, Drop, and Move:**

- The item type always appears.
- The extension appears for lists that have an extension.
- Added, deleted, or moved items are listed by ID or extension.
- Some examples are:

```
[2008-01-30 13:27:53 DBP] [Page Zones] Added 9600,9601,9602
[2008-01-30 13:30:27 DBP] [System Speed Dial] Added
001,002,003,004
[2008-01-30 13:31:30 DBP] [Hunt Groups\2000\Members] Added
1005,10220,10221 starting in position 1
[2008-01-30 13:32:01 DBP] [Hunt Groups\2000\Supervisors] Added
1000
[2008-01-30 13:32:32 DBP] [Forced\Non-Validated\All Calls] Added
1001,1002
[2008-01-30 13:32:44 DBP] [Forced\Non-Validated\Long-Distance Toll
Calls] Added 1002
[2008-01-30 13:32:59 DBP] [Account Codes\None] Added 1001
[2008-01-30 13:33:07 DBP] [Forced\Non-Validated\Long-Distance Toll
Calls] Removed 1002
[2008-01-30 13:33:37 DBP] [Page Zones] Deleted 9602
```

- **Change Extension:**

- Each extension appears on a separate line even if they are batch mode changes.
- Some examples are:

```
[2008-01-30 13:34:39 DBP] [Endpoints\1002] Changed extension to
2001
[2008-01-30 13:34:39 DBP] [Endpoints\1003] Changed extension to
2002
[2008-01-30 13:34:39 DBP] [Endpoints\1004] Changed extension to
2003
```

- **Copy and Paste:**

- The devices copied from and to are listed along with a list of attributes included in the copy.
- Some examples are:

```
[2008-01-30 15:45:26 DBP] [Loop Start\94257] Copied to 94258:
  Answer Supervision Type
  Connect Trunk-to-Trunk Call On Polarity Reversal
  DTMF Signaling
  Hybrid Balance
  Language
  Receive Gain
  Send Digits En Bloc
  Service Type
  Transmit Gain
  ---
[2008-01-30 15:46:09 DBP] [Hunt Group\2000] Copied to 2002:
  ACD Agent No Answer - DND Message Additional Text
  ACD Agent No Answer - DND Message Number
  ACD Hunt Group
  Agents
  Analog Voice Mail Hunt Group
  Announcement
  Audio for Calls Camped onto this Device
  Audio for Calls Ringing this Device
  Audio for Camped-On Announcement Calls
  Camp-Ons Allowed
  Group Call Pick-up
  Members
  Overflow
  Priority Level
  Recall
  Restart ACD Idle Time Upon Login
  Return ACD Calls to Hunt Group
  Search Type
  Send Camp-On Notifications to Members in DND
  Supervisors
  Timers
  Use ACD Agent IDs
```

- **Other Dialogs:**

- For changes made through dialogs (other than the wizards discussed later in the next section), the context is included in square brackets, and the field name appears with the new value.
- Some examples are:

```
[2008-01-31 14:09:53] [Key Assignments\IP/Digital Endpoint\1]
Changed Key 17 to Secondary Extension Key: 10220 - 5 rings
[2008-01-31 14:09:53] [Key Assignments\IP/Digital Endpoint\1]
Changed Key 19 to DSS/BLF Key: 10221
[2008-01-31 14:10:01] [Key Assignments\IP/Digital Endpoint\1]
Changed Key 32 to Programmable Key 15
```

Tools Menu

This section details the Tools Menu options of the Database Change Log:

- **Configuration Wizard:**

- Consists of a multi-line entry.
- “Configuration Wizard” appears as the first entry and a header.
- A line of text appears for each board and device configured and for each programming change.
- Examples:

```
[2008-02-06 06:28:45 DBP] Configuration Wizard:
Set SSH Server Enabled to No
Set Web Server Enabled to Yes
Set SSH Server Port to 22
Set Listening Port to 4000
Set Web Listening Port to 80
Set PPP IP Address to 192.168.201.209
[Inter-Tel 3.0.2.5] Added 1001
[1001] Set MAC Address to 00:10:36:00:10:01
[Bay 1] Added Loop Start Module - 4
[Bay 2] Added Dual T1/E1/PRI Module
[Inter-Tel 3.0.2.5\01.01] Added 94000 (Loop Start)
[Inter-Tel 3.0.2.5\02.01] Added 94001 (Loop Start)
[Inter-Tel 3.0.2.5\03.01] Added 94002 (Loop Start)
[Inter-Tel 3.0.2.5\04.01] Added 94003 (Loop Start)
[Bay 2 Port 1] Added T1 Module
[Bay 2 Port 2] Added E1/PRI Module
[DEI 1 Bay 1] Added Digital Endpoint Module - 16
[Inter-Tel 3.0.2.5\01.01] Added 1002 (Digital Endpoint)
[Inter-Tel 3.0.2.5\01.02] Added 1003 (Single Line)
```

- **Networking Wizard:**

- Consists of a multi-line entry.
- “Networking Wizard” appears as the first entry and a header.
- A line of text appears for each board and device configured and for each programming change.
- Examples:

```
[2008-02-06 06:31:20 DBP] Networking Wizard:
[Inter-Tel 3.0.2.5] Added 97002
[Inter-Tel 3.0.2.5] Added P8000
Set Node IP Connection Group to Conn to Node 2
Set Description to Chandler
Set Username to CHANDLER
[Inter-Tel 3.0.2.5] Added P6001
Set Remote IP Address to 192.168.200.208
Set Remote Audio Receive Port to 6004
Set Remote Listening Port to 5570
Set Description to ChandlerNode
Set Username to CNODE
[Remote Node\97002] Added Node Trunk/IP Connection Groups
(P8000) in position 1
```

- Example of results from the T1/PRI Networking Wizard:

```
[2008-02-06 06:33:58 DBP] Networking Wizard:
Set Node to 168
[Inter-Tel 3.0.2.5] Added 97501
Set Description to Conn to Node 2
Set Username to
Set Reference Clock List to 2
[Inter-Tel 3.0.2.5\02.01] Added 94004 (B-Channel)
[Inter-Tel 3.0.2.5\02.02] Added 94005 (B-Channel)
[Inter-Tel 3.0.2.5\02.03] Added 94006 (B-Channel)
[Inter-Tel 3.0.2.5\02.04] Added 94007 (B-Channel)
[Inter-Tel 3.0.2.5\02.05] Added 94008 (B-Channel)
[Remote Node\97002] Added Node Trunk/IP Connection Groups
(P8000,97501) starting in position 1
```

- **Resource Reservation Tool:**

- Consists of a multi-line entry.
- “Resource Reservation Tool” appears as the first entry and a header.
- A line of text appears for each programming change.
- The old value appears along with the new value.
- Examples:

```
[2008-02-06 06:36:19 DBP] Resource Reservation Tool:
Set [1000] Reserved to Yes
Changed G.711 Endpoints from 0 to 2 - OLM
Changed G.711 Trunks from 0 to 3 - OLM
Changed G.729 Endpoints from 0 to 6 - OLM
Changed G.729 Networking from 0 to 9 - OLM
Changed Emergency/911 Resources Reserved from 1 to 2
Changed Basic Voice Mail Port Resources Reserved from 0 to
2
Changed Maximum Simultaneous Fax Over IP (T.38) from 0 to
2
```

Operations Menu

This section details the Operations Menu options of the Database Change Log:

- **Database Save:**

- “Begin Database Save To <path>” appears as the first entry.
- “Begin Voice Data Save To <path>” appears as the second entry if voice data was saved also.
- The following entry consists of one of the following messages:
 - “Completed with Success” when the operation completes successfully.
 - “Terminated with Warning – <warning>” when the operation terminates with a warning.
 - Terminated with Failure – <error>” when the operation fails.
- Examples:

```
[2008-02-05 20:03:32 DBP] Begin Database Save To <path>...
[2008-02-05 20:03:32 DBP] Begin Voice Data Save To <path>...
[2008-02-05 20:10:37 DBP] Completed with Success
[2008-02-05 20:10:37 DBP] Terminated with Warning - <warning>
[2008-02-05 20:10:37 DBP] Terminated with Failure - <error>
```

- **Backup Database Save:**

- “Begin Backup Database Save” appears as the first entry.
- The following entry consists of one of the following messages:
 - “Completed with Success” when the operation completes successfully.
 - “Terminated with Warning – *<warning>*” when the operation terminates with a warning.
 - Terminated with Failure – *<error>*” when the operation fails.
- Examples:

```
[2008-02-05 20:10:33 DBP] Begin Backup Database Save...  
[2008-02-05 20:10:37 DBP] Completed with Success  
[2008-02-05 20:10:37 DBP] Terminated with Warning - <warning>  
[2008-02-05 20:10:37 DBP] Terminated with Failure - <error>
```

- **Database Restore:**

- “Begin Database Restore From *<path>*” appears as the first entry.
- “Begin Voice Data Restore From *<path>*” appears as the second entry if voice data was restored also.
- The following third entry consists of one of the following messages:
 - “SESSION TERMINATING WITH SUCCESS” when the operation completes successfully.
 - “SESSION TERMINATING WITH WARNING: *<warning>*” when the operation terminates with a warning.
 - “SESSION TERMINATING WITH ERROR: *<error>*” when the operation fails.
- “CP SESSION TERMINATED...” is the last entry always because the programming session always terminates after a Database Restore operation.
- Examples:

```
[2008-02-05 20:03:32 DBP] Begin Database Restore From <path>...  
[2008-02-05 20:03:32 DBP] Begin Voice Data Restore From <path>...  
[2008-02-05 20:03:48 DBP] SESSION TERMINATING WITH SUCCESS  
[2008-02-05 20:03:48 DBP] SESSION TERMINATING WITH WARNING:  
<warning>  
[2008-02-05 20:03:48 DBP] SESSION TERMINATING WITH FAILURE:  
<error>  
[2008-02-05 20:03:50 DBP] CP SESSION TERMINATED - Database  
Programming Client Address: 192.168.1.37
```


- **Default Database:**

- “Begin Default Backup Database” appears as the first entry.
- The next entry consists of one of the following messages:
 - “Completed with Success” when the operation completes successfully.
 - “Terminated with Warning – *<warning>*” when the operation terminates with a warning.
 - Terminated with Failure – *<error>*” when the operation fails.
- “Default Database” appears as the third entry.
- The fourth entry consists of one of the following messages:
 - “SESSION TERMINATING WITH SUCCESS” when the operation completes successfully.
 - “SESSION TERMINATING WITH WARNING: *<warning>*” when the operation terminates with a warning.
 - “SESSION TERMINATING WITH ERROR: *<error>*” when the operation fails.
- “CP SESSION TERMINATED...” is the last entry always because the programming session always terminates after a Database Restore operation.
- Examples:

```
[2008-02-05 06:05:45 DBP] Begin Default Backup Database...
[2008-02-05 06:05:45 DBP] Completed with Success
[2008-02-05 06:01:40 DBP] Default Database
[2008-02-05 06:01:44 DBP] SESSION TERMINATING WITH SUCCESS
[2008-02-05 06:01:44 DBP] CP SESSION TERMINATED - Database
Programming Client Address: 192.168.1.37
```

- **Error Information:**

- “Error Information History Queue Frozen” appears as the first entry when a history queue freeze occurs.
- “Begin Error Information Save” appears as the next entry when the error information is saved.
- The next entry consists of one of the following messages:
 - “Completed with Success” when the operation completes successfully.
 - “Terminated with Warning – *<warning>*” when the operation terminates with a warning.
 - Terminated with Failure – *<error>*” when the operation fails.
- “Error Information History Queue Unfrozen” is the last entry when a history queue unfreeze occurs.
- Examples:

```
[2008-02-06 06:01:35 DBP] Error Information History Queue Frozen
[2008-02-06 06:01:46 DBP] Begin Error Information Save...
[2008-02-06 06:01:49 DBP] Completed with Success
[2008-02-06 06:01:52 DBP] Error Information History Queue Unfrozen
```

- **Export/Import Devices:**

- “Begin Export” or “Begin Import” appears as the first entry when a device is exported or imported.
- The nodes are listed next, followed by the device types.
- After the list of device types, “Results” appears with a timestamp, followed by the specific results for each node.
- The last entry includes one of the following messages:
 - “Completed with Success” when the operation completes successfully.
 - “Terminated with Warning – *<warning>*” when the operation terminates with a warning.
 - Terminated with Failure – *<error>*” when the operation fails.
- An example of a successful export is:

```
[2008-02-06 14:33:50 DBP] Begin Export...
      Nodes included:
            1   Robec
      Device Types included:
            Digital Endpoint
            Single Line
            Hunt Group
            Page Port
            Page Zone
            Voice Mail
            Message Notification/Retrieval
            Call Routing Announcement
            Auto Attendant Recall
            Auto Attendant
            Record-A-Call
            Scheduled Time-Based Application Router (STAR)
            Unassociated Mailbox Off-Node Device
            Group List Off-Node Device
            B-Channel Station Off-Node Device
            IP Connection
            Modem
            Phantom Device
            Network Group
            ACD Agent ID
[2008-02-06 14:33:51 DBP] Results:
      Node 3: Export Source
      Node 1: COMPLETED
[2008-02-06 14:33:51 DBP] Completed with Success
```

- An example of a failed export is:


```
[2008-02-06 15:00:55 DBP] Begin Export...
      Nodes included:
            1   Robec
      Device Types included:
            Single Line
[2008-02-06 15:01:11 DBP] Results:
      Node 3: Export Source
      Node 1: Err -- Not Reachable
[2008-02-06 15:01:14 DBP] Terminated with Failure - The operation
failed for one or more nodes.
```

- **IP Device Status:** There is no logging information for this operation.
- **Print Reports:** There is no logging information for this operation.

- **Upload Software License:**

- “Begin Upload Software License” appears as the first entry along with the list of differences between the current license and the new license that will be uploaded.
- The second entry includes one of the following messages:
 - “Completed with Success” when the operation completes successfully.
 - “Terminated with Warning – *<warning>*” when the operation terminates with a warning.
 - Terminated with Failure – *<error>*” when the operation fails.
- The third entry appears if the license update requires a reset. This entry consists of one of the following messages:
 - “SESSION TERMINATING WITH SUCCESS” when the operation completes successfully.
 - “SESSION TERMINATING WITH WARNING: *<warning>*” when the operation terminates with a warning.
 - “SESSION TERMINATING WITH ERROR: *<error>*” when the operation fails.
- “CP SESSION TERMINATED...” appears as the last entry if the license update requires a reset because the session always terminates after a reset.
- Examples:

```
[2008-02-06 06:11:00 DBP] Begin Upload Software License...
    Changed Creation Date from Feb 01, 2008 (13:51:28) to Feb
04, 2008 (12:47:13)
    Changed System Health Report from No to Yes
    Changed Digital Expansion Interface # 3 from No to Yes
    Changed File-Based MOH Sources from 3 to 4
[2008-02-06 06:11:03 DBP] Completed with Success
[2008-02-06 06:11:03 DBP] SESSION TERMINATING WITH SUCCESS
[2008-02-06 06:11:04 DBP] CP SESSION TERMINATED - Database
Programming Client Address: 172.30.203.19
```

 If a reset was required.

- **System Manager CA Certificate Upload:**

- “Upload System Manager CA Certificate from *<path>*” appears as the first entry.
- The second entry includes one of the following messages:
 - “Completed with Success” when the operation completes successfully.
 - “Terminated with Warning – *<warning>*” when the operation terminates with a warning.
 - Terminated with Failure – *<error>*” when the operation fails.
- Examples:

```
[2008-02-06 06:11:00 DBP] Upload System Manager CA Certificate
from <path>
[2008-02-06 06:11:03 DBP] Completed with Success
```

- **Voice Processor Save or Restore:**

- “Voice Processor [Save/Restore] (<type>) [to/from] <path>” appears as the first entry (where <type> is the radio button selected, for example Audiotex Recordings, Group Lists, Mailbox Information, etc.).
- The second entry appears with the details about the saved or restored type of information. The example below includes Mailbox Information.
- The second entry includes one of the following messages:
 - “Completed with Success” when the operation completes successfully.
 - “Terminated with Warning – <warning>” when the operation terminates with a warning.
 - Terminated with Failure – <error>” when the operation fails.
- An example of a Database Save for mailbox information is:

```
[2008-07-11 17:15:24 DBP] Begin Voice Processor Save Mailbox Info
To U:/...
      Mailbox Info Included: Name/Greeting,Saved Msgs,New
Msgs,Data
      Items Included: 1000-1001,10220-10221
[2008-07-11 17:15:43 DBP] Completed with Success
```

- **Enable and Disable Basic Voice Mail:**

An example of the entry is:

```
[2008-02-06 06:11:00 DBP] [Enable|Disable] Basic Voice Mail
```

- **Reset Call Processing Application:**

An example of the entry is:

```
[2008-02-06 06:11:00 DBP] Reset Call Processing App
```

- **Reset System:**

An example of the entry is:

```
[2008-02-06 06:11:00 DBP] Reset System
```

View Menu

This section details the On-Line Monitor option, available from the View Menu, in the Database Change Log. An example of the entry is:

```
[2008-02-06 06:11:00 DBP] [Enable|Disable] View On-Line Monitor
```

Audio Diagnostics

As an end-user diagnostic tool, the Audio Diagnostics feature allows a user to generate diagnostics information about audio problems. Once the Audio Diagnostics feature is initiated, users are prompted to answer questions about the audio problems by pressing the associated buttons on their endpoints. Based on the user's selections, the system generates alarm 128, which is displayed on the Administrator endpoint and on the LCD panel of the chassis. If Automatic Diagnostics Delivery (ADD) is enabled, the collected data is then sent to Mitel Technical Support. By default, ADD is not enabled. For more information, refer to the *Mitel 5000 Reference Manual*, part number 580.8007.

The Audio Diagnostics feature can be accessed when the endpoint is idle or when the user is on an active call. The amount of diagnostics information that the endpoint provides to the system depends on the state of the endpoint when the feature is accessed. For example, an active call produces more diagnostic information than a endpoint in an idle state. If users do not want to access the Audio Diagnostics feature while on a call, they can access the feature immediately after they hang up.

NOTE

The Audio Diagnostics feature is not available with System OAI Display Control because the external applications have control of the menu buttons and dialpad.

If the user accesses the Audio Diagnostics feature but does not respond to the prompts on the display, the feature times out after 30 seconds. If the user or the other party terminates the call before completing the diagnostics, the feature is terminated. When the feature times out or is terminated, the diagnostics information is not captured.

See [page 7-23](#) to enable the Audio Diagnostics flag for an endpoint.

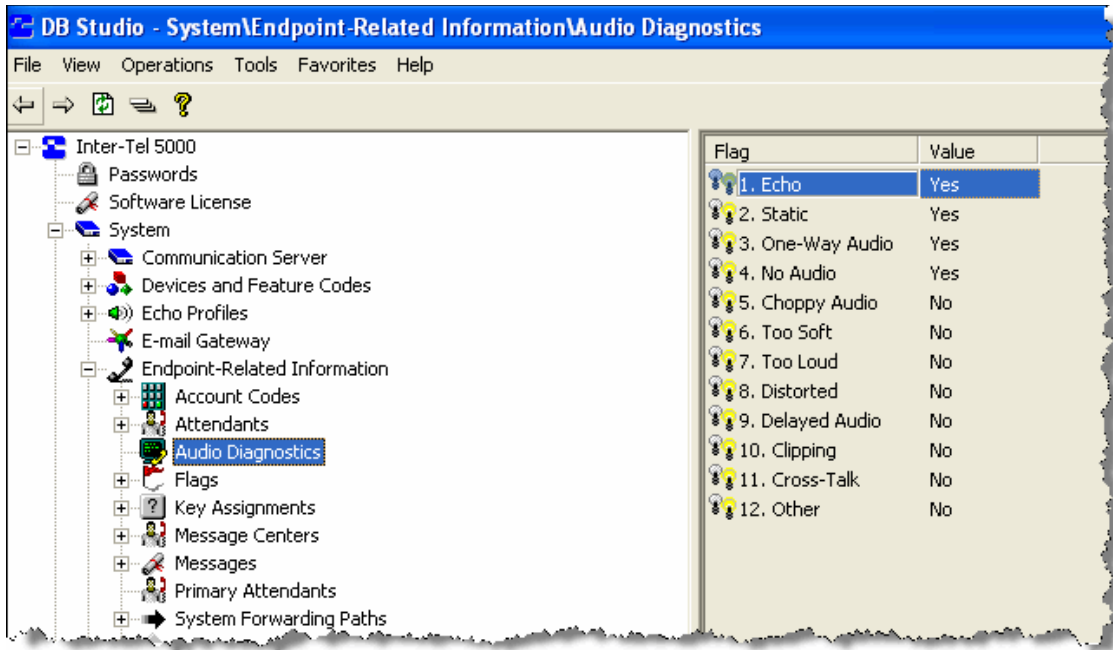
The Audio Diagnostics folder contains 12 flags that identify possible audio problems. You can have only four of the 12 problem numbers selectable from six-line display endpoints at any one time. The first four audio problem numbers are selected by default, including:

- 01 – Echo
- 02 – Static
- 03 – One-way audio
- 04 – No audio

To enable an Audio Diagnostics problem number:

1. Start a DB Programming session from the Mitel 5000 Session Manager.
2. From the left pane of DB Studio, select System – Endpoint-Related Information – **Audio Diagnostics**. The Audio Diagnostic flags and Yes/No options appear in the right pane, as shown in Figure 16-3.

Figure 16-3. Audio Diagnostics Options



3. Click one of the Yes values to turn it to No.
4. Click the value No value of the flag that you want to enable. The value turns to Yes.

The four selected audio problems appear as menu options on six-line display endpoints when the user accesses the Audio Diagnostics feature. Six-line users can also enter any of the 12 two-digit problem numbers from their dialpads, but they have the advantage of simply pressing a menu button if the audio problem is one of those enabled in DB Programming.

After accessing the Audio Diagnostics feature, two-line display and non-display endpoint users have only the option of entering one of the two-digit problem numbers to identify an audio problem. To use the feature, these users would need to have a list of the problem numbers and their meanings. Phantom devices and modems cannot apply the Audio Diagnostics feature code.Audio Problem

When the Audio Diagnostics feature—default feature code 320—is used, the system prompts the user to select a possible audio problem. Six-line display endpoint users can either press the menu button that corresponds to the displayed audio problem or enter the numeric codes. Users of 2-line display and non-display endpoints must enter the numeric codes because they do not have menu buttons.

Table 16-2 shows the 12 audio problems and their associated two-digit codes. However, only four can be enabled in DB Programming. By default, Audio Diagnostics problem numbers 01–04—Echo, Static, One-Way Audio, and No Audio, respectively—are enabled by default for display on six-line display endpoints.

Table 16-2. Audio Problem Codes

Audio Problem	Number	Audio Problem	Number
Echo	01	Too Loud	07
Static	02	Distorted	08
One-Way Audio	03	Delayed Audio	09
No Audio	04	Clipping	10
Choppy Audio	05	Cross-Talk	11
Too Soft	06	Other	12

Audio Diagnostics: In DB Programming, 12 flags identify audio problems that can be reported using Audio Diagnostics, default feature code 320. Any of the 12 flags can be entered from any endpoint dialpad after accessing the Audio Diagnostics feature. However, you can have only four problem numbers enabled at any one time to appear on six-line display endpoints.

In the default state, the first four audio problem flags are enabled, and the remaining eight are disabled. Once the selected audio problems are enabled (set to Yes), the problems are displayed as options on the endpoint when the user accesses feature code 320. Each audio problem has a unique number (01–12). These numbers are assigned for non-display users to access the feature. For instructions on how to use the feature, see “Using the Audio Diagnostics Feature” on [page 16-22](#).

Enable Audio Diagnostics: There is a Audio Diagnostics flag under System\Devices and Feature Codes\Endpoints\<Node>\<Extension>\Flags that enables the Audio Diagnostics feature for an endpoint. By default, this flag is disabled. To enable the Audio Diagnostics feature for the endpoint, set this flag to **Yes**.

Audio Diagnostic Alarm Suppression: This flag programmed under System\Flags gives you the option of suppressing Alarm 128, which is generated when the Audio Diagnostics feature is used. By default, this flag is set to **No**, which means that the alarm is generated and displayed on the administrator’s endpoint when a user access the Audio Diagnostics feature. If this flag is set to **Yes**, the alarm is suppressed.

Audio Direction

After selecting the audio problem, the system prompts the user to choose the direction of the audio problem. Options include:

- Only I hear it (2-line display and non-display users press **1**)
- Only the outside (2-line display and non-display users press **2**)
- We both hear it (2-line display and non-display users press **3**)

Record-A-Call

If the Record-A-Call feature has been programmed for the station, the user can record the call while using the Audio Diagnostics feature. See [page 16-22](#).

NOTE

The Record-A-Call feature cannot be used on certain calls such as Agent Help, Station Monitor, Conferences, Paging, and so on.

Data Collection

To collect the diagnostics data, retrieve the Freeze information or send the data to Technical Support via ADD. The diagnostics data that is collected consists of:

- Source endpoint (extension and module number)
- Destination endpoint (extension and module number)
- Phone number
- Echo canceller settings (IP Resource)
- Resource manager dump
- Crosspoint/voice channel information
- Current volume levels (near end)
- Hybrid balance values
- De-coupling values
- Network group

Using the Audio Diagnostics Feature

Only stations with the Audio **Diagnostics station flag** enabled can use the Audio Diagnostics feature. Only 6-line display endpoints have the menu buttons mentioned in the following instructions. The 2-line display and non-display endpoints must use the numeric entries to use the Audio Diagnostics feature.

To use the Audio Diagnostics feature:

1. **If the endpoint is idle**, while on hook enter the Audio Diagnostics feature code (320)

If you are on an active call, press ∞ then enter the Audio Diagnostics feature code (320).

ENTER TWO DIGIT AUDIO PROBLEM ECHO STATIC DELAYED AUDIO OTHER
--

The display shows ENTER TWO DIGIT AUDIO PROBLEM.

2. Do one of the following actions to select an audio problem:
 - Press the desired menu button.
 - Or, enter the two-digit numeric code (01–12) that corresponds to the audio problem—see [page 16-21](#). Consult your system administrator for the list of Audio Diagnostics codes that are used on your system.

The display shows PLEASE SELECT THE AUDIO DIRECTION.

3. Select the direction of the audio problem. Do one of the following actions:
 - Press the desired menu button.
 - Press the dialpad button that corresponds to one of the following responses:
 - Press **1** for ONLY I HEAR IT.
 - Press **2** for ONLY OTHER PARTY.
 - Press **3** for WE BOTH HEAR IT.

PLEASE SELECT
AUDIO DIRECTION

ONLY I HEAR IT
ONLY OTHER PARTY
WE BOTH HEAR IT

If the Record-A-Call feature is enabled for your endpoint, the display shows
WOULD YOU LIKE TO RECORD CALL?

4. If the Record-A-Call feature is available, you have the option of recording the call. Do one of the following actions:
 - a. Press the desired menu button.
 - b. Or, press the dialpad button that corresponds to one of the following responses:
 - Press **1** to record the call.
 - Press **2** to continue without recording.

WOULD YOU LIKE
TO RECORD CALL?

YES
NO

If the system cannot accurately record the call (e.g., because different cross-point connections are used) the display shows CALL CANNOT BE COMPLETED.

5. Hang up to complete the Audio Diagnostics feature. System Alarm 128 appears on the system administrator's display endpoint.

Responding to the Audio Diagnostics Feature

Once the user completes the Audio Diagnostics feature, the system generates Alarm 128 and the administrator station displays SYS ALARM #128 <EXT> AUDIO FRZ. This alarm indicates the extension that generated the Audio Diagnostics feature.

SYS ALARM #128
<EXT> AUDIO FRZ
CLEAR ALARM
CLEAR ALL ALARMS

IDLE MENU

To respond to Alarm 128:

Alarm 128 indicates that someone has completed the Audio Diagnostics feature, and you need to collect the freeze that contains Message Print entry. Review the freeze diagnostics data. If you need further assistance, submit the data to Technical Support for analysis.

For more information about collecting diagnostics data, contact Mitel Technical Support.

Network Group Diagnostics

Network Group Diagnostics feature allows you to verify that the Network Groups on the local node are programmed correctly. When the Network Group Diagnostics feature code is entered, the system initiates pings from each Mitel IP device on the local node and determines if the other devices respond to the ping. If a device does not respond to the ping or if a firewall is detected, the system issues a Message Print message.

When using Network Group Diagnostics, remember the following guidelines:

- The Network Group Diagnostics feature works on Mitel proprietary IP devices for the local node only. It does **not** work across nodes.
- Mitel recommends that you enable a port for Message Print before you run this diagnostics feature.
- Because this feature affects system performance, it is recommended that you run the diagnostics program when the system is idle (i.e., after normal business hours).

To run the Network Group Diagnostics:

1. At an administrator endpoint, enter the Diagnostics On/Off feature code (9900 by default) followed by the Network Group Diagnostics feature code (9963 by default). The display shows NET GRP CHECK (YES = 1, NO = 2).
2. When prompted, press 1 or **ACCEPT** to start the diagnostics feature. The display shows NET GROUP DIAG IN PROGRESS. In Europe, the default Diagnostics On/Off feature code is 9100, and the Network Group Diagnostics feature code is 9163.

When the diagnostics is complete, the endpoint displays one of the following messages:

- NET GROUP CHECK COMPLETED: Indicates that all IP devices within the Network Groups are capable of communicating via P2P audio.
- NET GROUP CHECK ERRORS FOUND: Indicates that either some of the IP devices are offline or there are NATs/firewalls located between the devices. Check Message Print to determine which errors occurred.

Oversubscription/IP Resource Sharing Statistics

The system performs periodic checks to verify whether the IP Device Resource Manager (IPDRM) and the DSP Resource Manager are in sync with IP calls in progress. From the data generated by these checks, the system computes and stores IP resource utilization statistics for diagnostic purposes, including the following measures:

- Average IP resource usage
- Average IP resource Camp On time
- Peak IP resource usage
- Number of times resources are *not* available for a user of a particular vocoder type
- Number of times resources are *not* available for a user of a particular call type
- Maximum Camp On time

All of the values can be viewed by using either AWS or System Monitor by dumping the IP Resource Statistics or the IPDRM Statistics. Additional information can be collected by dumping the IPDRM or the DSP Resource Manager.

IP Resource Sharing Log File

The IP Resource Sharing log file captures IP resource sharing, or oversubscription, information. You can view this log file from the Log Files page of the Administrative Web Session (refer to the AWS Help for details). The naming convention for the log filename is cp_sra_log_<date and time>.txt, where date and time indicates when the message was logged to the file. The maximum file size allowed is 200 KB. After the first log file reaches the maximum size, all new messages are rolled over to a second log file.

NOTE

The system stores only two oversubscription log files at any one time. After the second file is filled, the system wraps messages, overwriting the first log file.

Hybrid Balance Test

The Hybrid Balance Test automatically measures and assigns the best hybrid balance setting for analog loop start trunks. For optimum audio quality and performance, run the test for all loop-start trunks. Many system capabilities rely on proper Hybrid Balance settings, including echo cancellation (ECAN) and dual tone multi-frequency (DTMF).

You can use Message Print to confirm that the Hybrid Balance Test real-time test results. See “Viewing Hybrid Balance Test Results in Message Print” on [page 16-29](#).

For a complete feature description, refer to the “System Features” chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

NOTE

To obtain and maintain optimal Hybrid Balance Settings, do the following:

- Perform the test on each LSM port at initial installation of the system.
- Perform the test whenever an analog loop start trunk connection is added or changed.
- Run the test on a system that is idle or nearly idle.

Run the test until the greatest Echo Return Loss (ERL) measurement is within ± 2 dB twice in a row, as shown in Expanded Message Print. If the trunk-LSM port interface is optimally balanced, successive ERL readings should not vary much.

Improved Hybrid Balance Line Settings

There are eight line settings for the Electronic Industries Alliance (EIA) standard loop lengths, as shown in [Table 16-3](#). In DB Programming, you can view the line setting (see Figure 16-4 on [page 16-32](#)) that the system automatically assigns *after* running the Hybrid Balance test. However, you must restart DB Programming to view the setting (see “Running a Hybrid Balance Test” on [page 16-27](#)). You can also manually change this setting in DB Programming (see “Manually Changing the Hybrid Balance Setting” on [page 16-32](#)).

Table 16-3. EIA Standard Loop Length Line Settings and Descriptions

EIA Line	Description
0	Co-located, same AC impedance
1	2000 ft.
2	7000 ft.
3	8500 ft.
4	12,000 ft.
5	16,500 ft.
6	30,000 ft. loaded loop A
7	30,000 ft. loaded loop B

Hybrid Balance Test Options

The following are Hybrid Balance Test fields in DB Programming:

- **Hybrid Balance:** The line setting currently assigned to the trunk (see [page 16-32](#)).
- **Measured Echo Return Loss (ERL):** Shows the optimal ERL value measured during the last hybrid balance test. This field is undefined if the “Last Hybrid Balance Test Timestamp” shows “Untested.” Note this field is only updated when DB is first launched.
- **Last Hybrid Balance Timestamp:** Shows the month, day, year, and time of day of the last completed test. If this field contains the string “Untested,” the test has never run on the selected trunk and the “Measured Echo Return Loss” field is undefined.

The Measured Echo Return Loss (ERL) and the Last Hybrid Balance Test Timestamp values are updated only with the start of each DB Programming session. If a test is run during an active session of DB Programming, the fields will *not* be updated with the latest test results until DB Programming is restarted. If Expanded Message Print is enabled, the test results appear in Message Print output. See “Viewing Hybrid Balance Test Results in Message Print” on [page 16-29](#).

- **Connected to CO:** Indicates whether or not the trunk is connected to another PBX or the CO (see [page 6-17](#)).
- **Loop Start AC Impedance:** Indicates the type of line provided by the CO (see [page 6-33](#)).

Running a Hybrid Balance Test

You can run a Hybrid Balance Test on a single trunk or on all trunks, as described in the following sections.

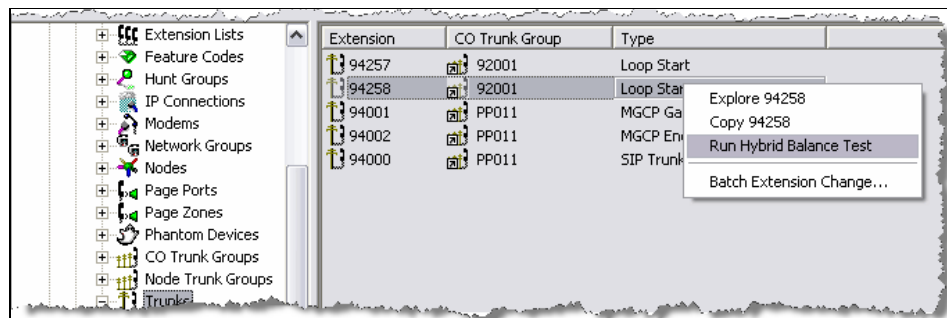
Running a Hybrid Balance Test on Single Trunk

To run the Hybrid Balance Test on a single trunk:

NOTE

Unless you use Message Print, you must exit and restart DB Programming to view Hybrid Balance Test Results (see “Viewing Hybrid Balance Test Results in Message Print” on [page 16-29](#)).

1. Select System – Devices and Feature Codes – **Trunks**. A list of trunks appears in the right pane, identified by Extension, CO Trunk Group, and Type, as shown below.

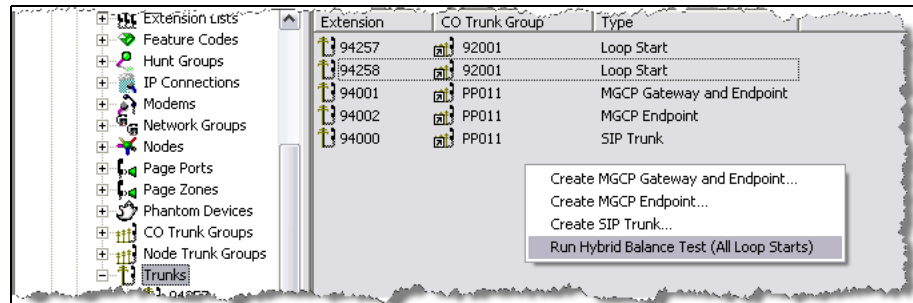


2. In the Type column, right-click the individual loop start trunk that you want to test and then click **Run Hybrid Balance Test**. While the Hybrid Balance Test runs, the selected trunk is placed in a Busy condition.
3. If the Hybrid Balance “Help” message appears, read the message, and then click **OK** to continue.

Running A Hybrid Balance Test for All Trunks

To run the Hybrid Balance Test on all trunks:

1. Select System – Devices and Feature Codes – **Trunks**, as shown below.



2. Right-click in the right pane, and then select **Run Hybrid Balance Test (All Loop Starts)**. The trunks are made busy during the test and test results for each trunk appears in Message Print. Each set of ERL values and the recommended Optimal Hybrid Balance Setting for each trunk must be processed individually.
3. If the Hybrid Balance “Help” message appears, read the message, and then click **OK** to continue.

Viewing Hybrid Balance Test Results in Message Print

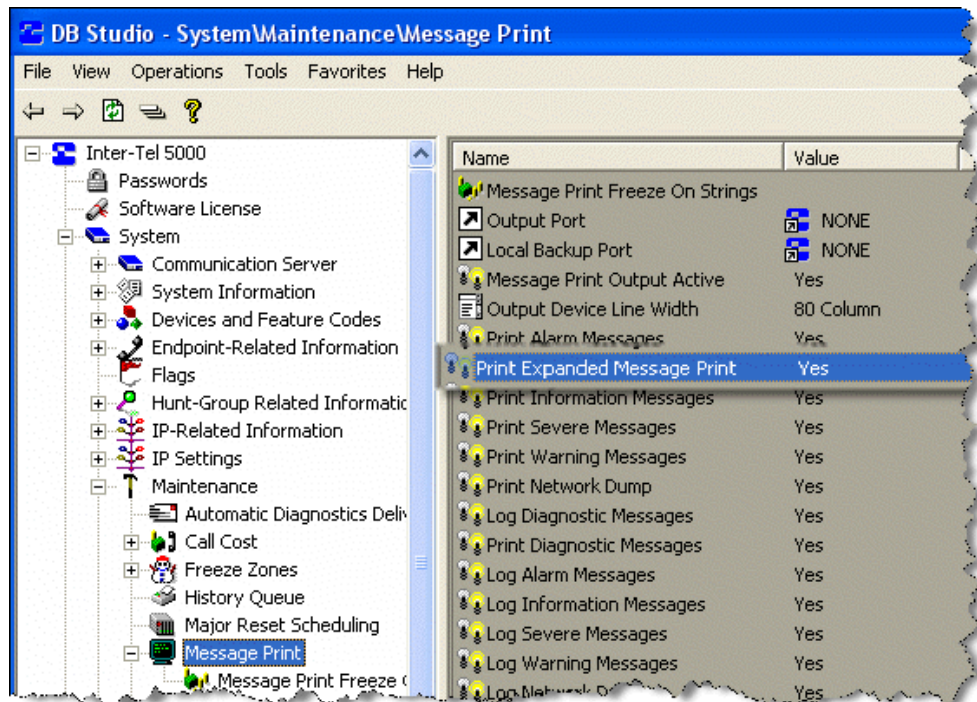
NOTICE

Online Monitor (OLM) Authorization: To perform the following procedures *only*, you may enter the OLM mode without the supervision of Mitel Technical Support personnel. As required in the procedures, you must make sure that Expanded Message Print is enabled. Any further or other programming in OLM mode is strictly prohibited without specific guidance from Mitel Technical Support personnel. Your cooperation is appreciated.

You can use Message Print to view real-time Hybrid Balance Test results. You can use the results to confirm that the test has run or to manually change the Hybrid Balance Test line setting.

To set up Expanded Message Print capability:

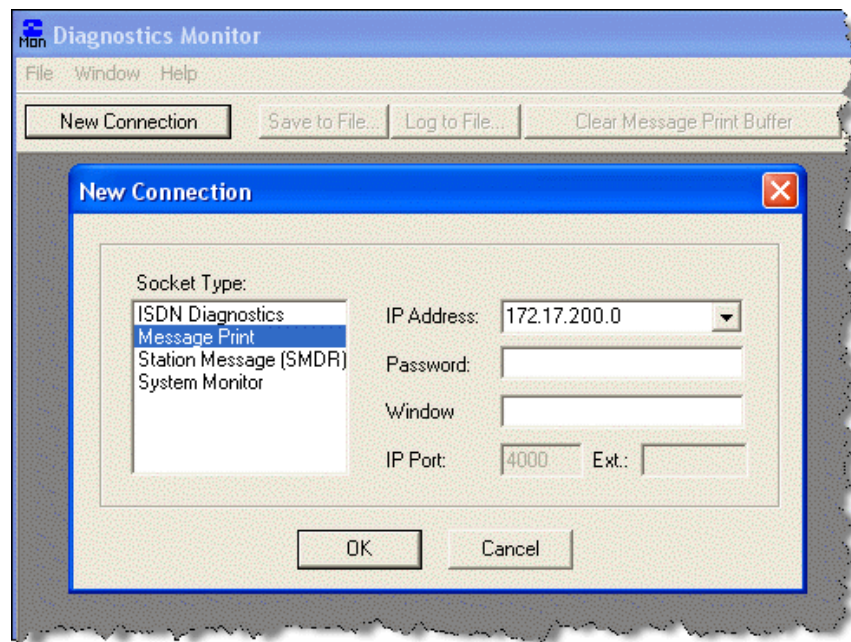
1. Before you run a Hybrid Balance Test (see [page 16-27](#)), on an idle or nearly idle system, start Session Manager.
2. From DB Studio, select **View**, and then select **On-line Monitor**. The OLM warning message appears.
3. Click **OK**. The OLM view of DB Programming appears, as indicated by a darker background in the right pane and the appearance of previously hidden folders in the left pane.
4. From the left pane, select System – Maintenance – Message Print – **Print Expanded Message Print**. Make sure the value is set to **Yes**. The default is No.



5. After verifying that the Print Expanded Message Print option is enabled, click View and then click online Monitor to clear the option. You exit OLM mode and the regular DB Programming window appears. As applicable, proceed either to the procedure to run a Hybrid Balance Test on a single trunk or on all trunks. See "Running a Hybrid Balance Test" on [page 16-27](#).

To activate the Message Print client:

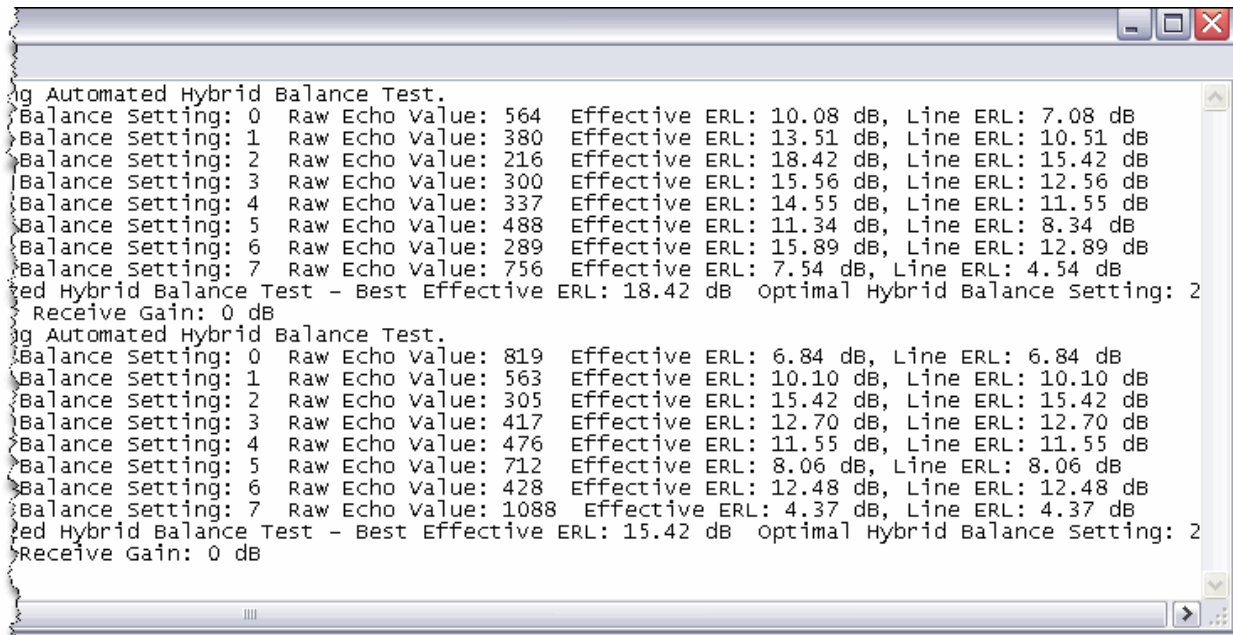
1. From your Windows desktop, select Start – Inter-Tel 5000 DB Programming – **Diagnostics Monitor**. The Diagnostics Monitor and New Connection windows appear.



2. Select **Message Print**, enter the password if one has been set in DB Programming under the Sockets folder, and click **OK**. Scrolling Message Print output from the system appears in the Diagnostics Monitor window.
3. Minimize the Diagnostics Monitor window until needed.

Viewing Hybrid Balance Results

1. After running the Hybrid Balance Test, you can view the results in Message Print and manually change the setting if desired.
2. Maximize the Diagnostics Monitor window displaying the Expanded Message Print output. For the selected trunk, a free-form Message Print output displays the Echo Return Loss (ERL) for each of the 8 possible Hybrid Balance Settings and—based on the greatest ERL value of the 8 settings—sets the Optimal Hybrid Balance Setting, as shown in the following example.



```

g Automated Hybrid Balance Test.
Balance Setting: 0 Raw Echo Value: 564 Effective ERL: 10.08 dB, Line ERL: 7.08 dB
Balance Setting: 1 Raw Echo Value: 380 Effective ERL: 13.51 dB, Line ERL: 10.51 dB
Balance Setting: 2 Raw Echo Value: 216 Effective ERL: 18.42 dB, Line ERL: 15.42 dB
Balance Setting: 3 Raw Echo Value: 300 Effective ERL: 15.56 dB, Line ERL: 12.56 dB
Balance Setting: 4 Raw Echo Value: 337 Effective ERL: 14.55 dB, Line ERL: 11.55 dB
Balance Setting: 5 Raw Echo Value: 488 Effective ERL: 11.34 dB, Line ERL: 8.34 dB
Balance Setting: 6 Raw Echo Value: 289 Effective ERL: 15.89 dB, Line ERL: 12.89 dB
Balance Setting: 7 Raw Echo Value: 756 Effective ERL: 7.54 dB, Line ERL: 4.54 dB
ed Hybrid Balance Test - Best Effective ERL: 18.42 dB Optimal Hybrid Balance Setting: 2
Receive Gain: 0 dB
g Automated Hybrid Balance Test.
Balance Setting: 0 Raw Echo Value: 819 Effective ERL: 6.84 dB, Line ERL: 6.84 dB
Balance Setting: 1 Raw Echo Value: 563 Effective ERL: 10.10 dB, Line ERL: 10.10 dB
Balance Setting: 2 Raw Echo Value: 305 Effective ERL: 15.42 dB, Line ERL: 15.42 dB
Balance Setting: 3 Raw Echo Value: 417 Effective ERL: 12.70 dB, Line ERL: 12.70 dB
Balance Setting: 4 Raw Echo Value: 476 Effective ERL: 11.55 dB, Line ERL: 11.55 dB
Balance Setting: 5 Raw Echo Value: 712 Effective ERL: 8.06 dB, Line ERL: 8.06 dB
Balance Setting: 6 Raw Echo Value: 428 Effective ERL: 12.48 dB, Line ERL: 12.48 dB
Balance Setting: 7 Raw Echo Value: 1088 Effective ERL: 4.37 dB, Line ERL: 4.37 dB
ed Hybrid Balance Test - Best Effective ERL: 15.42 dB Optimal Hybrid Balance Setting: 2
Receive Gain: 0 dB

```

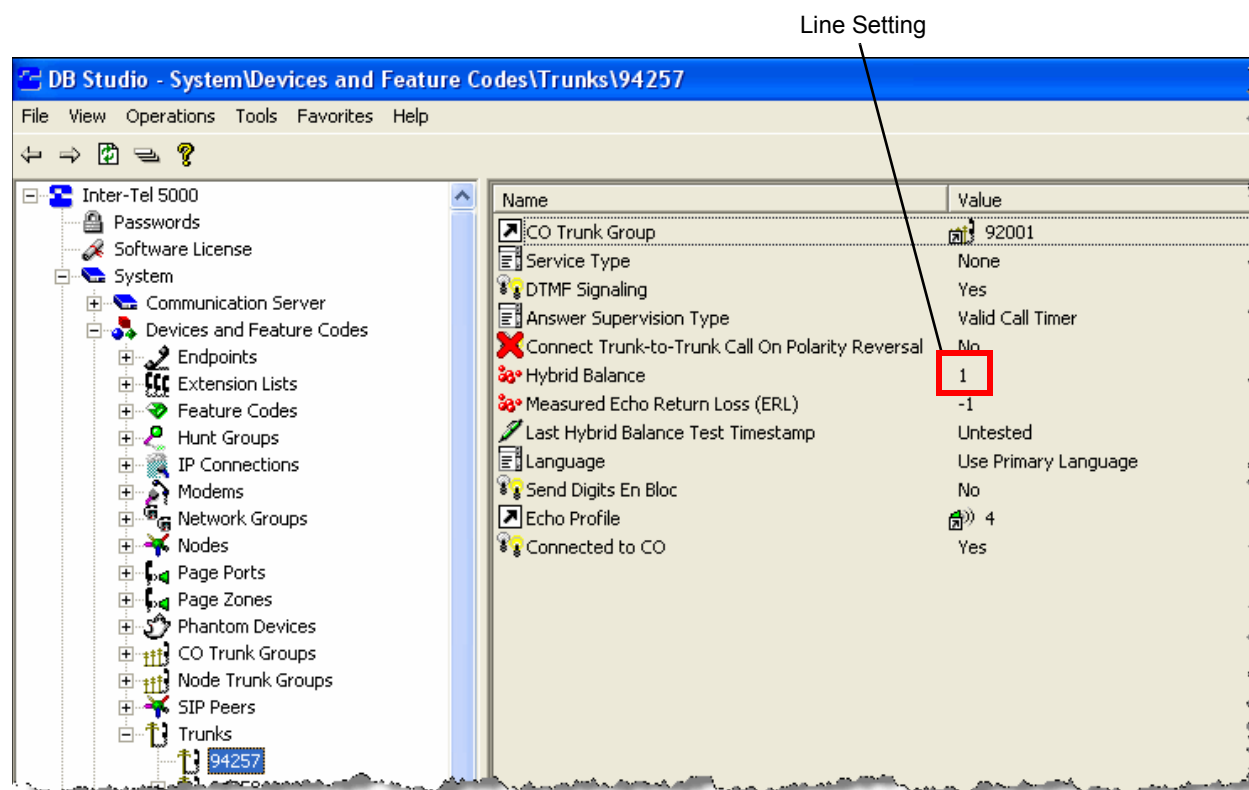
3. Record the pertinent results printed in the Message Print client.
4. *If you want to manually change the Hybrid Balance setting*, return to the DB Programming session. Select System – Devices and Feature Codes – Trunks – **<trunk extension tested>**. For the Hybrid Balance option, enter the value recommended for the Optimal Hybrid Balance Setting (see “Manually Changing the Hybrid Balance Setting” on [page 16-32](#)).
5. Repeat this procedure and compare the greatest ERL values. Acceptable tolerance between the first and second runs is ± 2 dB.
 - *If the second Hybrid Balance Test results are within tolerance*, the process is complete.
 - *If the greatest ERL in second run is more than the allowed tolerance*, run the test and set the Hybrid Balance value until you obtain consecutive ERL results within the ± 2 dB tolerance.

Manually Changing the Hybrid Balance Setting

To view or change the Hybrid Balance line setting:

Select System – Devices and Feature Codes – Trunks – **<trunk number>**. The Hybrid Balance option shows the line setting, as shown in Figure 16-4. Select the current Value and scroll to the desired option to change the line setting.

Figure 16-4. Hybrid Balance Line Setting



Alarms

Alarms are output as the result of continuous self-diagnostics run within the system and are a basic indicator that there is a problem or potential problem with the system. The severity and type of alarm determines the corrective action necessary to resolve the problem. A Major alarm indicates a problem that needs the immediate attention of a field service technician. Most Minor alarms an administrator can clear and do not require a service call. However, all alarms should be noted and monitored to determine if they occur on a regular basis, which may indicate a more severe problem. See the following section for definitions of alarm types.

In some instances, the corrective action for the condition requires contacting Mitel Technical Support personnel. The service technician is expected to be prepared and have the error information ready prior to calling Technical Support. For a complete list of the alarm messages and their corrective actions, refer to the *Message Print Diagnostics Manual*, part no. 550.8018.

Alarm Types

On the Mitel 5000 platform, alarms are grouped into the following categories:

- **Minor System alarms (000–019):** These alarms indicate a Call Processing problem that normally are corrected without calling service personnel.
- **Minor Voice Processing alarms (020–039):** These alarms indicate a voice processing problem that normally are corrected without calling service personal.

NOTE

Even when a voice processing alarm has been registered, the system may still function correctly.

- **Major System alarms (100–199):** These alarms indicate a Call Processing problem that require attention from service personnel.
- **Major Voice Processing alarms (200–224):** These alarms indicate a voice processing problem that require attention from service personnel.
- **Network alarms (225–244):** These alarms indicate either Call Processing and voice processing problems that are generated from a remote node. These alarms are handled the same as the local alarm is handled. When a network alarm occurs, the local alarm (number) equivalent is displayed on the first line of the administrator's endpoint and the node where the alarm originated is indicated on the second line. What distinguishes a network alarm from a local alarm is the node information that appears on the second line of the endpoint's display.

NOTE

The actual alarm numbers 225–244 are used internally by the system and are not displayed on the administrator's endpoint. Instead, the administrator's endpoint shows the equivalent local alarm number between 000 and 224. Nothing appears in the Message Print output of a remote node, only on the local node is the Network alarm displayed.

Network Alarms

To allow one administrator to monitor multiple nodes, the system provides both system alarms and network-wide alarms:

- **Network-Wide Alarms:** When an event occurs that generates a network-wide alarm, the alarm is broadcast to every node in the system.
- **System Alarms:** System alarms appear only on the node on which the alarm was generated.

The following two flags in DB Programming determine whether a node broadcasts and/or receives network-wide alarms:

- The **Send Network Alarms** flag determines whether a node broadcasts alarms that occur on that node to the rest of the network. See “System Flags” on [page 10-19](#).
- The **Receive Network Alarms** flag determines whether the node receives and displays alarms sent by other nodes in the network. The default state is No. See “System Flags” on [page 10-19](#).

To differentiate between network-wide and local alarms, network-wide alarms appear on administrator endpoints preceded by “NET ALARM” and local system alarms are preceded with “SYS ALARM.”

On remote nodes, network-wide alarms indicate the name of the node on which the alarm occurred. The node name is obtained from the username in Database (DB) Programming, if one is entered. Otherwise, only the node number is displayed.

Displaying Alarms

Depending on the settings in Minor System, alarm messages can be programmed to appear on the display of all administrator endpoints or on the primary attendant’s display only. This is enabled by setting the Broadcast Alarms To All Administrators flag to Yes (see “System Flags” on [page 10-19](#)). Regardless of programming, major System alarm messages appear on all affected endpoint displays.

Network-wide alarms override system alarms on an administrator’s endpoint display and on the LCD panel.

The display on an administrator’s endpoint and the LCD panel on the unit function alike when displaying network-wide and system alarms. That is, alarms are automatically shown when the display is idle, and the alarms which appear on the LCD Panel are the same as those shown on an administrator’s endpoint.

Only one alarm message is displayed on the LCD panel at any one time. Call Processing controls the generation of alarms, so if more than one alarm is generated the alarm with the higher priority is displayed or replaces an alarm that is of a lesser priority. Because alarms are queued, the next alarm based on priority, is displayed once the previous alarm is cleared.

NOTE

If the LCD panel displays ERROR, this is **not** a System alarm. See the following paragraph for more information.

When the LCD panel displays ERROR after you attempt to make a system change using the LCD application, the log file should be examined to determine the cause of the error. View the `rch_app_8.log` file by accessing the Log Files Web page. Refer to Administrative Web Session (AWS) Help for more information. The level of logging may need to be adjusted and the error recreated for the problem to show in the log files. All LCD application-related log entries have the form `<date> <time> rch_app[<log level>]: LCD APP: <log message>`.

Alarm Queue

This feature prioritizes system and network alarms based on severity and allows system administrator to view and handle critical alarms before addressing minor alarms. The administrator can then clear the individual alarm, or clear all the alarms in the queue (up to 30). When clearing alarms individually, the alarms are displayed in order of severity. The Emergency Alarm (A011) is the only priority 1 alarm. Other prioritized alarms have a 2, 3, or 4 priority, based on the severity of the alarm.

Not all alarms are prioritized. The numbered priority scheme is limited to alarms that can cause a major or minor system reset. Those alarms in the Alarm Queue that have a numbered priority are displayed before the alarms that do not have a numbered priority. (Priority 1 alarms have the highest priority.) Alarms that do not have a numbered priority are prioritized in the queue by date and time. When alarms are generated:

- The highest priority alarm is placed in the front of the queue, regardless of when lower priority alarms are generated. For example, if A114 (priority 3) and A116 (priority 4) are currently in the queue, but A119 (priority 2) is generated, A119 is placed first in the queue.
- Alarms with the same priority level are placed in the queue based on the time the alarm was generated. For example, if A010 (priority 3) is generated at 10:30 AM, and A012 (priority 3) is generated at 10:32 AM, A012 is placed in the queue after A010.
- If the queue contains 30 alarms, the oldest, lowest priority alarm is overwritten with the new alarm. For example, if the queue currently holds 30 alarms, 20 of which are priority 4, and a priority 3 alarm is generated, the oldest priority 4 alarm is overwritten.
- Repetitive alarms such as A125, are placed in the queue only once. If the alarm is regenerated, the alarm that is currently in the queue is overwritten with the new alarm data (if applicable) and time. For example, A125 is overwritten each time it is regenerated, which is every five minutes. This prevents the queue from being filled with duplicate alarms.

Table 16-4 shows which alarms have a numbered priority.

Table 16-4. Alarms and Priorities

Alarm #	Priority	Alarm #	Priority	Alarm #	Priority	Alarm #	Priority
A010	Low	A026	Low	A112	Med	A128	Low
A011	Critical	A031	Low	A114	Med	A134	High
A012	Low	A032	Low	A115	Med	A135	High
A013	Low	A100	Low	A116	Low	A137	High
A014	Low	A101	Low	A117	Low	A138	High
A015	Low	A102	Low	A118	Low	A200	Low
A016	Low	A103	Low	A119	High	A201	Low
A017	Low	A104	Med	A120	Med	A202	Low
A018	Low	A105	Low	A121	High	A203	High
A020	Low	A106	Low	A122	High	A204	High
A021	Low	A107	Low	A123	High		
A022	Low	A108	Low	A124	Med		
A023	Low	A109	Med	A125	High		
A024	Low	A110	Med	A126	Med		
A025	Low	A111	Med	A127	Med		

Clearing an Alarm

An administrator can clear a network-wide alarm on the local node only or on every node in the network using their designated endpoint.

- **Clear Network Alarm (9851):** Entering this feature code clears network-wide alarms on every node in the network, but does not affect system alarms. The Clear Network Alarm feature code may be entered on any node in the network, but the Send Network Alarms flag must be set for the administrator to clear alarms on other nodes in the network.
- **Clear System Alarm (9850):** Entering this feature code clears all local and network-wide system alarm displays on your node.

NOTE

The LCD panel only displays alarms and cannot be used to clear an alarm. Only when the LCD application receives a message from Call Processing indicating the message is removed, is the LCD panel cleared.

Responding to a Major Alarm

Since major alarms indicate that all or part of the system is inoperative, they require immediate attention from service personnel. If a system-wide failure is detected, a MAJOR ALARM message appears on all endpoint displays. If the major alarm message appears only on a group of endpoints, their associated module may have failed. If the major alarm message appears on a single endpoint, the endpoint or its cabling may be defective. When a system-wide major alarm occurs, do the following:

1. **DO NOT ATTEMPT TO REBOOT THE SYSTEM.** Open a Web session and check if all applications are running. Typically, if an application is stopped, it is restarted by Call Processing, which can be observed by viewing the LCD panel messages. Check Message Print and save the output to a log file, if necessary.
2. If a Web session cannot be opened, check the network connection and ping the unit. Connect to the USB-B port and run online Monitor to view diagnostics.
3. Only as a last option should you reboot the system. Do not pull AC power. Reboot the system through the LCD Panel menu. If the system still does not recover from the alarm, use the troubleshooting charts beginning on [page 17-16](#) to try and identify the problem. If it is determined that the Processor Module or any other part is faulty, return it for repair and include any indicated error messages in the problem description.

NOTE

When returning a faulty part, indicate all applicable error messages on the Material Return Authorization (MRA) tag. For more information about returning faulty or damaged equipment, see [page 17-89](#).

Diagnostics Through DB Programming

This section describes the diagnostic utilities available from the Database (DB) Programming interface.

Automatic Diagnostics Delivery

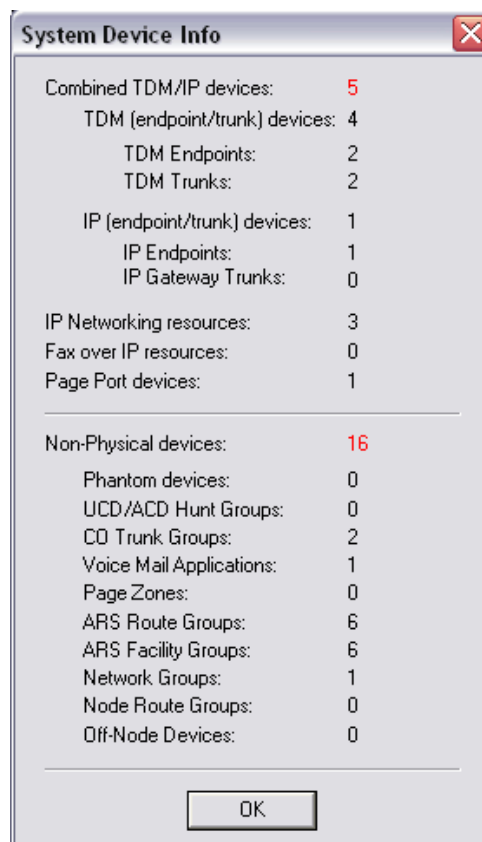
The Automatic Diagnostics Delivery (ADD) feature is a diagnostics utility available. When ADD is configured, the system automatically collects and sends diagnostic information to Mitel when it is triggered by the detection of an error that occurs within a set of defined parameters.

Because the information is sent directly to Mitel Technical Support is able to retrieve system freezes without involving a technician, providing quicker response times.

Call Processing uses port 443 for communicating with the Mitel ADD server. If this port is blocked when attempting to send freezes, an error message is displayed in Message Print. ADD is available only in online Monitor (OLM) mode. To enable ADD, you must contact Mitel Technical Support.

System Device Information

There is an option on the View menu in DB Studio (View – **System Device Info**) that opens the System Device Info dialog box. This dialog box allows you to display all of the system devices in a centralized location for the system. The TDM and IP devices are displayed at the top of the dialog box, followed by the system's non-physical devices.



Associated Devices and References

In database programming for any specific endpoint, the Associated Devices and References feature allows you to see the devices associated with an endpoint, mailbox, or hunt group. This feature also allows you to query various groups in the database to locate the associated references to the extension. To search for associated devices or references, right-click the endpoint, mailbox, or hunt group and select **Associated Devices and References**. A dialog box, similar the one shown below, appears.

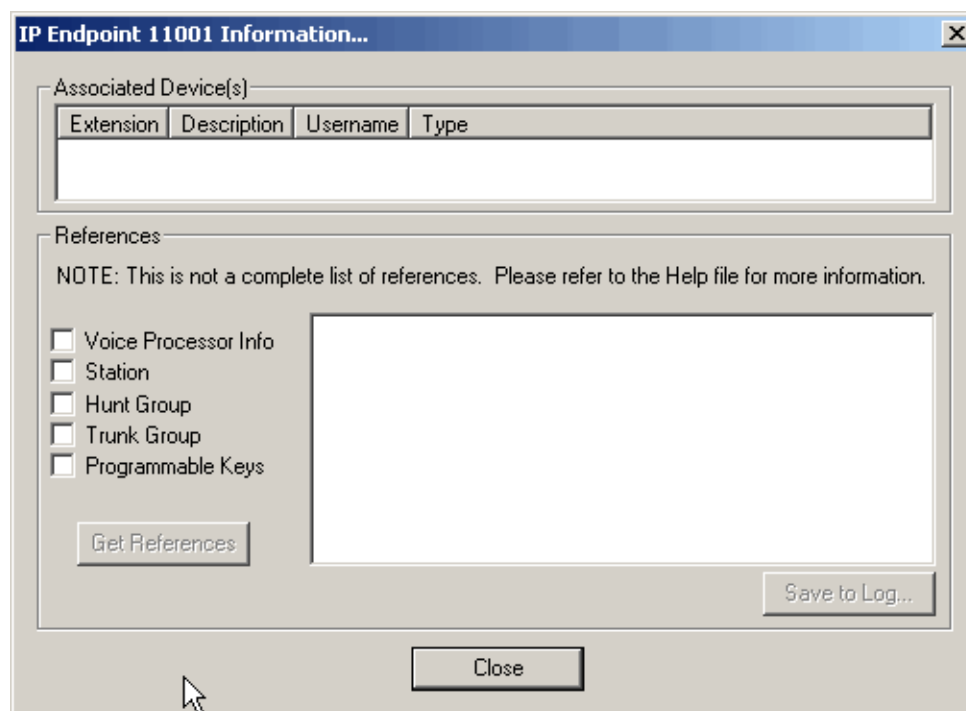


Table 16-5 shows the groups that you can query in the database for references, the type of information included in the groups, and the associated fields.

Table 16-5. Database Query Options

Group	Type of Information	Fields
Voice Processor Information	Applications AVDAP Information Call Routing Announcements Local Mailbox (Primary/Alternate Cascade Levels) Group List Members	Alternate Message Source Attendant Transfer Recall Destination Dial-0 Day Destination Type (Mailbox/Extension) Dial-0 Night Destination Type (Mailbox/Extension) System Administrator Mailbox Fax Delivery Destination Device (Extension)
Endpoint	Call Routing Entries Endpoints Emergency Day Outgoing Access List Emergency Night Outgoing Access List Forwarding Points	Ring-In (Extension) Attendant Message Center Transfer Recall Destination Device (Extension)
Hunt Group	Hunt Group Supervisors Hunt Group ACD Agent IDs Hunt Group Members Hunt Groups	Device (Extension) Announcement (Extension) Overflow (Extension) Recall (Extension)
Trunk Group	CO Trunk Group Day Answer Access List CO Trunk Group Day Multiple Ring In List CO Trunk Group Night Answer Access List CO Trunk Group Night Multiple Ring In List Trunk Group Day Outgoing Access List Trunk Group Night Outgoing Access List CO Trunk Groups	Device (Extension) Day Single Ring In (Extension) Night Single Ring In (Extension)
Programmable Keys	Programmable Keys Single Line Default Programmable Keys Keyset Default Programmable Keys Keyset KeyMap Keys	Device (Extension)

Periodic Diagnostics

Periodic Diagnostics is a feature that extends and improves the functionality and checks and reconciliations performed on various resources in the system. Periodic Diagnostics is responsible for two areas of the system: system resources and the static database.

Periodic Diagnostics checks, reconciles, and/or repairs the following system elements:

- DTMF receivers
- Caller ID receivers and transmitters
- Speakerphone resources
- Connection IDs
- Voice channels
- IP resources
- System hardware
- Static database
- Off-node device information
- Unassociated mailbox information
- Temporary extensions

System Software Performance Statistics

The Software Performance Statistics log contains software availability information. This information includes detailed performance and reset statistics.

By default, the system is configured to log software performance statistics. The information included in the log is used by Mitel Technical Support. The Internal Statistics Logging flag under System\Flags in OLM mode enables/disables this function. The default setting for this flag is **Yes**.

Database Operations

The following sections provide database operations information.

Error Information

To capture related data when a system error occurs, open the Operations menu and select **Error Information....** The following screen appears.

The screenshot shows the 'Error Information' dialog box. It has a title bar with 'Error Information' and a close button. The dialog is divided into several sections. The first section is 'History Queue' with two radio buttons: 'Freeze' (which is selected) and 'Unfreeze'. The second section is 'Select Error Logs to Save' with three checkboxes: 'Reset Log', 'Device Information', and 'Network Diagnostics', all of which are checked. Below this is a large empty text box labeled 'History Queue' with a 'Retrieve Timestamps' button underneath it. Below that is another large empty text box labeled 'Message Print Queue' with a 'Retrieve Timestamps' button underneath it. At the bottom right of the dialog are 'Save' and 'Cancel' buttons.

Select **Freeze** in the History Queue and perform the following steps:

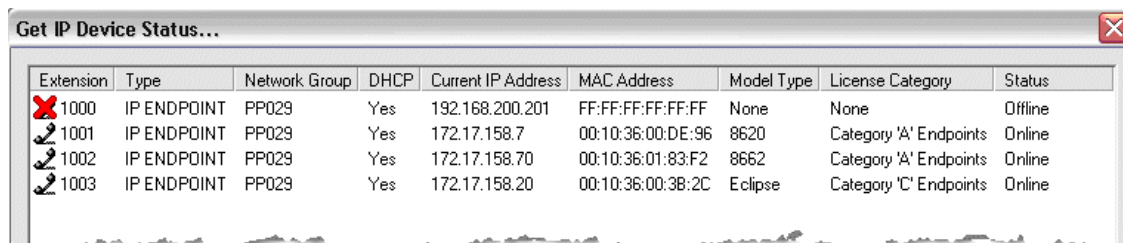
1. Select the Error Log(s) to save in the freeze.
 - **Reset Log:** What is included in this information?
 - **Device Information:** What is included in this information?
 - **Network Diagnostics:** When you select Network Diagnostics option before you complete a system freeze, the freeze includes a Network Diagnostics Log file with an extension of `.ndl`. Currently, this log file captures CP, IP Resources and IP settings, as well as insufficient bandwidth alarms. This information is included as one of several diagnostics dumps
2. Select History Queue and/or Message Print Queue and click on **Retrieve Timestamps** for the queues that you want to save.
3. Click **Save**. This prompts you for a location to save the information. When a freeze is performed the system automatically creates a variety of error logs and stores them in the location selected. By default, the number of freezes that can be saved is 30.
4. Once the freeze is completed you are prompted to unfreeze the database, select **Yes**.

IP Device Status

The IP Device Status folder resides under the Operations menu at the DB Studio window. The model column describes the model of endpoint being displayed. From the DB Studio menu bar, click Operations and then **Get Status** to retrieve IP Device status.

When an endpoint comes online, it searches for a valid license. The license category column displays which category of license the endpoint has consumed, as shown in [Figure 16-5](#).

Figure 16-5. Example of Get IP Device Status Window



The screenshot shows a window titled "Get IP Device Status..." with a table containing the following data:

Extension	Type	Network Group	DHCP	Current IP Address	MAC Address	Model Type	License Category	Status
1000	IP ENDPOINT	PP029	Yes	192.168.200.201	FF:FF:FF:FF:FF:FF	None	None	Offline
1001	IP ENDPOINT	PP029	Yes	172.17.158.7	00:10:36:00:DE:96	8620	Category 'A' Endpoints	Online
1002	IP ENDPOINT	PP029	Yes	172.17.158.70	00:10:36:01:83:F2	8662	Category 'A' Endpoints	Online
1003	IP ENDPOINT	PP029	Yes	172.17.158.20	00:10:36:00:3B:2C	Eclipse	Category 'C' Endpoints	Online

For more information, see "IP Device Status" on [page 9-4](#).

Voice Processing Diagnostics

The voice processing diagnostics that you use depends on what type of voice mail is running on the system. Refer to the *Voice Processing Diagnostics Manual*, part no. 550.8019.

With basic voice mail, the avdapmon log file can be reviewed through the Web page and if necessary, a freeze of the information can be taken using database programming. See "Error Information" on [page 16-41](#).

Running `avdapmon.exe` is useful when more information is needed to be displayed than what gets logged into the log file. To run AvdapMon from a computer, go to the **Start** menu, then select **Run**. Enter the file pathname, IP address of the system you are monitoring, and 4444 (port). The example below uses the default pathname.

```
C:\InterTel\CS5000\AvdapMon\avdapmon.exe 172.xxx.xxx.xxx 4444
```

In DB Studio under Voice Processor/Maintenance, the Expanded Diagnostics flag has been enabled (Yes), to allow the user to enter commands outlined in the diagnostics manual. When the flag is enabled, the Voice Processor logs all diagnostics output (including alarms) generated by voice processing to a file on the computer. Using that file, you can troubleshoot problems dealing with message lamps, delayed messages, remote messaging, etc. Once the diagnostics flag is enabled, it can be left on at all times without affecting performance of the system.

Once connected, the AvdapMon window opens and you are prompted to enter a password. The password is blank and cannot be changed, press **Enter**. With the Expanded Diagnostics flag enabled, perform the desired command referred to in the *Voice Processing Diagnostics Manual*.

Other Diagnostic Features

There are other diagnostics available in addition those mentioned in the previous sections that cannot be easily categorized or are a combination of diagnostic features. These include such things as diagnostic feature codes, audio diagnostics, and OLM command line.

Administrator Endpoint Support

For troubleshooting purposes, diagnostics information is available from an administrator's endpoint. You can enable and disable diagnostics functions and also dump extension or node information to Message Print from an administrator's endpoint.

NOTE Mitel recommends that you contact Technical Support for assistance with diagnostics issues.

The IP Device Resource Manager information is dumped to Message Print using an administrator endpoint. To dump the IP Device Resource Manager information, press 9900 [9100 in Europe] on the dialpad buttons to enable system diagnostics. Press 9933#47377 [9133] and then press the SPKR button to complete the dump.

Diagnostics Feature Codes

The Diagnostics Mode feature code (9900) [9100 in Europe] must be entered at the administrator endpoint to enable system diagnostic mode before the feature codes summarized in [Table 16-6](#) can be used.

Table 16-6. *Diagnostics Feature Codes*

Feature Name	Code U.S. (Europe)	Definition
Compression On/Off	9982 (9182)	Compresses call processing messages sent to DB Programming, speeding up transfers. You should not disable this feature unless instructed to do so by Mitel personnel.
Compression Statistics	9981 (9181)	Dumps various statistics related to the DB Programming compression algorithm. This feature should be used only when directed to do so by Mitel personnel.
Diagnostic – ASAI Snoop Off	9926 (9126)	Turns off the ASAI output to Message Print. ASAI is the protocol the system uses to talk to DB Programming and the AVDAP. Turning this feature on helps the Mitel Engineers debug the messaging between Call Processing and DB Programming or Call Processing and the AVDAP.
Diagnostic – ASAI Snoop On	9927 (9127)	Turns on the ASAI output to Message Print. ASAI is the protocol the system uses to talk to DB Programming and the voice processing system. Turning this feature on helps the Mitel Engineers debug the messaging between Call Processing and DB Programming or Call Processing and the AVDAP.
Diagnostic – Dump Extension	9933 (9133)	Allows the field technician to dump a device or structure when debugging a problem. The system dumps the internal data structures for that extension to Message Print. If you press the pound button (#) you are prompted for a command. The command allows you to enter an alphanumeric string of the structure to dump.

Table 16-6. Diagnostics Feature Codes (Continued)

Feature Name	Code U.S. (Europe)	Definition
Diagnostic – Dump Node Information	9936 (9136)	<p>Pressing the Dump Node Information feature code dumps specified node information to Message Print for diagnostic purpose. When the system prompts for a node number, enter the applicable node number or zero (0) for all nodes within a network. If the node does not exist, an error message saying INVALID NODE NUMBER appears and prompts you for a node number again.</p> <p>After entering a node number, the system displays a confirmation message on the endpoint display. This helps you analyze which nodes are up and which nodes are down (the word 'down' does not mean that the node is completely down, it simply means the node is unreachable). For Example:</p> <p>If all nodes are up, the display shows ALL NODES ARE UP X. The 'X' represents the total number of the nodes.</p> <p>If node 3 and 5 of a 5-node network are down, the display shows # NODES DOWN 2 3 5.</p>
Diagnostic – Heap Dump	9943 (9143)	This is used by Mitel software developers and cannot be used in Beta or Production software.
Diagnostic – Heap Statistics	9947 (9147)	This feature code outputs miscellaneous heap information to Message Print as well as putting up a message on the endpoint that indicates the percentage of available dynamic heap memory. This feature code is useful in determining if the system is losing heap memory and how quickly the system may be losing it.
Diagnostic – ISDN View	9948 (9148)	<p>This feature code is toggles through the three different ISDN view output modes.</p> <p>Entering the feature code the first time puts the ISDN view feature into headers only mode. In this mode the system outputs all ISDN messages to Message Print in header format (i.e., it does not contain any ISDN information elements).</p> <p>Entering the feature code the second time puts the ISDN view feature into full mode. In this mode the system outputs all ISDN message to Message Print in full format (i.e., each ISDN information element).</p> <p>Entering the feature code one more time turns this feature off.</p>
Diagnostic – Major Reset	9962 (9162)	This is used by Mitel software developers and cannot be used in Beta or Production software.
Diagnostic – Mark As Leaks	9945 (9145)	This is used by Mitel software developers and cannot be used in Beta or Production software.
Diagnostic - Mark As Quiescent	9946 (9146)	This is used by Mitel software developers and cannot be used in Beta or Production software.
Diagnostic – Minor Reset	9964 (9164)	This is used by Mitel software developers and cannot be used in Beta or Production software.
Diagnostic – Network Freeze Zone System Histories	9939 (9139)	The system fault history for any freeze zone in the network can be halted (frozen) or re-enabled using these feature codes when diagnostics mode is enabled. The fault history can then be extracted from each zone and used by service personnel when troubleshooting the system.
Diagnostic – Network Unfreeze Zone System Histories	9989 (9189)	

Table 16-6. *Diagnostics Feature Codes (Continued)*

Feature Name	Code U.S. (Europe)	Definition
Diagnostic – Network Groups	9963 (9163)	Allows an administrator to verify that the Network Groups on the local node are programmed properly. When 9963 is entered at an administrator's endpoint, the telephone system initiates pings from each Mitel IP device on the local node and determines if the other devices respond to the ping. If a device does not respond to the ping or if a firewall is detected, the system issues a Message Print message.
Diagnostic – Print Auxdata	9972 (9172)	(Not Programmable) Sends a report to a designated printer or file that shows system reset history information to be used for troubleshooting purposes.
Diagnostic – Print Message Log	9975 (9175)	(Not Programmable) Sends a report to a designated printer or file that lists system error messages to be used for troubleshooting purposes.
Diagnostic – Print Network Log	9976 (9176)	This feature code prints the network log to Message Print. This feature is useful in determining the system of a networked system.
Diagnostic – Query Node Traffic	9978 (9178)	Using this feature code you can query the status of various devices on the system based on the status of the traffic flags in DB Programming. The output is sent to Message Print.
Diagnostic – Show Version	9928 (9128)	To check the call processing software version at an administrator's endpoint, you can enable diagnostics mode, then enter this feature code to view the version and date of the call processing software. However, feature code 9928 displays the firmware version of the endpoint if it is in SIP mode.
Diagnostic – SIP View	9987 (9187)	Allows the user to change the system wide SIP output value. Options include No Output, Headers and Full Output.
Diagnostic – Spare 1–3	9910–9912 (9110–9112)	This is used by Mitel software developers and cannot be used in Beta or Production software.
Diagnostic – System History	9974 (9174)	This is used by Mitel software developers and cannot be used in Beta or Production software.
Diagnostic – View Displays	9983 (9183)	This is used by Mitel software developers and cannot be used in Beta or Production software.
Program Database	9932 (9132)	Can be used for programming endpoint, system, and trunk parameters.
Seize Device	9973 (9173)	Used during troubleshooting to seize a specific trunk or endpoint by indicating the board number, port number, and device number.
System History – Freeze System History – Unfreeze	9993 (9193) 9998 (9198)	The system fault history can be frozen or unfrozen using these feature codes when diagnostics mode is enabled. Fault history is used by service personnel when troubleshooting the system.

Online Monitor Command Line

The Online Monitor (OLM) provides a diagnostics view of the operating system for troubleshooting purposes. The OLM system diagnostic commands described in this section provide additional details about the system and help troubleshoot errors.

Use only the commands provided in this chapter unless otherwise directed to by Mitel Technical Support personnel.

The OLM is accessible from either a remote location through an Secure Shell (SSH) interface using a third-party application or locally through the USB-B port on the front of the chassis. The USB-B port provides access to the system when the IP network is down. The OLM shell requires appropriate drivers to be loaded before the feature can be accessed.

Access to the OLM shell requires a username and password. The default login for the username is **it5k** and the default password is **itpassw**. The “OLM>” should appear on the screen indicating that it is the OLM shell. Mitel recommends that you change this password at the earliest convenience.

The OLM shell provides access to commands in the `olm_bin` directory. Only the commands in the `olm_bin` directory are available to the OLM shell. Using the `help` command with no arguments provides a list of the available OLM commands along with a brief description. From the OLM shell, this help is accessible by typing the command followed by “-h.” A question mark can also be substituted for “-h” for built-in and system diagnostics commands. If the command entered fails indicating an invalid option error, the option is not supported.

There are two commands “Exit” and “.” built-in to the shell which are not executed from the `olm_bin` directory. Using either of these commands exits out of the OLM shell.

System Diagnostics Commands

System diagnostic commands are executed from the `olm_bin` directory and provide diagnostic information on the system. Commands denoted with an “*” allow additional arguments to be passed to them.

- cls** — Clear the terminal screen
- free*** — Display the amount of free and used system memory (free)
- help (or ?)** — Display the available commands or help on a specific command
- ifshow** — Display the status of the currently active interfaces (ifconfig)
- ls*** — List directory contents (ls | more)
- netstat*** — Display information about networking subsystem (netstat | more)
- ping*** — Send echo request to network hosts (ping)
- ps*** — Report a process status (ps)
- route*** — Display the kernel routing tables (netstat -rn)
- top*** — Display the top CPU processes (top)
- vmstat*** — Display virtual memory statistics (vmstat)

Application Diagnostics Commands

Application diagnostic commands are executed from the `olm_bin` directory and provide diagnostic information on the individual application. These commands can be run on any of the following applications: T1, IP Resource Application (IPRA), Loop Start, Single Line and RCH. The application diagnostic commands allow additional arguments to be passed to them as listed in the table.

applogctrl — Enable/Disable Application log directories, change log file directories, and clear log files. The log files are stored in RAMDisk (`/var/log/intl/`) or Flash (`/usr/local/intl/logs/`). The following arguments can be used in conjunction with the application command.

-n <AppName> Name of the application, select from the following: `t1_app`, `ls_app`, `iprc_app`, `sl_app`, `rch_app`

-s <Bay Number> Specify the bay number the application is running on.

-e Enables logging.

-d Disables logging.

-l <dir> Changes the log file directory.

-c Clears the log.

appstatus — Display the basic execution status of an application

-n <AppName> Name of the application, select from the following: `t1_app`, `ls_app`, `iprc_app`, `sl_app`, `rch_app`

-s <Bay Number> Specify the bay number the application is running on.

-e Provides extended information

The following application command is applicable only to the IP Resource application.

iprc_diag_stats — Display IP Resource statistics information - device connection information, send and receive session information etc.

-a <Bay Number> Bay Number for IP Resource is usually 7 and 9 for expansion module.

-V Displays IP Resource version information.

-T <PortID> Displays endpoint information for the particular port ID. If PortID is ALL it displays information of all the endpoints in the system.

-t <PortID> Displays detail endpoint information for the particular PortID.

-S <SessionID> Displays Send Session Information for the Session ID provided. ALL provides details for all the send sessions on the IP Resource

-s <SessionID> Displays Audio Session Information for the Session ID provided

-R <SessionID> Displays Rx Session Information for the Session ID provided. ALL provided information for all the Rx session on the IP Resource.

-r <SessionID> Displays In-Time packet graph for the Session ID provided.

The following application command is applicable only to the Modem application.

modem_diag_stats — Display Modem statistics information in terms of transmit and receive speeds, echo level, Signal Quality, Signal to Noise Ratio information etc.

-a <Bay Number> Bay Number for modems is usually 8.

LCD Panel Diagnostic Options

The liquid crystal display (LCD) panel displays system status and command messages on two lines of 14 characters each. The LCD displays system status information to determine the operating condition of the system, and it displays menus and options for programming, changing, or resetting the system.

For more information about LCD functions, refer to the "Installation" chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

Resource Manager CPH Diagnostics Flag

The Log Resource Manager Output flag exists in the System\Maintenance\History Queue folder to enable or disable the resource manager Call Processing History (CPH) diagnostics feature. CPH is a collection of inputs and outputs used to diagnose problems that occur on the system. This flag can only be accessed in online Monitor (OLM) mode. By default, this flag is set to **No**.

NOTICE

Do *not* use OLM mode unless you are instructed to do so by support personnel.

Call Processing History (CPH) Freeze File Compression

When a system freeze is performed, a snapshot of the memory-mapped files is taken and copied into a freeze directory. The directory contains a new Freeze_00 file which is always the most current. The CPH Freeze File Compression feature zips the freeze files into a compressed file that includes the node number and the start and end freeze dates and times in the zip file name. For example, `n12_06-02-04_123010_06-02-04_freeze.zip` represents a node 12 system freeze that occurred on June 2nd, 2004, between 12:30 PM and 10 seconds and 4:00 PM and 23 seconds. `160023_freeze.zip`.

The time stamp includes hours, minutes, and seconds to handle situations if the Call Processor (CP) on the PM-1 should happen to freeze multiple times in the same minute. The zipped freeze file resides in the C:\ICP\FREEZE directory on the CPS. When a freeze occurs, the compression utility appears in a console window. After one to two seconds, the console window will minimize automatically. High system use may increase the delay before the system minimizes the window. When a freeze occurs, the compression utility appears in a console window. After one to two seconds, the console window minimizes automatically. High system use may increase the delay before the system minimizes the window. When Automatic Diagnostics Delivery (ADD) is enabled, the system sends the single zipped file.

History Queues/Log Files – Clearing

System software allows the history queue to be cleared to baseline a site for monitoring purposes. To clear a history queue and log files, move/delete the Memory Map Files (`.mmf`), but do not delete the static `_mmf` file. To clear the history queues and log files, use the Clear Error Information option in DB Studio while in OLM mode. When this operation is performed, the system generates a new Message Print “M6099 Corrupted Queue was Cleared,” which confirms when the queue or log file has been cleared.

Traceroute

The Traceroute application tests the communication path to any IP address in the network. For example, a technician could perform a traceroute from the IPRA to an IP endpoint to confirm the IPRA can communicate with it. The technician could also run a traceroute to any IP device in the network (a PC, some public IP address, and so on). The traceroute command lists the IP addresses of each router that exist along the path from the local host to the given IP address of a destination host on the network.

The method for acquiring this information relies on ICMP (Internet Control Message Protocol) Echo and Time Exceeded messages which some routers are programmed to not send or ignore. The traceroute will list a “no reply” when it encounters a router that ignores the request. A traceroute command is available from the IPRA with OLM consoles.

To run the traceroute command: Select the “Debug Session” option from a telnet console. At the prompt, invoke the command by entering “tracert” followed by an IP address in numeric form at the prompt.

External Diagnostic Resources

This section describes the general functionality of the System Manager and the Raw Commands Web page as diagnostic tools for the Mitel 5000 platform.

Administrative Web Session

NOTES

Administrative Web Session Pages support Microsoft® Internet Explorer® (IE) through version 7.

Administrative Web Session (AWS) is Mitel 5000 Web interface that provides a comprehensive view of the communication server to gather diagnostic information about applications that are running on the system. AWS is initiated from any computer that has Internet access, allowing you to view and analyze a system without having to be on-site.

To access AWS:

1. In the address bar of a Web browser, type the IP address of the system that you want to access.
2. After communication is established with the system, type the username and password. By default, "it5k" is the username (which cannot be changed), and "itpassw" is the password.

For more information about AWS, refer to AWS Help or the *Mitel 5000 Reference Manual*, part number 580.8007.

System Manager

System Manager is a server-based application that centralizes management functions for the system and various peripheral components. For the Mitel 5000 platform, System Manager uses a Web interface. With appropriate licensing, System Manager allows you to view system information such as Message Print, IP Resources, and trunk diagnostics.

System Manager can be configured to perform a variety of functions, one of which is the ability to freeze log files. For more information about the system interface, refer to the *System Manager Installation and Maintenance Manual*, part no. 835.2743.

Raw Commands

System Manager users have the option to view IP resource oversubscription statistics for a Mitel CS-5x00 Agent. The various types of resource statistics are displayed when commands are entered on the Raw Commands Web page. The following commands apply to the Mitel 5000 platforms:

- IP DRM Resource Diagnostics
- IP Resource Diagnostics
- VoIP DSP Manager
- PS/Base Server Socket Statistics

Troubleshooting

Introduction	17-3
Troubleshooting Methodology	17-3
Troubleshooting Processes	17-5
Preliminary Activities	17-5
System Reset Analysis	17-6
Troubleshooting Guidelines	17-6
Hot-Swapping an Expansion Module	17-7
Call Flow	17-8
Network Diagram	17-9
Troubleshooting Charts	17-10
99 Nodes Support	17-11
Administrative Web Session	17-12
Basic Voice Mail	17-12
Caller ID Forwarding	17-13
Caller ID Propagation	17-14
CO [Local Exchange] Trunks	17-16
Database Change Log	17-20
Digital Endpoint Interface	17-20
Endpoints	17-21
Expansion Modules	17-27
File-Based MOH	17-28
Four-Port Single Line Module	17-29
Import Endpoints from CSV Files	17-30
IP Resource Application (IPRA)	17-32
IP Devices	17-32
IP Device Audio	17-36
IP Device Connection	17-37
IP Device Echo	17-39
IP Device VLAN Tagging	17-41
IP Networking	17-42
Licensing Issues	17-46
Loop Loss Measurement	17-46
Mini-DSS Unit	17-47
Multi-Protocol Endpoints	17-48
Network Node	17-52
Oversubscription/IP Resource-Sharing	17-53
Persistent Music-On-Hold Selection	17-54
Phantom Devices	17-55

Processor Module (PM-1)	17-57
Processing Server (PS-1)	17-58
Retry ARS Call If Call Rejected	17-59
Scheduled Backups – Warnings and Error/Failure Reasons	17-59
Information	17-59
Warning	17-59
Error/Failure	17-61
Scheduled Backups – Error Messages	17-66
Scheduled Backups – General Troubleshooting Tips	17-69
Single Line Endpoints	17-71
System Health Report	17-74
System Features	17-74
System-Level Issues	17-78
T1/E1/PRI Modules	17-81
Upgrade Process	17-83
UPS Monitoring	17-84
Voice Processing	17-84
VoIP Echo Canceller Troubleshooting	17-88
VPIM Networking	17-89
Customer Support	17-90
Technical Support	17-90
Emergency Assistance	17-90
Defective Equipment Return Policy	17-90

Introduction

Use the standardized troubleshooting methodology described in this section to identify and correct problems with the Mitel 5000 system. The troubleshooting process described shows where diagnostic utilities may be used when troubleshooting to efficiently isolate and resolve an identified problem. By following the process, you are more likely to gather necessary information and avoid having to repeat the effort.

The charts starting on [page 17-10](#) are included as supplemental information to identify a potential problem for a place to start troubleshooting. If you begin your analysis with the troubleshooting charts, be sure to continue working through the troubleshooting process to gather information which may otherwise be lost. By not continuing through the process, the solution you implemented may have only been a symptom of the actual problem, which could compound the time it takes to isolate and correct the real problem.

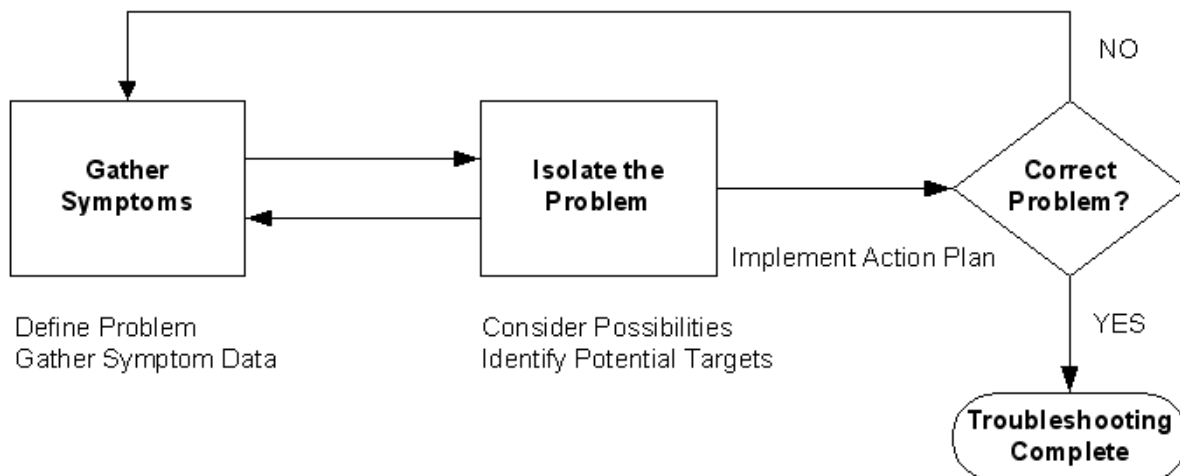
Troubleshooting Methodology

The processes in this section are not detailed step-by-step instructions but practical guidelines to direct you in your approach to resolving the problem. The purpose of the troubleshooting methodology is to:

- Provide a systematic approach to problem solving until the condition is corrected by the service technician or the need to involve Mitel Technical Support is identified.
- Help in the collection of data and documentation of troubleshooting steps to reduce system downtime.
- Promote better communication of the problem to technical support personnel, by providing the necessary information and supplemental data that results in a quicker resolution.

The following diagram illustrates a simplified view of the troubleshooting process.

Figure 17-1. *Troubleshooting Process Flow Diagram*



1. **Gather Symptoms:** Describe the problem, describe the environment (system, versions, configuration, etc.), list symptoms, list possible causes, investigate the problem
 - Define the problem – State exactly what the problem is and be specific.
 - Gather symptom data – Collect as much information as possible within the given amount of time to support or eliminate from the list of possible causes. Interview users, use diagnostic utilities, etc.
2. **Isolate the Problem:** Using the information from step 1, identify causes (targets) then try to eliminate as many as possible. Check if the information collected points to a specific group of possible causes then try to rank them by probability.
 - Consider possibilities
 - Identify potential targets

If the problem is isolated then start on a plan to correct it. Otherwise, go back and gather more data.
3. **Correct the Problem:** Begin with the most likely cause first. Start with the most simple cause when there are multiple causes. Perform steps that change 1 variable at a time, this helps identify the effect of an action on the problem. Before executing a solution make sure you have a plan to get back to where you started. Don't make the existing problem any more complex than when you started.
4. **Implement action plan:** When the corrective action implemented resolves the problem and does not cause other problem, then troubleshooting is complete. Otherwise, if the corrective action does not resolve the problem or effectively reduce the symptoms, then go back and gather more data. If the corrective action did not resolve the problem or had no (noticeable) effect, it may be a good decision to back out that change before implementing another change.

The fundamentals of the methodology do not change, but how the results are accomplished may be achieved using any one of these three approaches: bottom-up, top-down, or divide-and-conquer. Whatever approach is selected, the goal remains the same: to correct the problem the most efficient way in the least amount of time. When deciding on the approach to use, consider that not every problem will cause the system to go down, but when it happens, one approach may be better suited based on problem data collected, scope of the problem, and level of your experience. Always consider what the normal behavior of the system is like when you begin to identify and trace a potential problem.

- **Bottom-up:** This approach starts with the physical aspects of the system, working through the connectivity up to the application. If the data collected and the symptoms appear to be physical, then this would be the approach to consider. Keep in mind that this approach could require checking every physical device. A challenge to this approach is which device do you check first?
- **Top-down:** This approach starts with the application and looks at the application specific components. If the data collected and the symptoms appear to be software related, then this would be the approach to consider. This approach requires checking every application on the network end-device. A challenge to this approach is which application do you check first?
- **Divide-and-Conquer:** This approach starts somewhere in the middle and works going in both directions. If the data collected does not appear to favor either of the other approaches, then this would be the approach to consider. Use the data that you collected on the symptom and then base your decision on your level of experience.

Troubleshooting Processes

The following troubleshooting process illustrates how the methodology applies to problem solving system discrepancies. This section provides troubleshooting components to consider using when a problem is identified.

Preliminary Activities

Before you begin troubleshooting:

1. Always have the USB console connection active to see if there are any problems.
2. If there is a possibility of disrupting system call processing, run a courtesy check to see if there are any active calls via Diagnostics Monitor using the Call Diagnostics dump or via the LCD panel.
3. Establish a Message Print socket when possible and monitor output of the system.
4. Create a call flow diagram which could include a high-level view on how the system processes calls.
5. Check the resources that are available and use them to help resolve the problem: (Resource information may be minimal for initial release of product.)
 - Installation and Maintenance Manual
 - Knowledge Base
 - Reseller Discussion Forum
 - Tech Notes
6. Create a checklist that will help identify where to start and how to progress through a problem situation.
7. Verify correct programming using Application Programming Checklists
8. Verify correct installation using Installation chapter from the manual
9. Use the diagnostics utilities available as described in previous sections of this chapter.
10. Review the acceptance criteria and the information that you need prior to calling Technical Support.
11. Contact Technical Support.

System Reset Analysis

When a system reset occurs:

1. Perform a History Freeze.
2. Open Web session and view CP log files.
3. Diagnose the problem.
 - Check alarm display.
 - Check reset log.
 - Check .dmp file if you know what to look for.
 - Was it really a system reset, or was it just a halt?
 - Is the problem system-wide, cabinet-wide, internal/external?
4. Take corrective action if possible.
5. If you can't correct it, turn on diagnostics, freeze zones, freeze strings.
6. If the preceding steps do not help, call Mitel Technical Support.
 - Use ADD (needs IP connection).
 - Use Resource Manager in Message Print.
 - Use Start Mon/Diagnostics Monitor.

NOTE

If you have a slowdown of the system, do **not** turn on flags because it will cause the system run even slower.

Troubleshooting Guidelines

If the problem involves one of the following system features, see the applicable troubleshooting table in this chapter.

- Repeated occurrence of all calls in progress dropping.
- All endpoints are inoperative.
- Database restore aborts before finishing.
- DISA is inoperative.
- Unable to interface with a computer call-up device.
- Remote maintenance modem cannot communicate properly with the system.
- No Music-On-Hold background music.
- RFI/EMI present over conversations.
- Faulty DID numbers displayed at attendant endpoints.
- Out of memory error while loading database programming software on the programming computer.
- DID numbers routed before all digits are dialed.

NOTICE

Network security is the responsibility of the customer's network administrator. Mitel is not responsible for network problems due to security violations involving the IP address of the Mitel IP devices. This includes, but is not limited to, toll fraud and interrupted network service.

Hot-Swapping an Expansion Module

The Mitel 5000 platform allows a technician to replace modules without taking the system out of service. The system constantly detects which type of module occupies the bays, and the hot swap capability is available without additional system configuration.

NOTICE

Data corruption hazard. Shut down the system before removing the Processor Module (PM-1) to avoid corruption of the file system on the compact flash-type memory card. For detailed instructions, refer to the Installation chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

When a technician inserts a new module into one of the three expansion bays and seats it correctly, the module latch lever goes to the up position. The system detects the event and applies power to the module, turns off the green LED labeled REMOVE, and invokes the appropriate software. The green LED labeled ONLINE turns on.

To remove a module, the technician loosens the module fastener, then presses the module release lever down. When the green LED labeled REMOVE turns on, the module is ready to be removed. After removing the module, the technician inserts the replacement module. When the module is seated and the latch snaps into the up position, the green LED labeled REMOVE turns off and the necessary software automatically starts. The green LED labeled ONLINE turns on, and the module fastener can then be screwed in.

For detailed instructions for correctly installing or replacing the different types of modules, refer to the Installation chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

Hot swap failure is indicated when the green LED does not change from its initial state when a module is inserted or removed with the system powered-up. The problem may be caused by faulty hardware or corrupted software. Select from the following two conditions, then apply the action and see if the problem still exists.

1. When the module latch is in the down position, the green LED labeled REMOVE does not come on.

Action: Shut down the system. Remove the module and restart the system. For more information, refer to the Installation chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

2. With the module inserted and its latch in the up position, the green LED labeled ONLINE does not turn off.

Action: Shut down the system. Insert the module and restart the system. For more information, refer to the Installation chapter in the *Mitel 5000 Installation and Maintenance Manual*, part number 580.8000.

Call Flow

When troubleshooting a possible call processing problem, a complete and accurate description of the call flow is needed to help determine a possible cause. You must document the flow starting from when the call comes into the system, detailing each step up through where the problem occurred. The following call flow examples describe the same problem. Both examples are accurate but only one of them is acceptable, if you want help from technical support.

Example 1: The call rang into the auto attendant and then was answered by the CEO's secretary.

Example 2: The call rang in on a PRI trunk in Bay 2 on node 1 at 7:42am. The trunk group is a single ring into call routing table 3. The 800-xxx-xxxx number was then routed to a STAR application on the third-party voice processing application on node 2. The STAR application (2516) transferred the call a CRA (2530) which times out to 'Transfer to extension 2044' which is a hunt group on node 4. The CEO's secretary answered the call at extension 1250 which is on node 2. This is when (xyz) problem occurred.

Additional conditions to consider when determining the call flow appear in [Table 17-1](#).

Table 17-1. *Call Flow Troubleshooting Considerations*

Step	Name	Example
1	Phone Number	480-961-9000
2	Trunk Group/Type of Trunk	92001/Loop Start
3	First Ring At	CRA App
4	Extension	What to do: <ul style="list-style-type: none">• Dial• Timeout
5	End result of call	Extension Hunt Group <ul style="list-style-type: none">• Recall• Announcement• Overflow

Information similar to that given in the above example is basic information needed to start with for troubleshooting and it is a requirement if you are calling in to Technical Support. Knowing this detailed information can often point in the direction of the problem, but it will always be useful to narrow the possibilities. Then, if you are unable to resolve the problem and need to call Technical Support, you will already have that information to give the Product Specialist. In addition, when a system or network freeze of the problem is required, an accurate call flow is needed by the product specialist to find and follow the call in the data file.

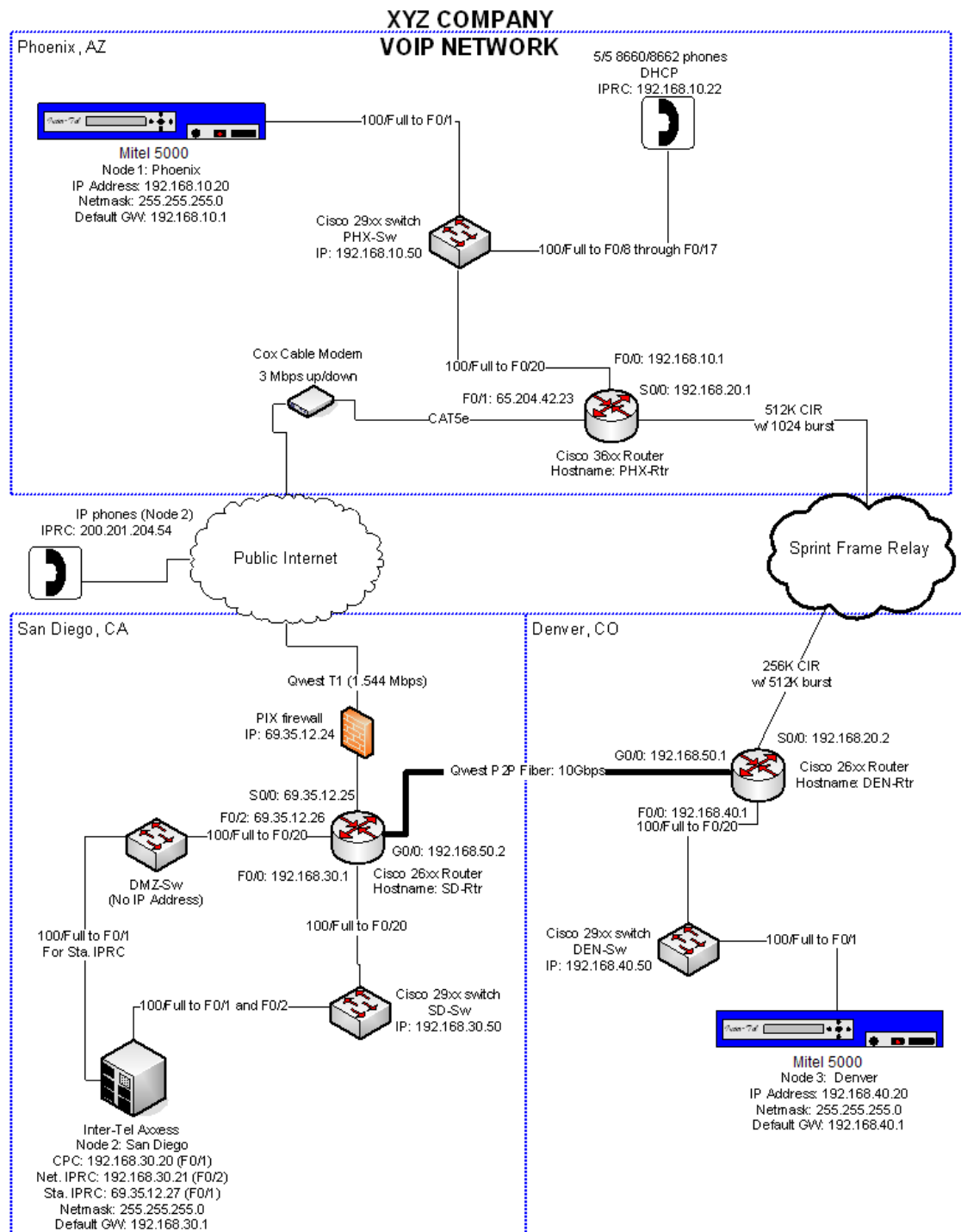
NOTE

A call flow is information that the service technician is required to have ready when they call in for technical support.

Network Diagram

In addition to a call flow, having a detailed network diagram to use is essential when troubleshooting potential IP or network problems. A network diagram is typically required when the system is originally installed, so a network administrator should be able to provide this information. Make sure the network diagram you are given is current and shows the information you need to help define the problem. An example of a detailed network diagram is illustrated in Figure 17-2.

Figure 17-2. Network Diagram Example



Troubleshooting Charts

The following troubleshooting charts have been designed so you can look up a particular problem in the appropriate chart and perform the suggested corrective actions. Troubleshooting procedures are summarized in the following sections:

- “99 Nodes Support” on [page 17-11](#)
- “Administrative Web Session” on [page 17-12](#)
- “Basic Voice Mail” on [page 17-12](#)
- “Caller ID Forwarding” on [page 17-13](#)
- “Caller ID Propagation” on [page 17-14](#)
- “CO [Local Exchange] Trunks” on [page 17-16](#)
- “Database Change Log” on [page 17-20](#)
- “Digital Endpoint Interface” on [page 17-20](#)
- “Expansion Modules” on [page 17-27](#)
- “Endpoints” on [page 17-21](#)
- “File-Based MOH” on [page 17-28](#)
- “Four-Port Single Line Module” on [page 17-29](#)
- “Import Endpoints from CSV Files” on [page 17-30](#)
- “IP Resource Application (IPRA)” on [page 17-32](#)
- “IP Devices” on [page 17-32](#)
- “IP Device Audio” on [page 17-35](#)
- “IP Device Connection” on [page 17-36](#)
- “IP Device Echo” on [page 17-38](#)
- “IP Device VLAN Tagging” on [page 17-40](#)
- “IP Networking” on [page 17-41](#)
- “Licensing Issues” on [page 17-45](#)
- “Loop Loss Measurement” on [page 17-45](#)
- “Mini-DSS Unit” on [page 17-46](#)
- “Multi-Protocol Endpoints” on [page 17-47](#)
- “Network Node” on [page 17-51](#)
- “Oversubscription/IP Resource-Sharing” on [page 17-52](#)
- “Persistent Music-On-Hold Selection” on [page 17-53](#)
- “Phantom Devices” on [page 17-54](#)
- “Processing Server (PS-1)” on [page 17-57](#)
- “Processor Module (PM-1)” on [page 17-56](#)
- “Retry ARS Call If Call Rejected” on [page 17-58](#)
- “Scheduled Backups – Warnings and Error/Failure Reasons” on [page 17-58](#)
- “Single Line Endpoints” on [page 17-70](#)
- “System Features” on [page 17-73](#)
- “System Health Report” on [page 17-73](#)
- “System-Level Issues” on [page 17-77](#)
- “T1/E1/PRI Modules” on [page 17-80](#)
- “Upgrade Process” on [page 17-82](#)
- “UPS Monitoring” on [page 17-83](#)
- “Voice Processing” on [page 17-83](#)
- “VoIP Echo Cancellation Troubleshooting” on [page 17-87](#)
- “VPIM Networking” on [page 17-88](#)

99 Nodes Support

Table 17-2 contains troubleshooting information for 99 Nodes support. For more information about 99 Nodes, refer to the *Mitel 5000 Reference Manual*, part number 580.8007.

Table 17-2. 99 Nodes Support Troubleshooting Issues

Symptom	Possible Cause	Corrective Action
Increased Node Capacity: A system is continuously experiencing software exceptions and resetting. The system resides in a network of 63+ nodes. The node is running earlier than v2.1 software.	The node that is resetting is running an invalid software version. After the network is operating at a 63+ node network, nodes cannot downgrade to earlier than v2.1.	Upgrade the node to v2.1 or later.
Attendant Console Causes Slow-Downs: The system slows down when an Attendant Console application connects to a system.	This is a “brute force” OAI command that requests all the off-node device information from the system. The slow down is directly related to the number of off-node devices in the system.	Leave the Attendant Console running continuously rather than shutting off the application during non-work hours. This will reduce the number of refreshes the console performs to get status of the devices in the network.
“Brute Force” Network Broadcasts: The system uses the last IP resource. Per design in Axxess 7.0 IP networking, the system sends a broadcast message to all nodes in the network to inform them that it cannot handle IP networking calls. As an IP resource frees up, the system sends a broadcast message to all nodes in the network again to inform them that it can handle IP networking calls. If the system oscillates between this last IP resource, it can cause a tremendous amount of IP traffic on the entire network.	Insufficient IP networking resources.	This condition of oscillating on the last IP resource is undesirable. If the system is in this state, upgrade to a Processor Expansion card to increase the number of IP resources. If the system is a Mitel CS-5400, attempt to reduce the number of IP endpoints to allow more networking IP resources. Note that v2.1 or later will modify this logic to prevent the “brute force” network broadcasts.

Administrative Web Session

Table 17-3 summarizes troubleshooting strategies recommended for resolving Administrative Web Session discrepancies.

Table 17-3. Administrative Web Session Troubleshooting Strategies

Symptom	Possible Cause	Corrective Action
A 404 Not Found error comes up when the user tries to access the Web page.	The user tried to access a page that does not exist on the server.	Use the links provided by the menu to access available pages.
A “Cannot find server” error comes up when the user tries to access the Web page.	The user typed the IP address incorrectly.	Make sure the IP address is the address of the system and was not typed incorrectly. Also, make sure the system is running, plugged in, and the lighted server is running.
A 401 Unauthorized error comes up when the user tries to access the Web page.	The user typed the username or password incorrectly.	Make sure the user name and password is for the correct system and was not typed incorrectly.
The T1M-2 application does not show up on the AWS page for the corresponding expansion bay	The module might not be online.	Verify that the module is properly seated in the desired expansion bay and that the Online LED is green.
While making several outgoing or incoming calls, the status of the channels still shows up as idle.	The channels are not actually in-use.	Verify that incoming and outgoing access is programmed correctly in DB Programming and that the CO trunk groups contain the desired list of trunks to test. Also verify, when testing calls over private networking, that the correct route group is programmed properly.
After busying out a port, some channels still show up as active when accessing the channel status page.	Channels already actively on a call while the user attempts to busy out the port will go into the Pending Busy state.	When the calls have completed, the channels will then go to the Busy state.
The following error message appears: “Due to your network configuration, cannot locate Processing Server. “	You have attempted to access the Base Server directly from the public network.	You must use the Processing Server proxy to access the Base Server from the public network. Refer to the AWS online Help for details and configuration examples.

Basic Voice Mail

Table 17-4 summarizes the troubleshooting strategies recommended for resolving discrepancies that may occur with Basic Voice Mail (BVM).

Table 17-4. Basic Voice Mail Troubleshooting Strategies

Symptom	Possible Cause
BVM is running on the PS-1. IP endpoints or digital endpoints have bad quality.	Voice packets are not getting from the Base Server to the PS-1 in a timely manner. This could happen for the following reasons: <ul style="list-style-type: none">• Network is overloaded• PS-1 and Base Server are not on the same LAN and VLAN using the same switch
BVM is running on the PS-1. IP endpoints or digital endpoints have bad quality.	Voice packets are not getting from the PS-1 to the endpoints in a timely manner. This could happen if PS-1 or any of the IP endpoints have duplicate IP addresses. Power cycling can sometimes cause routers/switches to default to previous values.

Caller ID Forwarding

The following table lists troubleshooting information for the Caller ID Forwarding feature.

Table 17-5. Caller ID Forwarding Support Troubleshooting Issues

SYMPTOM	POSSIBLE CAUSE	CORRECTIVE ACTION
The customer reports incoming trunk caller ID does not forward to an outbound PSTN call.	The original incoming trunk call did not have caller ID.	Enable service with the CO provider to ensure incoming trunk calls have caller ID.
	The system administrator has not enabled the "Propagate Original Caller ID for Unanswered Calls" flag for the correct CO trunk group.	Enable the "Propagate Original Caller ID for Unanswered Calls" flag for the correct CO trunk group.
	The outbound call is sent out a non-ISDN PSTN line.	For Caller ID Forwarding, the customer must use an ISDN line to forward caller ID.
	The original trunk is answered by the system (either through a Voice Mail application, human operator, or Unified Communicator).	Currently, the system does not support propagating caller ID for incoming trunk calls that are answered and then transferred back out to the PSTN.
	If the answer is none of the above, the CO may not support the ISDN message for propagating caller ID.	Call the CO provider to determine why the ISDN caller ID information is not forwarded. If the CO cannot resolve this issue, contact Technical Support and provide the following information: 1) the ISDN switch type where outbound calls was made; and 2) freeze of this call scenario.
The customer reports endpoint caller ID does not forward to external PBX.	The system administrator has not enabled the "Send Station Caller ID to Attached PBX" flag for the correct CO trunk group.	Enable the "Send Station Caller ID to Attached PBX" flag for the correct CO trunk group.
	The outbound call is sent out a non-ISDN PSTN line.	For Caller ID Forwarding, the customer must use an ISDN line to forward caller ID.
	An unsupported SIP gateway is used to connect the system to an external PBX.	Verify that the SIP gateway has been officially tested. If the SIP gateway is officially supported, call Technical Support and provide the following information: 1) the ISDN switch type where outbound calls was made, 2) type of gateway used to connect to external PBX, 3) ISDN switch type settings on SIP gateway, and 4) freeze of this call scenario.
The customer reports endpoint caller ID name (and only name) is not propagating to an external PBX. The customer is using a SIP gateway to communicate to an external PBX.	Two specific conditions cause this to happen: 1) the outbound ISDN line is configured as a DMS-100; and 2) the originating extension is calling out ARS and ARS is routing the call to a remote node.	There is a scenario where endpoint Caller ID Forwarding is used over a networked ARS configuration, and the endpoint user name will not be passed in the ISDN calling party name field. If the outgoing ISDN line uses the "display IE" method to transfer the calling party name, the calling party name will not use the endpoint's user name. Instead of the user name, the system uses the calling party name as the name.

Caller ID Propagation

The following table lists troubleshooting information for the Caller ID Propagation feature. For complete information about Caller ID Propagation, refer to the “System Features” chapter in the *Mitel 5000 Reference Manual*, part number 580.8007.

Table 17-6. *Caller ID Propagation Support Troubleshooting Issues*

Symptom	Possible Cause	Corrective Action
Incoming trunk caller ID does not propagate to an outbound PSTN call.	The original incoming trunk call did not have caller ID.	Enable service with the Central Office (CO) provider to ensure incoming trunk calls have caller ID.
	The “Propagate Original Caller ID for Unanswered Calls” flag for the correct CO trunk group is not enabled.	Enable the “Propagate Original Caller ID for Unanswered Calls” flag for the correct CO trunk group.
	The outbound call is sent out on a non-ISDN PSTN line.	For Caller ID Propagation, the customer must use an ISDN line to propagate caller ID.
	The original trunk is answered by the system (either through a Voice Mail application, human operator, or Unified Communicator).	Currently, the system does not support propagating caller ID for incoming trunk calls that are answered and then transferred back out to the PSTN.
	If the cause is none of the above, the Central Office may not support the ISDN message for propagating caller ID.	Call the CO provider to determine why the ISDN caller ID information is not propagated. If the CO cannot resolve this issue, contact Mitel Technical Support and provide the following information: 1) the ISDN switch type where outbound calls were made; and 2) freeze of this call scenario.
Caller ID does not propagate to external PBX.	The “Send Station Caller ID to Attached PBX” flag is not enabled for the correct CO trunk group.	Enable the “Send Station Caller ID to Attached PBX” flag for the correct CO trunk group.
	The outbound call is sent out on a non-ISDN PSTN line.	For Caller ID Propagation, the customer must use an ISDN line to propagate caller ID.
	An unsupported SIP gateway is used to connect the system to an external PBX.	Verify that the SIP gateway has been officially tested. If the SIP gateway is officially supported, call Mitel Technical Support and provide the following information: 1) the ISDN switch type where outbound calls were made; 2) the type of gateway used to connect to external PBX; 3) ISDN switch type settings on SIP gateway; and, 4) freeze of this call scenario.

Table 17-6. *Caller ID Propagation Support Troubleshooting Issues (Continued)*

Symptom	Possible Cause	Corrective Action
The customer reports station caller ID name (and only name) is not propagating to an external PBX. The customer is using a SIP gateway to communicate to an external PBX.	Two specific conditions cause this to happen: 1) the outbound ISDN line is configured as a DMS-100; and 2) the originating extension is calling out ARS and ARS is routing the call to a remote node.	There is a scenario where station Caller ID Propagation is used over a networked ARS configuration, and the station username will not be passed in the ISDN calling party name field. If the outgoing ISDN line uses the “display IE” method to transfer the calling party name, the calling party name will not use the station's username. Instead of the username, the system uses the calling party name as the name.

CO [Local Exchange] Trunks

Table 17-7 summarizes the troubleshooting strategies recommended for resolving CO [Local Exchange] trunk discrepancies.

Table 17-7. CO Trunk Troubleshooting Strategies

Symptom	Possible Cause	Corrective Action
CO trunk inoperative throughout the system	Defective CO trunk from central office	At the associated CO block, remove the bridging clips for the trunk. On the telco side of the block, use a test set to verify the CO trunk connection. Also, move the CO trunk to a known good CO circuit. If the problem follows the trunk, contact the telephone company.
	Trunk is dedicated to a secondary carrier requiring an access code	Verify the type of CO trunk. Instruct users to dial access code if required.
	Defective cabling or mis-wired amphenol connector on the trunk module	Using a test set, ensure presence and correct location of the CO trunk at the associated CO block.
	Programming error	Ensure that the trunk is assigned to the correct CO trunk group and endpoints have been given access to it. See "Assigning Trunks to CO Trunk Groups" on page 6-5 .
	Defective trunk module	Replace the associated trunk module.
	Defective processor module	Replace the module if faulty.
Cannot obtain CO dial tone	If reorder tone is heard, programming error	Ensure that endpoint has outgoing access. Also, check to see if the endpoint is programmed for ARS only. Ensure trunk is assigned to the correct trunk group. See "Assigning Trunks to CO Trunk Groups" on page 6-5 .
	If progress tone is heard, user error	System is programmed to expect a forced account code. See "Account Codes" on page 7-69 .
	Selected trunk is designated as incoming-only	Cannot dial out on an incoming-only trunk.
	Defective trunk module	Replace the associated trunk module.
	Defective processor module	Replace the module if faulty.
Low volume on all CO trunks; cannot break CO dial tone	Defective CO trunk from central office	At the CO block, remove the bridging clips for the trunk. On the telco side of the block, use a test set to verify the CO trunk connection. Also, move the CO trunk to a known good CO circuit. If the problem follows the trunk, contact the telephone company.
	Open or loose connection in the cable between the power supply and the backplane	If, with all trunk modules removed, the system volt ages are still not within tolerance, turn off the system and check the cable and connector with an ohmmeter. Replace or repair the faulty cable.
	Defective power supply	Replace the chassis if the power supply is faulty.

Table 17-7. CO Trunk Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
Cannot break CO dial tone	CO circuit is programmed for wrong signaling type	Ensure that CO trunk and CO circuit use same type signaling (DTMF or dial pulse). See “DTMF Signaling” on page 6-13 .
	Defective CO trunk from central office	At the CO block, remove the bridging clips for the trunk. On the telco side of the block, use a test set to verify the CO trunk connection. Also, move the CO trunk to a known good CO circuit. If the problem follows the trunk, contact the telephone company.
	Timer error	If trunk is DTMF, the DTMF Digit Duration/ Pause timer setting may not be compatible with the trunk. See “Timers and Limits” on page 10-24 .
	Defective trunk module	Replace the associated trunk module.
	Defective processor module	Replace the module if faulty.
NOTE See also endpoint problems on page 17-21 .		
Cannot place an outgoing call; CO dial tone is present; intercom works	Programming error	Check endpoint class of service (COS). Check that equal access and absorbed digit programming for the trunk group are correct. Check ARS. See “Toll Restrictions” on page 8-16 .
	Defective CO trunk from central office	At the CO block, remove the bridging clips for the trunk. On the telco side of the block, use a test set to verify the CO trunk connection. Also, move the CO trunk to a known good CO circuit. If the problem follows the trunk, contact the telephone company.
	Defective endpoint	Replace the endpoint and/or perform the endpoint self-test as outlined in the Installation chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Selected trunk is designated as incoming-only	Cannot dial out on an incoming-only trunk.
	Defective trunk module	Replace the associated trunk module.
	Defective processor module	Replace the module if faulty.
NOTE See also endpoint problems on page 17-21 .		
Other endpoint conversations can be heard on the CO trunk (crosstalk)	Defective CO trunk(s)	Isolate the trunk(s) with crosstalk by removing the bridging clips from the CO block. On the telco side of the block, attach a test set to each trunk and check for crosstalk. If present, contact the telephone company.
	Defective cabling or mis-wired amphenol connector on the trunk module	Using a test set, ensure presence and correct location of the CO trunk at the associated CO block.
	Defective digital endpoint module	Replace the associated digital endpoint module.
	Defective trunk module	Replace the associated trunk module.
	Defective processor module	Replace the module if faulty.

Table 17-7. CO Trunk Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
Outside calls dropped during conversation or upon answering CO trunk	User error (trunk button being pressed after initial connection is made)	Instruct users not to press the trunk button while on a call. Or, if necessary, set the CO Reseize timer to a higher value. Default value is 3 seconds. Or, program the endpoint to disable CO reseize. See “Timers and Limits” on page 10-24 .
	Defective CO trunk from central office	At the CO block, remove the bridging clips for the trunk. On the telco side of the block, use a test set to verify the CO trunk connection. Also, move the CO trunk to a known good CO circuit. If the problem follows the trunk, contact the telephone company.
	Insufficient loop current supplied by central office	Central office must supply 18 mA minimum loop current.
	IC-CO Disconnect timer value is set too short	Ensure timer value is long enough to ignore normal interruptions in CO loop current. Default value is 0.6 seconds. See “Timers and Limits” on page 10-24 .
	Defective digital endpoint module	Replace the endpoint and/or perform the endpoint self-test as outlined in Installation chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Defective trunk module	Replace the trunk module if faulty.
	Defective processor module	Replace the module if faulty.
CO trunk cannot be reseized	CO Reseize feature is disabled	Check endpoint programming. If the CO Reseize option has been disabled, the user cannot reseize a trunk until it has been disconnected by hanging up or pressing another trunk button. See “Timers and Limits” on page 10-24 .
	CO Reseize timer is set too high	Set the timer to a lower timer value. Default value is 3 seconds. See “Timers and Limits” on page 10-24 .
	User error	If the endpoint is programmed with the validate account codes option and the user enters an invalid Account Code For All Calls Following, calls will not be allowed at the endpoint until the code is removed or reprogrammed. See “Account Codes” on page 7-69 .
Noise on CO trunk at all endpoints	Defective CO trunk	At the CO block, remove the bridging clips for the trunk. On the telco side of the block, use a test set to verify the CO trunk connection. Also, move the CO trunk to a known good CO circuit. If the problem follows the trunk, contact the telephone company.
	Defective trunk module	Replace the associated trunk module.
	Defective power supply	Replace the chassis if the power supply is faulty.
	Defective processor module	Replace the module if faulty.

Table 17-7. CO Trunk Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
CO trunk remains seized after a call has been ended	Characteristic of some ESS central offices	Central office must provide disconnect signal. Or, install a trunk release module available from most supply houses.
	IC-CO or CO-CO Disconnect timer value set too long	Central office disconnect signal was not detected by IC-CO or CO-CO Disconnect timer. Default value of the IC-CO timer is 0.6 seconds; the CO-CO timer is 0.35 seconds. See “Timers and Limits” on page 10-24 .
	Defective CO trunk	At the CO block, remove the bridging clips for the trunk. On the telco side of the block, use a test set to verify the CO trunk connection. Also, move the CO trunk to a known good CO circuit. If the problem follows the trunk, contact the telephone company.
	Defective endpoint	Replace the endpoint and/or perform the endpoint self-test as outlined in the Installation chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Defective trunk module	Replace the associated trunk module.
	Defective processor module	Replace the module if faulty.
The module port is not synchronized to the CO [Local Exchange].	Reference clock may be incorrectly programmed.	Verify that the reference clock for the port is programmed correctly.

Database Change Log

Table 17-8 lists troubleshooting information for the Database Change Log feature.

Table 17-8. Database Change Log Troubleshooting Issues

Symptom	Possible Cause	Corrective Action
Changes are not being recorded in a log on the Mitel 5000.	The mode is Local.	You must use a Network connection for database changes to be logged in the Mitel 5000.
The Database Change Log and backups do not hold enough information.	The files are too small.	Contact Technical Support to increase the maximum file size in System\Maintenance\Logging Options\Database Change Log in Online Monitor mode (OLM). NOTE Do not use OLM mode unless you are instructed to do so by support personnel.
	There are not enough files.	Contact Technical Support to increase the maximum number of files in System\Maintenance\Logging Options\Database Change Log in Online Monitor mode (OLM). NOTE Do not use OLM mode unless you are instructed to do so by support personnel.

Digital Endpoint Interface

Table 17-9 shows troubleshooting information for Mitel 5000 DEI.

Table 17-9. DEI Troubleshooting Strategies

Symptom	Possible Cause	Possible Solution
Alarm 130 appears on the Base Server LCD panel display.		See “Licensing Issues” on page 17-45 .

Endpoints

Table 17-10 summarizes troubleshooting strategies recommended for resolving endpoint discrepancies.

Table 17-10. Endpoint Troubleshooting Strategies

Symptom	Possible Cause	Corrective Action
Endpoint inoperative; LED indication present while any button with an LED is held down; reorder tone is heard when button is pressed.	System lockout caused by excessive data errors (displays SYSTEM LOCKOUT).	Remove and replace the line cord to reset the endpoint.
	Programming error (circuit identified as dual single line sets—SLA; no reorder tone is heard)	Identify the circuit for endpoint use, not dual single line sets (SLA). See the “Endpoints and Devices” on page 7-1 .
	Defective cabling or connections	Ensure that all cables are correctly connected to the modular jack as shown in the Installation chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000. Check for loose or open connections in the endpoint cabling and the line cord.
	Defective endpoint	Replace the endpoint if faulty.
	Defective digital endpoint module	Replace the associated module.
Endpoint inoperative; LED indication present while any button with an LED is held down; reorder tone is heard when button is pressed	Defective processor module	Replace the module if faulty.
	Programming error or Improper configuration of IP connections, firewall and/or network address translation	Make sure the IP endpoint is programmed on the same subnet. See Appendices A and B for configuration guidelines.
	Older version or incompatible firmware on the endpoint	Verify the correct firmware and upgrade to the latest version through the endpoint Web interface. Reset the Web page to check for the latest version of firmware installed on the endpoint.
	IP resources are not allocated correctly; Display shows “No IP Resources Allocated”	Make sure you have enough IP resources and they are allocated correctly.
	No IP connection and endpoint will continually reboot and recycle	Verify the LAN link light is active on the IP endpoint.
	Defective switch port, cabling, or improper power supply for the endpoint and endpoint will continually reboot and recycle	See if you can ping the system and check for network connectivity. Replace the faulty switch port, cabling, or install the correct power supply.

Table 17-10. Endpoint Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
Endpoint inoperative; no LED indication when any button is pressed; no audio is present	Defective endpoint	Perform the endpoint self-test as described in the Installation chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.80000, and replace the endpoint if faulty.
	Defective cabling or connections	Ensure that 24/48 VDC is present at the power supply or the Power Over Ethernet (POE) switch and is correct. Check for loose or open connections in the endpoint cabling. For more information about hardware connections, refer to the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Defective power supply	Verify the endpoint has the correct power supply voltage.
	Defective digital endpoint module	Replace the associated module.
Erratic endpoint operation (lamp status incorrect)	Endpoint cable exposed to interference	Ensure proper endpoint cable runs. For more information about cable runs, refer to the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Loop limits exceeded	Perform the endpoint loop resistance test as outlined in the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Defective cabling or connections	Ensure that 24/48VDC is present at the power supply or the Power Over Ethernet (POE) switch and is correct. Check for loose or open connections in the endpoint cabling. For more information, refer to the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Defective endpoint	Perform the endpoint self-test as described in the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000. Replace the endpoint if faulty.
	Programming error	Ensure that the proper keymap has been assigned to the endpoint. See “Keymaps” on page 7-27 .
	Defective digital endpoint module	Replace the associated module.
	Defective processor module	Replace the module if faulty.
	Database corruption	Run the database through the Test Utility.
	System memory is low	Run the diagnostics heap statistics to determine if the system is losing heap memory and how quickly the system may be losing it.
Endpoint squeals on outside calls or when receiving a handsfree intercom call from a single line endpoint (feedback)	Speaker volume is too loud	Reduce feedback by lowering speaker volume using endpoint volume controls.
	Poor acoustics	Poor acoustics can cause poor quality on handsfree calls. Try placing a private call through the handset.

Table 17-10. Endpoint Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
NOTE A two- to four-wire converter is used during communication between endpoints and single line stations. Reflection is a normal characteristic of these converters. Feedback on intercom calls is eliminated when the single line station user places a private intercom call by pressing the pound/hash (#) button before dialing the intercom number or by entering the ring intercom always feature code – 377 (provided the endpoint user does not press the SPKR button to respond).	Defective endpoint	Perform the endpoint self-test as described in the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Defective trunk module	Replace defective trunk module.
	Defective digital endpoint module	Replace the associated module.
	Defective processor module	Replace the module if faulty.
NOTE See also CO trunk problems.	Defective endpoint	Perform the endpoint self-test as described in the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000. Replace the endpoint if faulty.
	Defective digital endpoint module	Replace the associated module.
	Defective processor module	Replace the module if faulty.
	Defective endpoint	Perform the endpoint self-test as described in the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000. Replace the endpoint if faulty.
Cannot break intercom dial tone	Defective digital endpoint module	Replace the associated module.
	Defective processor module	Replace the module if faulty.
	Defective endpoint	Perform the endpoint self-test as described in the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000. Replace the endpoint if faulty.
	Defective digital endpoint module	Replace the associated module.
Cannot place intercom call; IC dial tone is present, but reorder tone is heard when call is attempted	Defective processor module	Replace the module if faulty.
	User error	Invalid intercom number or improper dialing procedure.
	Defective endpoint	Perform the endpoint self-test as described in the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000. Replace the endpoint if faulty.
	Defective digital endpoint module	Replace the associated module.
	Defective processor module	Replace the module if faulty.

Table 17-10. Endpoint Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
Cannot receive Off-Hook Voice Announce (OHVA) calls	Programming error	Ensure that the system option for OHVA is enabled—see “System Flags” on page 10-19 —that the called endpoint is programmed to receive OHVA calls, and that the calling endpoint is programmed to transmit OHVA calls—see the “Endpoint Flags” on page 7-22 .
	User error	The called endpoint is a single-line set or an endpoint that is programmed not to receive OHVA calls. Or, the called endpoint user may have blocked the OHVA call. For more information about OHVA, refer to the “System Features” chapter in the <i>Mitel 5000 Reference Manual</i> , part number 580.8007.
	Secondary voice path busy	The endpoint does not receive off-hook voice announce calls when the secondary voice path or speakerphone are in use. For more information about OHVA, refer to the “System Features” chapter in the <i>Mitel 5000 Reference Manual</i> , part number 580.8007.
	Defective PCDPM Module	Check installation and connections, and replace PCDPM if defective. For more information about PCDPM installation requirements, refer to the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Defective endpoint	Perform the endpoint self-test as described in the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000. Replace the endpoint if faulty.
	Defective digital endpoint module	Replace the associated module.
	Defective processor module	Replace the module if faulty.
Cannot place off-hook voice announce calls	Programming error	Ensure that the system option for OHVA is enabled—see “System Flags” on page 10-19 —that the called endpoint is programmed to receive OHVA calls, and that the calling endpoint is programmed to transmit OHVA calls—see the “Endpoint Flags” on page 7-22 .
	User error	The called endpoint is a single line set or an endpoint that is programmed not to receive OHVA calls. Or, the called endpoint user may have blocked the OHVA call.
	Secondary voice path busy	The called endpoint cannot receive off-hook voice announce calls when its secondary voice path or speakerphone are in use.
	Defective endpoint	Perform the endpoint self-test as described in the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000. Replace the endpoint if faulty.
	Defective digital endpoint module	Replace the associated module.
	Defective processor module	Replace the module if faulty.

Table 17-10. Endpoint Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
Data device connected to endpoint not operating properly	User error	Refer to manufacturer's operating instructions.
	Secondary voice path busy	The endpoint will not transmit data calls when the secondary voice path or speakerphone are in use.
	Problem with data device	Disconnect data device and check operation according to the manufacturer's instructions.
	PCDPM, MDPM, or AC transformer not installed properly or defective	Check installation and connections. For more information about hardware connections, refer to the "Installation" chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Data Port Module not installed properly or defective	Check Data Port Module installation and jumper strap settings. For more information about the Data Port Module, refer to the "Installation" chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000. Replace if defective.
	Defective endpoint	Perform the endpoint self-test as described in the "Installation" chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000. Replace the endpoint if faulty.
	Defective digital endpoint module	Replace the associated module.
Data noise in any off-hook condition	Defective processor module	Replace the module if faulty.
	Defective cabling or connections (e.g., line cord, amphenol connector, bridging clip, etc.)	Check for loose or open connections, or crossed wires.
	Defective endpoint	Try another endpoint.
Optional headset inoperative	Defective digital module	Replace the associated module.
	User error	Ensure the enable headset feature code (315) was entered. Check feature code programming to see if code was changed. See "Feature Codes" on page 10-33 .
	Incorrect or defective headset	Ensure the headset contains the appropriate microphone (dynamic or electret). Ensure the headset's configuration dial is set to where you can hear the tone (refer to the manufacturer's installation sheet). Replace headset if necessary.
	Defective endpoint	Try another endpoint.
	Defective processor module	Replace the module if faulty.
	Defective power in headset.	Replace the power or batteries. Also verify the manufacturer's settings for correct operation of the headset.

Table 17-10. Endpoint Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
Delayed audio connection on incoming calls when using a headset with an Attendant Console computer	Headset in battery saving mode	Some headsets have a battery saving feature that turns the headset off after a certain period of inactivity. To prevent these headsets from missing portions of incoming calls, the endpoint flag can be programmed to generate a "Send Alert Burst To Headset" that activates the headset before connecting to an incoming call. See the "Endpoint Flags" on page 7-22 . Or, if necessary, disable the feature and/or replace the batteries with a transformer.
	User error	Ensure the enable headset feature code (315) was entered. Check feature code programming to see if code was changed.
	Incorrect or defective headset	Ensure the headset contains the appropriate microphone (dynamic or electret). Ensure the headset's configuration dial is set to where you can hear the tone (refer to the manufacturer's installation sheet). Replace headset if necessary.
	Defective endpoint	Try another endpoint.
	Defective processor module	Replace the module if faulty.
AgentSet inoperative	Not in headset mode	Ensure the enable headset feature code (319) was entered. Check feature code programming to see if code was changed. At the endpoint, unplug the headset or handset (to take the AgentSet off hook) and enter the Headset On/Off feature code (319) to enable headset mode. Then plug in the headset or handset.
	Incompatible headset	Use only a Mitel headset.
LRA device connected to analog endpoint not operating properly	Problem with LRA device	Disconnect LRA device and check operation according to the manufacturer's instructions.
	Data Port Module not installed properly or defective	Check Data Port Module installation and jumper strap settings. For more information about installing the Data Port Module, refer to the "Installation" chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000. Replace if defective.
	Defective analog endpoint	Try another endpoint.
	Programming error.	Make sure the Extended Ring Cadence flag is enabled.

Expansion Modules

Table 17-11 summarizes troubleshooting strategies recommended for resolving discrepancies involving expansion modules.

Table 17-11. *Expansion Module Troubleshooting Strategies*

Symptom	Possible Cause	Possible Solution
The BRM-S module ONLINE LED is off.	The module is not inserted all the way into the bay.	Make sure the module is inserted all the way into the bay and programmed correctly.
Cannot set the module to support station in NT mode.	The module does not support NT mode.	N/A
Cannot hook-up a video conference directly to a BRM-S module.	BRM-S does not support video conferences.	N/A
The module port is not synchronized to the CO [Local Exchange].	Reference clock may be incorrectly programmed.	Verify that the reference clock for the port is programmed correctly.

File-Based MOH

Table 17-12 lists troubleshooting information for the File-Based MOH feature.

Table 17-12. *File-Based MOH Troubleshooting Issues*

Symptom	Possible Cause	Corrective Action
A subscriber tries to listen to the file-based MOH source. No audio is heard and the endpoint displays "Waiting for Resources."	The defined file-based MOH source is configured correctly and has an allocated VoIP resource, but the endpoint does not play the associated audio if there are no VoIP resources available for the endpoint.	The subscriber hears silence until a VoIP resource becomes available.
A subscriber tries to listen to the file-based MOH source, but no audio is heard.	The file-based MOH source has a filename configured, but a corresponding audio file does not exist. Either the file-based MOH source was deleted or it is not modified to use the proper file in DB Programming.	Reconfigure the file-based MOH source to use the proper music file.
A subscriber tries to listen to the file-based MOH source, but no audio is heard. The file-based MOH source is configured correctly.	The device is using a file-based MOH source that cannot obtain a VoIP resource because there are not enough licenses for the list of defined file-based MOH sources.	The file-based MOH source that does not have a VoIP resource cannot play audio until enough of the other file-based MOH sources are unequipped, therefore freeing up an associated license.
A subscriber tries to listen to the file-based MOH source, but silence is heard. The file-based MOH source is configured correctly. VoIP resource and software license is available.	The file-based MOH source is not in the correct format.	Audio files for this feature must be in the G.711 format. The IP Resource Application (IPRA) still plays back a file even if it is not in the correct format. Convert the file to the proper format before you upload it to the compact flash-type memory card.
A subscriber tries to listen to the file-based MOH source, audio is heard, but the correct audio is not.	The file-name associated with the file-based MOH source is not the correct file.	Associate the correct file name with the desired file-based MOH source in DB Programming.
You cannot upload an audio file to the Mitel 5000 using the Administrative Web Session (AWS).	The compact flash-type memory card is at 80% capacity.	Delete some files on the compact flash-type memory card (either MOH audio files or voice mail messages) to make space available.
You cannot associate a filename with a particular file-based MOH source in DB Programming.	The filename is already in use by another file-based MOH source.	This is as-designed. Use another filename for the file-based MOH source.

Four-Port Single Line Module

Table 17-13 summarizes the troubleshooting strategies recommended for resolving SLM-4 discrepancies.

Table 17-13. *Single Line Module (SLM-4) Troubleshooting Strategies*

Symptom	Possible Cause	Corrective Action
SLM-4 does not work after being plugged in.	Software prior to v2.x does not support SLM-4.	Upgrade all software to 2.x using the upgrade utility.
SLM-4 does not work when plugged in.	SLM-4 is not programmed in DB Programming.	Mitel does not support Auto-Equip for SLM-4 modules. When the module is plugged in for the first time, it still has to be programmed in DB Programming for the appropriate bay.
After plugging in multiple SLM-4 modules only one is working.	Only one SLM-4 can be installed on the v2.0 or later system.	Using more than one SLM-4 on the current system is not allowed. Only one SLM-4 can be programmed in DB Programming. An SLM-4 can be installed into any of the three bays on Base Server, and for proper operation only one SLM-4 should be plugged in at a time.
DTMF receiver not available for SLM-4 or the SL module.	All of the DTMF receiver resources are in use.	Although this occurrence is extremely rare, try again when resources free up.

Import Endpoints from CSV Files

Table 17-14 lists troubleshooting information for importing endpoints from CSV files.

Table 17-14. *Import Endpoints from File Troubleshooting Strategies*

Error Message	Possible Cause	Corrective Action	IP Endpoint	Digital Endpoint										
One or more extensions are invalid.	One or more extensions may: <ul style="list-style-type: none">• conflict with existing extensions in the database.• conflict with any extensions in the dialog box.• contain invalid characters.• exceed five digits.	Click any of the extension fields, and then either type in a new extension or select a valid extension from the Extension list.	✓	✓										
One or more descriptions contain invalid characters.	Descriptions are restricted to 20 characters and all printable characters except for “[.”	Click the description in the list, and then remove the invalid characters from the field.	✓	✓										
One or more usernames contain invalid characters.	User names are restricted to 10 characters and all printable characters except for “\,” “~,” and “[.”	Click the user name in the list, and then remove the invalid characters from the field.	✓	✓										
One or more usernames were too long and have been truncated.	If more than 10 characters exist for any user name imported, the user name is truncated to 10 characters	None. As designed. ¹	✓	✓										
One or more descriptions were too long and have been truncated.	If more than 20 characters exist for any description imported, the description is truncated to 20 characters.	None. As designed. ¹	✓	✓										
One or more MAC Addresses are invalid.	One or more MAC Addresses may: <ul style="list-style-type: none">• conflict with existing MAC Addresses in the database.• conflict with any MAC Addresses in the dialog box.• contain invalid characters,.	Click any of the MAC Address fields, and then edit the field in the Edit MAC Address box.	✓											
You may only import X IP Endpoint(s). You will need to delete Y endpoint(s) to continue with the import.	<div>The number of endpoints read from the file exceeds the system limit described below.</div> <div>Table 17-15. IP Endpoint System Limit</div> <table><tr><th>System Type</th><th>Limit</th></tr><tr><td>CS-5200</td><td>75</td></tr><tr><td>CS-5400</td><td>175</td></tr><tr><td>CS-5600</td><td>250</td></tr><tr><td>All Types</td><td>250¹</td></tr></table> <div>1. Includes IP endpoints and IP trunks.</div>	System Type	Limit	CS-5200	75	CS-5400	175	CS-5600	250	All Types	250 ¹	Delete Y endpoints from the list.	✓	
System Type	Limit													
CS-5200	75													
CS-5400	175													
CS-5600	250													
All Types	250 ¹													

Table 17-14. *Import Endpoints from File Troubleshooting Strategies*

Error Message	Possible Cause	Corrective Action	IP Endpoint	Digital Endpoint
You selected X port(s) for installing new endpoints. You will need to delete Y endpoint(s) to continue with the import.	More endpoints are read from the file than ports selected. The X indicates the number of ports selected before invoking this dialog and the Y indicates the number of endpoints to delete from the endpoints listed.	Delete Y endpoints from the list .		✓

1. This error message does not disable the Import button.

IP Resource Application (IPRA)

Table 17-16 summarizes the troubleshooting strategies recommended for resolving discrepancies occurring with the IPRA.

Table 17-16. *IPRA Troubleshooting Strategies*

Symptom	Possible Cause	Corrective Action
IP endpoints will not come online.	The system pre-allocates one IP resource for each IP device. If the system has insufficient IP resources, the IP device will not be functional.	Get more IP resources.
		Dedicate IP resources for endpoint usage.
DESTINATION UNREACHABLE is shown on an endpoint when making a call across private networking.	<p>There is a blocking condition somewhere in the call path. Blocking conditions may include:</p> <ul style="list-style-type: none">• An IP private networking connection with busy IP resources.• A PRI private networking connection with busy B-channels.• A private networking node that is not operational.	<p>Try to place the call again when resources become available. If the condition persists, try the following:</p> <ul style="list-style-type: none">• Verify that all nodes in the call path are operational.• Get more IP resources in the case of a busy IP private networking connection.• Program more B-channels in the case of a busy PRI private networking connection.

IP Devices

Table 17-17 summarizes the troubleshooting strategies recommended for resolving discrepancies that may occur when using IP devices.

Table 17-17. *IP Devices Troubleshooting Strategies*

Symptom	Possible Cause	Corrective Action
IP endpoint displays VOIP RESOURCE IS UNAVAILABLE	The number of programmed IP devices exceeds the number of available voice channels, and all programmed voice channels are in use.	Verify that IP resources are properly allocated. See the "Resource Reservation Tool" on page 9-42 .
Message Print output indicates that a SIP endpoint extension is invalid or incomplete.	The SIP endpoint is calling its own number or a number that is programmed but not networked.	Verify the cause but do nothing to attempt to fix the condition. The cause of the printout is the SIP server performing its normal cycle of events.
The Upload Utility is not connecting to the IP devices.	The endpoint does not have the latest firmware and they are constantly retrying the connection and blocking the Upload Utility.	In general, you should upgrade the IP devices before you upgrade the IPRA. If, however, you have already upgraded the IPRA, you must manually place the devices in the download state before you upload the firmware.

Table 17-17. IP Devices Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
The Upload Utility is not working for IP devices.	You have not entered a password for the connection.	Make sure the Password field is complete before you click Start . For more information the Upload Utility password, refer to the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	The IP address entered is wrong.	Reprogram the endpoint as a static IP address. Or verify you entered the correct IP address.
NOTE The Upload Utility applies to the Model 8660 and IP PhonePlus endpoints only.		
A call was established, but the device cannot send DTMF digits.	The IP endpoints are programmed for P2P audio, but they do not support the same DTMF encoding setting.	Remove the IP devices from the Network Group. Consider adding them to a Network Group that contains IP devices that support the same DTMF encoding setting.
A call was established between two IP endpoints, but there is no audio.	The IP endpoints are programmed for P2P audio, but they do not support the same vocoder.	Remove the IP devices from the Network Group. Consider adding them to a Network Group that contains IP devices that support the vocoder.
	The IP endpoints are programmed for P2P audio, but they do not support the same number of audio frames per IP packet.	Remove the IP devices from the Network Group. Consider adding them to a Network Group that contains IP devices that support the same number of audio frames per IP packet.
	There is a firewall or NAT between the two devices.	Place the devices into different Network Groups or disable the Use Peer-To-Peer Audio flag for the group. See Appendices A and B for configuration guidelines.
		Make sure the correct IP ports are open. See the “Endpoint and Device IP Settings” on page 9-36 or the Web interface for the current available ports that can be used.
The network is experiencing audio and/or connection problems.	There is a port conflict or the firewall, NAT, or router is blocking the port.	Run Network Qualifier to test the ports to make sure they are not blocked. For more information about the Network Qualifier, refer to the <i>Network Qualifier Reference Manual</i> , part number 835.2427.
		Verify the ports are not blocked. Try changing the ports associated with IP call control and/or audio. Make sure none of them conflict with ports that other protocols use (e.g., SIP uses 5060). See Appendices A and B for configuration guidelines.
Accessing the Record-A-Call or Agent Help feature while using an IP SLA results in the call ringing and then disconnecting as soon as the agent helper or voice mail application answers.	The IP SLA is currently on a peer-to-peer (P2P) call with another IP device. Record-A-Call and Agent Help features are not available on P2P calls.	Remove the IP SLA from a Network Group that supports P2P
Incoming and outgoing calls do not reach the destination.	Incorrect Database or SIP gateway programming. SIP gateway is not on the network. The IPRA is not on the network.	Verify the SIP gateway/IPRA is plugged into the network and the correct IP address is programmed in.

Table 17-17. *IP Devices Troubleshooting Strategies (Continued)*

Symptom	Possible Cause	Corrective Action
There is a One-Way Audio or No Audio problem.	Incorrect Database or SIP gateway programming, There may be Session Description Protocol (SDP) problems.	Verify that the network groups are programmed correctly for both the SIP trunks and any IP endpoints involved in the call.
		Identify if the audio should be peer-to-peer or not.

IP Device Audio

Table 17-18 summarizes the troubleshooting strategies recommended for resolving discrepancies that may occur with IP device audio.

Table 17-18. *IP Device Audio Troubleshooting Strategies*

Symptom	Possible Cause	Corrective Action
Audio quality is poor	The network cannot support VoIP calls.	<p>Pre-Installation: Verify the network's ability to support a VoIP call or calls using the Network Test in the Network Qualifier software application. For more information about the Network Qualifier, refer to the <i>Network Qualifier Reference Manual</i>, part number 835.2427.</p> <div> <p>NOTE</p> <p>The Network Qualifier requires a computer on each site. The computers should not be used for any other purpose because other Windows applications could cause jitter.</p> </div> <p>Post-Installation: Verify the in-time frames percentage using the In-time Packet Graph in the Receive Audio Status page on the Web interface. You can also watch live values through the Audio Receive Statistics on the Telnet interface. Be sure to watch the percentages on both the IPRA and device. Note that the percentages will be quite low with Voice Activity Detection (VAD) enabled. These low values give some indication of the bandwidth saved by not transmitting silent audio packets.</p>
	An IP endpoint does not receive audio packets properly	
	Network related issues: there is heavy traffic contending for bandwidth, a hardware problem with switch or router, or defective cabling.	<p>To improve audio quality, try any of the following:</p> <ul style="list-style-type: none"> • Increase playback (jitter) buffer; however, adds delay or latency. • Use G.729B (B = VAD); does not send silent packets. • Increase Audio Frames/IP packet to reduce bandwidth needed; however, increases latency. • Use switches not hubs. • Prioritize the packets through routers; most simply prioritize the audio port (typically UDP 5004), but could also use DiffServ or TOS. • Add more bandwidth. • Paging and background music consume bandwidth; if a site has low bandwidth, they probably should not put all IP endpoints in the page zone. • Do not use the hub or switch on the IP endpoint for a Computer or other device that will consume a large amount of bandwidth in bursts or constantly.
	Not enough bandwidth to support voice and data.	
		Run the Network Qualifier to assess your bandwidth. For more information about the Network Qualifier, refer to the <i>Network Qualifier Reference Manual</i> , part number 835.2427.

Table 17-18. IP Device Audio Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
An IP endpoint lost audio suddenly while on a muted call	IP endpoints are behind a firewall	When the Voice Activity Detection option is enabled and if any IP endpoints are behind a firewall, the IP endpoints may suddenly lose audio (while on a muted call) or lose background music. The IP endpoint does not send silent audio packets to the IPRA; however, the IPRA continues to send non-silent audio packets to the IP endpoint. Eventually, most firewalls block this unsolicited IP audio stream from the IPRA to the IP endpoint. See Appendices A and B for configuration guidelines.
An IP endpoint lost background music suddenly		

IP Device Connection

Table 17-19 summarizes the troubleshooting strategies recommended for resolving discrepancies with that may occur when connecting IP devices.

Table 17-19. IP Device Connection Troubleshooting Strategies

Symptom	Possible Cause	Corrective Action
Cannot connect a device to the IPRA	Endpoint is not programmed	<p>Check the status in the Connected field in the Circuit Status page on the Web interface or the Network Status field in the Network Information on the Telnet.</p> <p><i>If the device is connected</i>, but not operational, then it is a call processing problem. Verify that the System Database is programmed as follows:</p> <ul style="list-style-type: none"> The MAC address of the device is programmed in DB programming under System – Devices and Feature Codes – <i><endpoints></i> <p><i>If the device is not connected</i>, ensure the Device Type, Device ID, and/or Ethernet Address match the device. The following describes where the Ethernet address or device ID is located on each IP device type.</p> <ul style="list-style-type: none"> IP PhonePlus displays its Ethernet address as it cycles through its power up screens. IP SLA has a sticker with the Ethernet address. IP SoftPhone controls the device ID under the settings option on startup. MGCP Gateway needs the device IP address, instead of the Ethernet address. MGCP endpoint needs the endpoint name, instead of the Ethernet address. <p>On the Web interface, check the IPRA log to make sure the endpoint is connecting to the IPRA.</p>

Table 17-19. IP Device Connection Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
Cannot connect a device to the IPRA	The debug output is not normal	Check the debug output in the Web interface. Normal output appears as follows: <<UDP Broadcast Range/LAN ONLY>> Find server for 00:10:36:00:07:01 from 172.16.10.171:5567 -- port 13 <<UDP PART>> IP ID for 00:10:36:00:07:01 from 172.16.10.171:5567 -- port 13 <<TCP PART>> Connection from 172.16.10.171 on port 13 If the output is not normal, contact Mitel Technical Support.
	The endpoint does not have the latest firmware	Verify the endpoint has the latest firmware by viewing the latest version in the endpoint Web interface. For more information, refer to the "Installation" chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000
General connection issues	The Link LEDs are not lit	Verify the following settings: <ul style="list-style-type: none"> • The Link LED is lit on the processor module and/or device. • The Link LED is lit on the switch or hub to which these devices connect. • The IPRA or device has a unique IP address. • You can ping the IP address from another computer on the same subnet. • You can ping the IP address of the problem device, and also you can ping in the other direction from the problem device or IPRA. • Appropriate ports for IP devices are opened on a firewall, router, and/or NAT. See Appendices A and B for configuration guidelines. To verify the port connection, use the Port Test in the Network Qualifier software application. For more information about the Network Qualifier, refer to the <i>Network Qualifier Reference Manual</i>, part number 835.2427.

IP Device Echo

Table 17-20 summarizes the troubleshooting strategies recommended for resolving discrepancies that may occur with IP device echo.

Table 17-20. IP Device Echo Troubleshooting Strategies

Symptom	Possible Cause	Corrective Action
IP endpoint users hear echo on their endpoint while talking to an analog trunk	Hybrid balance is not on the correct setting	<p>To reduce echo, first test echo and verify the following settings. Then, follow the instructions on the following page.</p> <div> <div>NOTE</div> <p>When testing echo, make sure you dial the same phone number using the same trunk. Seize the trunk directly, and do not use the trunk group or ARS. Different trunks have different characteristics.</p> </div> <p>Verify the hybrid balance setting. If the trunk does not connect to a public CO, or if the CO is relatively close, then the hybrid balance should be set to "Short." No matter what the current setting is, try the other setting and dial the same number through the same trunk. One setting should be dramatically worse than the other. You should disable the Echo Suppression option so you can actually hear the echo from the beginning of the call.</p>
<div> <div>NOTE</div> <p>Refer to the Echo Troubleshooting Guide you can download from the edGe Online Manuals and Guides Web site (www.inter-tel.com/techpublications).</p> </div>		
IP endpoint users hear echo on their endpoint while talking to <i>an analog circuit</i> like on the onboard single lines or trunk	The audio volume for the IP device is too high	<p>To reduce echo from an analog circuit, reduce the audio volume the IPRA drives on to the backplane. This will help the echo canceller adapt quicker. Follow the instructions below:</p> <ol style="list-style-type: none"> 1. Adjust the Backplane Transmit Signal Gain option in DB programming. The default setting is 0dB (without any reduction). Any change you make will reduce the volume. 2. After the adjustment, dial the same number through the same trunk. You should disable the Echo Suppression option so you can actually hear the echo from the beginning of the call. The side effect is that the person on the other end of the call may have a hard time hearing the IP user because the volume is reduced.

Table 17-20. IP Device Echo Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
IP users hear a low-volume, clean, clear echo during the beginning of the audio session	Echo Suppression Sensitivity Level is not balanced	Enable the Echo Suppression option. With this option enabled, adjust the Echo Suppression Sensitivity Level during the beginning of an audio session to find the balance between the IP user hearing a slight echo and hearing a half-duplex condition on the handset. The Echo Suppression Sensitivity Level does nothing if the Echo Suppression is disabled. Disable the Echo Suppression when using the IP SLA for fax operations or as a last resort to eliminate the half-duplex condition on the handset during the beginning of the audio session.
An IP user hears raspy or distorted echo as he speaks quite loudly or holds the handset close to his mouth	The Echo Saturation Blocker option is not enabled	Enable the Echo Saturation Blocker option.
An IP user hears choppiness or a half-duplex condition on the handset as they speak quite loudly or holds the handset close to their mouth.	The Echo Saturation Blocker option is enabled	Disable the Echo Saturation Blocker option.

IP Device VLAN Tagging

Table 17-21 summarizes the troubleshooting strategies recommended for resolving discrepancies that may occur with IP device Virtual Local Area Network (VLAN) tagging.

Table 17-21. IP Device VLAN Tagging-Related Troubleshooting Strategies

Symptom	Possible Cause	Corrective Action
The user cannot connect to the Web interface for a multi-protocol endpoint.	The computer that the user uses may not be in the same VLAN group as the endpoint.	Make sure that the computer and endpoint are in the same VLAN group. If not, set the endpoint VLAN ID to match the computer or disable the VLAN feature for the endpoint.
The user cannot connect to the Model 8690 Web interface but could connect to the Model 8622 or 8662 Web interface. The VLAN ID of the endpoint port is disabled but the VLAN ID of the downlink port is enabled (not zero).	The VLAN ID of the endpoint is disabled.	This is a limitation of the 8690 internal endpoint Ethernet switch. The 8690 Ethernet switch inserts the default VLAN ID which is 1 if the frames from the endpoint are untagged. Connect the computer to one of the downlink ports which has VLAN ID set to zero.
DAISY CHAINING IP ENDPOINTS IS NOT SUPPORTED BY INTER-TEL Two endpoints are daisy chained. The endpoints at the end of the chain cannot connect to the server.	The VLAN ID programmed in the endpoint at the front of the chain may be programmed with a VLAN ID that does not match the VLAN ID of the endpoint at the end of the chain.	Program the VLAN ID at the downlink port at the front of the chain to match the VLAN ID of the endpoint at the end of the chain.
The user powers up the endpoint with the correct VLAN ID, but the endpoint receives the wrong IP settings from the wrong DHCP from another VLAN.	The network switch may not support VLAN or wrong VLAN ID is programmed at the switch port of the core switch network.	Make sure that the core network switch is programmed correctly.
The user powers up 8690 but the network settings still show the settings with the old VLAN values.	The endpoint application may not be updated so the new VLAN settings may not have been propagated to the VPS. If the endpoint application is up to date, then the new VLAN IDs may not have been sent down to the VPS in time.	Make sure that the endpoint application is up to date, and reset the endpoint after the VLAN ID in the endpoint port has been changed from the networking control panel of Windows CE.

IP Networking

Table 17-22 summarizes the troubleshooting strategies recommended for resolving discrepancies that may occur with IP networking.

Table 17-22. IP Networking Troubleshooting Strategies

Symptom	Possible Cause	Corrective Action
Cannot make calls across the IP network	No VoIP channels are available.	Make sure you have the proper networking resources allocated.
	The remote IP address is programmed incorrectly.	Make sure the off-node IP connections have the correct Remote IP Address programmed. See “Remote Node IP Connections” on page 9-21 . This address must match the IP address programmed locally on that node.
	The node cannot find the IP connection.	Make sure the correct Node IP Connection Group is added to the appropriate node. See “Remote Node IP Connections” on page 9-21 .
No audio on network calls	Improper configuration of IP connections, firewall and/or network address translation (NAT)	See Appendices A and B for network configuration guidelines.
	The audio stream receive ports are not programmed correctly.	Make sure the audio stream ports fields match for the affected nodes. See “Local Processor Module and Expansion Card IP Settings” on page 9-17 .
Endpoint display shows INSUFF BANDWIDTH FOR VOICE	The Ethernet cable came unplugged from the IPRA and/or data network (i.e., hub) during a call.	Make sure the Ethernet cable is plugged into the IPRA and data network.
	The data network does not meet the minimum specifications required for IP networking.	Run the Network Qualifier to assess your data network. For more information about the Network Qualifier, refer to the <i>Network Qualifier Reference Manual</i> , part number 835.2427.
	The data network is experiencing problems (e.g., excessive packet loss and traffic).	Contact your network administrator.
One-way audio on network calls	Improper configuration of IP connections, firewall and/or network address translation	See Appendices A and B for network configuration guidelines.
	The audio stream receive ports are not programmed correctly.	Make sure the audio stream ports fields match for the affected nodes. See “Local Processor Module and Expansion Card IP Settings” on page 9-17 .

Table 17-22. IP Networking Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
Poor call quality on network calls	The data network is experiencing problems (e.g., excessive packet loss and traffic).	Contact your network administrator.
	The data network does not meet the minimum specifications required for VoIP.	Run the Network Qualifier to assess your data network. Then verify that your data network meets the minimum specifications. For more information about the Network Qualifier, refer to the <i>Network Qualifier Reference Manual</i> , part number 835.2427.
	The G.711 vocoder is using too much bandwidth.	Switch to a G.729 vocoder, which uses less bandwidth.
	The G.729 vocoder is compressing audio data, resulting in poorer quality.	Switch to a G.711 vocoder, which does not compress audio data, resulting in higher call quality.
	Choppy audio	Adjust the Audio Frames per Packet in DB programming. Try adjusting it up or down to see if it improves audio quality.
DTMF tones are not detected	DTMF tone length is too short.	Set the DTMF Digit Duration/Pause field to 100ms or higher. See “Timers and Limits” on page 10-24 .
	The wrong DTMF vocoder is programmed.	Make sure the DTMF Encoding field is set to either G.711 or RFC2833. See “DTMF Encoding Setting” on page 9-30 .
Cannot fax across the network	IP faxing resources are not allocated appropriately.	Make sure you do not have more IP fax resources allocated than networking resources.
	Insufficient bandwidth	Run Network Qualifier to determine the bandwidth. For more information about the Network Qualifier, refer to the <i>Network Qualifier Reference Manual</i> , part number 835.2427.
The network is experiencing audio and/or connection problems	There is a port conflict or the firewall, NAT, or router is blocking the port.	Try changing the ports associated with IP call control and/or audio. Make sure none of them conflict with ports that other protocols use (e.g., SIP uses 5060). See Appendices A and B for network configuration guidelines.
	Improper configuration of IP connections, firewall and/or network address translation.	See Appendices A and B for network configuration guidelines.
	Insufficient bandwidth	Run Network Qualifier to determine the bandwidth. For more information about the Network Qualifier, refer to the <i>Network Qualifier Reference Manual</i> , part number 835.2427.

Table 17-22. IP Networking Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
Echo is heard (half-duplex)	Noise levels are too high.	Talk at a lower volume while on a call.
	Callers are talking at the same time (doubletalk).	When simultaneous and similar audio on both sides of the call is detected, the application may try to cancel this perceived "echo," causing audio and echo problems. Try to avoid doubletalk.
	The data network does not meet the minimum specifications required for IP networking.	Run the Network Qualifier to assess your data network. Then verify that your data network meets the minimum specifications. For more information about the Network Qualifier, refer to the <i>Network Qualifier Reference Manual</i> , part number 835.2427.
	The backplane configuration settings (echo settings in particular) are not optimized.	Change the backplane configuration settings. See the "Echo Profiles" on page 10-5 .
Cannot call devices on other nodes after configuring IP Network using the Networking Wizard.	Wrong Off-Node IP Connection IP Address.	Check IP Connection IP Addresses on the local and the remote nodes.
	Missing IP Connection Group or Off-Node IP Connection.	Verify that there's a Node IP Connection Group in the target node's Node Trunk/IP Connection Groups folder. Make sure there's an Off-Node IP Connection in that NIPCG, and verify the IP Address.
	Missing IP Networking Port License(s) or Private Networking software license.	Check the License and software license features for Networking.
	WAN connection is down.	Check your WAN connection.
Cannot call devices on other nodes after configuring T1/E/PRI Networking using the Networking Wizard.	No B-Channels.	Make sure the T1M or T1M-2 module is licensed for PRI, is online, and the appropriate B-Channels are equipped.
	No Reference Clock.	Check reference clock list on this and other nodes. Make sure one node is master for private and the other is slave to private.
	Bad License, no software license features.	Make sure the PRI license is valid.
Cannot import/export to/from new target node after using the Networking Wizard.	Networking is not programmed correctly.	Verify that there's a Node Trunk/IP Connection Group to the remote node.
		Verify that the Node Trunk/IP Connection Group includes the Node Trunk Group or Off-Node IP Connection to the remote node. Depending on the type of programming.
		Refer to the Help file for each programming area.

Table 17-22. *IP Networking Troubleshooting Strategies (Continued)*

Symptom	Possible Cause	Corrective Action
No audio on a call between two IP devices (in the same Network Group) configured to use peer-to-peer audio.	The Network Group is set for peer-to-peer audio, but there is a firewall or NAT in between endpoints.	Verify that there is no firewall or NAT between the two endpoints in the Network Group. See Appendices A and B for network configuration guidelines.
	Improper configuration of IP connections, firewall and/or network address translation	See Appendices A and B for network configuration guidelines.
	A Network Group is programmed to use peer-to-peer audio on one node, but not on another node.	Verify that the Use Peer-to-Peer Audio flag is set to Yes on all nodes.
	A Network Group is not configured to use peer-to-peer audio.	Verify that the Use Peer-to-Peer Audio flag is set to Yes on all nodes.

Licensing Issues

Table 17-23 summarizes troubleshooting strategies recommended for resolving licensing discrepancies.

Table 17-23. *Licensing Troubleshooting Strategies*

Symptom	Possible Cause	Possible Solution
The system resets due to a “Major Reset Due To an IP Endpoint Licensing Error.”	The user has uploaded a software license that causes the number of online Advanced IP endpoints to exceed the number of licensed Advanced IP endpoints.	Mitel recommends <i>not</i> downgrading a software license. Before committing the new license, a message pop-up in DB Programming indicates that the system will reset if the new license is installed.
Alarm 127 appears on the administrator endpoint display and on the Base Server LCD display.	An IP endpoint cannot come online because the appropriate license is not available.	The customer needs to upload a license to support the endpoint model type.
Alarm 130 appears on the Base Server LCD panel display.	A DEI unit is trying to come online but cannot due to the lack of an appropriate software license.	The customer needs to upload a license that supports the use of the particular DEI unit—0 or 1—being installed.

Loop Loss Measurement

Table 17-24 lists troubleshooting information for the Loop Loss Measurement Test feature.

Table 17-24. *Loop Loss Measurement Troubleshooting Issues*

Symptom	Possible Cause	Corrective Action
Results are not consistent with the test equipment.	The fields are not programmed correctly in DB Programming.	Add more test passes to adjust the timing or change the delay in DB Programming.
	The local test number and transmit level of the CO is not the same as what is configured in DB Programming.	Confirm the local test number and transmit level of the CO. Make sure DB Programming matches the CO.

Mini-DSS Unit

Table 17-25 summarizes the troubleshooting strategies recommended for resolving operational discrepancies with Mini-Direct Station Select (Mini-DSS) units.

Table 17-25. Mini-DSS Unit Troubleshooting Strategies

Symptom	Possible Cause	Corrective Action
Mini-DSS Unit inoperative; no LED indication present while button is pressed	Improper installation	Check for loose connections. For more information about hardware connections, refer to the "Installation chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Defective Mini-DSS unit	Replace the Mini-DSS unit.
		Endpoint is identified for endpoint use, not as a Mini-DSS unit. See "Programming DSS Keymaps" on page 7-44 .
	The endpoint is not a Model 8660	Make sure you are using a Model 8660 endpoint.
	The endpoint is not a Model 8520 or 8560	Make sure you are using a Model 8520 or 8560 endpoint
Mini-DSS unit inoperative; LED indication present while button is pressed	Programming error	Endpoint is identified for endpoint use, not as a Mini-DSS unit. See "Programming DSS Keymaps" on page 7-44 .
	Defective Mini-DSS unit	Replace the Mini-DSS unit.
Mini-DSS unit LED indications incorrect	Programming error	Check Mini-DSS button assignments and make sure the endpoint is enabled as a Mini-DSS unit. See "Programming DSS Keymaps" on page 7-44 .
	Defective Mini-DSS unit	Replace the Mini-DSS unit.
	Defective processor module	Replace the module if faulty.
Calls are transferred to the wrong endpoint	User error	Refer to the applicable endpoint user guide for feature instructions.
	Programming error	Check Mini-DSS button assignments. See "Programming DSS Keymaps" on page 7-44 .

Multi-Protocol Endpoints

Table 17-26 summarizes the troubleshooting strategies recommended for resolving discrepancies that may occur with multi-protocol endpoints.

Table 17-26. Multi-Protocol Endpoint Troubleshooting Strategies

Symptom	Possible Cause	Corrective Action
The multi-protocol endpoint powers up and all the lamps remain lit permanently.	The endpoint software is corrupt	<p>The multi-protocol endpoint must be recovered using the following steps:</p> <ol style="list-style-type: none"> 1. Set up a computer on the same LAN as the endpoint. 2. Make sure the computer has a TFTP server and the correct software image file. 3. Rename the software image from 86xx_x_x_x.bin (where the _x_x_x represents the version number) to 86xx.bin. For example: <ul style="list-style-type: none"> — Rename 8600_1_1_5.bin to 8600.bin — Rename 8620_1_1_5.bin to 8620.bin (note that the Models 8620 and 8622 share the same binary image) — Rename 8662_1_1_5.bin to 8662.bin (note that the Models 8622 and 8622 share the same binary image) — Rename 8690_1_1_5.bin to 8690.bin 4. Point the TFTP server at the directory that contains this software image file. 5. Configure the IP address of the computer as 192.168.200.202. The endpoint starts pulling this file from the TFTP server. When finished, the endpoint resets on its own.
<p>The Model 8622 or 8662 endpoints are not uploading new firmware images as specified in the TFTP configuration files.</p> <p>OR</p> <p>The TFTP configuration files have been modified with new image versions, but the Model 8622 or 8662 endpoints have not uploaded the new firmware.</p>	The image strings have not been updated	<p>Make sure that these strings have been updated. For example,</p> <p>From 1.01S, 1.0.31, 1.0.33, or 1.1.5 to 2.0.03:</p> <p>86xx_image_ver: HWID 2.0.03</p> <p>86xx_image_url: 192.168.200.202/86xx/86xx_2_0_03.bin</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>NOTE If upgrading an 8622 from 1.01S to 1.1.5, use the following image string: 8620_image_ver: 8620 HWID 1 1.1.5</p> </div> <p>For future releases (2.0 and later):</p> <p>itphone_image_ver: 2.0.03</p> <p>itphone_image_url: 192.168.200.202/itphone itphone_2_0_03.bin</p>

Table 17-26. Multi-Protocol Endpoint Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
While installing the client application on the Model 8690, an error message indicating that the setup failed appears	The endpoint does not have sufficient memory resources or the endpoint has lost power before the upgrade is complete	The client application installation on the Model 8690 has failed. You must reformat the flash file system on the endpoint.
The Windows CE.Net stops during the firmware upgrade	This may be caused by using most of the system resources (processor and RAM) during an upgrade	<p>Try doing one of the following:</p> <ul style="list-style-type: none"> Restart the Windows CE upgrade by going into Pending Upgrades. Windows CE will still show up as “Pending” because it has not completed copying, which results in a reset of the Model 8690. Press OK to restart the upgrade and eventually this causes the original upgrade time out and displays the dialog box to restart that upgrade. Press No to cancel the original upgrade and continue with the second download that is in progress (usually still erasing flash at this point). Launch the 8690 manually by using a USB mouse. The USB mouse does not require a lot of memory in the CPU. With the USB mouse attached the user can perform some basic functions and still see the Model 8690 endpoint responding. The mouse should be attached before the upgrade is started. <p>NOTE When an upgrade is in progress, avoid using the Model 8690 endpoint.</p>
The Model 8622 or 8662 endpoint flashes the error message ERROR WRONG HWID when attempting to download a new image	The image that the Model 8622 or 8662 endpoint is attempting to download does not support the endpoint's hardware.	Use a more recent image, preferably at or above the version shipped with the endpoint.
A multi-protocol endpoint flashes the error message ERROR WRONG VERSION when attempting to download a new image	The version number in the xxxx_image_ver string may not match up with the image's version.	Correct the xxxx_image_ver image version number or the image name (if pointing at the wrong image file).

Table 17-26. Multi-Protocol Endpoint Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
The Model 8622 endpoint flashes the error message ERROR WRONG VERSION when attempting to download a new image.	The endpoint does not have the latest firmware	<p>The Model 8622 endpoints running firmware version 1.01S displays the error ERROR WRONG VERSION when attempting to download new firmware. To upload to new firmware to the 8622, first use one of the following version strings to upgrade to either versions 1.0.33 or 1.1.5:</p> <p>8620_image_ver: 8620 1.0.33</p> <p>or</p> <p>8620_image_ver: 8620 HWID 1 1.1.5</p> <p>Once the newer firmware has been loaded on the Model 8622 endpoint, change the image version string back to one of the following:</p> <p>8620_image_ver: 1.0.33</p> <p>or</p> <p>8620_image_ver: HWID 1 1.1.5</p> <p>or</p> <p>itphone_image_ver: 2.v.w. (the v.w. indicates the firmware version, such as 2.0.03)</p> <div> <p>NOTE</p> <p>After the firmware has been upgraded, the endpoint will again display the error ERROR WRONG VERSION every time it attempts to upgrade until the configuration version line is returned to the normal state noted above in either the TFTP file or the Web page (i.e., "8620_image_ver: 1.0.33").</p> </div>

Table 17-26. Multi-Protocol Endpoint Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
When the multi-protocol endpoints reset, network connectivity on the downlink (i.e., the LAN port labeled “PC” on the back on the endpoint) is temporarily lost.	<p>The endpoints generally reset for one of the following reasons:</p> <ul style="list-style-type: none"> Endpoint setting or firmware updates - the endpoints may require a reset for certain configuration changes to take place and will reset if the firmware is updated. Telephony system updates - the endpoints will reset when the Call Processing system disconnects their connection for updates on the Call Processing side. The endpoint will continue to reset every several minutes until the telephony system recovers and the endpoint can re-connect. Loss of network connectivity - the endpoints will reset when network congestion or loss of network connectivity prevents necessary keep-alive packets from being exchanged between Call Processing and the endpoint. 	<p>Workarounds for this issue are as follows:</p> <ul style="list-style-type: none"> Minimize endpoint resets due to system updates - Schedule telephony system and endpoint updates for non-peak hours when endpoint and network connectivity outages are less service affecting. Isolate and eliminate any network issues - Isolate and eliminate any network congestion issues that may cause the endpoint to lose communication with Call Processing and thus reset. For critical applications that cannot tolerate any interruptions in LAN service, use an external switch in place of the downlink port for network connectivity until resets due to external factors can be minimized. <p>In the case of (3) loss of network connectivity, make sure that the network in question meets the minimum requirements specified in the <i>Inter-Tel's VoIP Data Network Requirements</i>, part no. 835.2885. You can find the manual on the edGe Online Manuals and Guides Web site (www.inter-tel.com/techpublications).</p>

Network Node

Table 17-27 summarizes the troubleshooting strategies recommended for resolving discrepancies that may occur with a network node.

Table 17-27. Network Node Troubleshooting Chart

Symptom	Possible Cause	Corrective Action
Cannot access an endpoint on another node. Display shows OUTGOING ACCESS DENIED	The endpoint or application making the call does not have outgoing access for the Node Trunk Group that it needs	Program a Node Trunk Group, if one does not exist. Program outgoing access for the endpoint or application. You can use an extension list to make this task easier. See “Extension Lists” on page 8-4 .
Cannot access an endpoint on another node. Display shows DESTINATION UNREACHABLE	There is no IP connection.	For IP networking, make sure you can ping both nodes. For PRI networking, make sure the connection is there and the span is up.
	There is no Node IP Connection Group programmed for the node.	Program a “P8XXX” Node IP Connection Group for the networked nodes. See “Node IP Connection Group” on page 9-22 .
	A single port is busied out on a node.	For example, a system has networked node 1 and node 2. When a single port is busied out on node 1, node 2 will not be notified that the channel has been busied out. That same port must be manually busied out on node 2. For more information about specifying Busy Out commands for ports, refer to the “System Features” chapter in the <i>Mitel 5000 Reference Manual</i> , part number 580.8007.
When calling an endpoint on another node, using the Automated Attendant, calls go directly to voice mail without trying the extension number first	The off-node device is not associated with a mailbox of the same number	Make sure the mailbox is associated with a corresponding extension number. If so, make sure the off-node device exists on the node attached to the external voice processing unit using the Export/Import feature. Then delete the off-node device for the endpoint that was associated with the mailbox and create a new off-node device with a temporary extension. Change the extension number of the temporary off-node device to the extension number associated with the mailbox.
When using a PRI span on another node, calls do not go out properly (e.g., callers hear ringing but there is no answer)	The PRI span does not have the “CO Provides Tones” flag enabled	Enable the CO Provides Tones flag for the span. See “System Flags” on page 10-19 .
Cannot establish an IP connection	NATs/firewalls are present.	See Appendices A and B for network configuration guidelines.
	The IP connection extension for the node is not unique.	Make sure the IP connection extensions (P6XXY) are unique.
	There is no Node IP Connection Group programmed for the node.	Program a “P8XXX” Node IP Connection Group for the networked nodes. See “Node IP Connection Group” on page 9-22 .
	The IP address and subnet mask information for each IPRA is not valid.	Make sure each IPRA has the correct IP address and subnet mask programmed. See the “System IP Settings” on page 9-5 .

Oversubscription/IP Resource-Sharing

Table 17-28 summarizes the troubleshooting strategies recommended for resolving oversubscription, or IP resource-sharing discrepancies.

NOTE

Each IP resource reserved for a particular device or function reduces the amount of resources that can be effectively oversubscribed.

Table 17-28. Oversubscription/IP Resource-Sharing Troubleshooting Strategies

Symptom	Possible Cause	Corrective Action
User cannot make calls from their IP endpoint.	The system attempts to allocate IP resources for each particular call. If IP resources are unavailable, the call will not be completed (including peer-to-peer).	Reserve more IP resources for IP endpoint usage or dedicate IP resources for a particular IP endpoint.
User cannot make IP private networking calls.	The system allocates IP resources for each IP private networking call. If no IP resources are available, the call will not be completed.	Reserve more IP resources for IP private networking usage.
IP endpoint user cannot listen to background music.	Each user must have an allocated IP resource to be able to listen to background music. If no IP resources are available, the user will not hear background music but will camp on for the IP resources.	Reserve more IP resources for IP endpoint usage or dedicate IP resources for a particular IP endpoint.
IP endpoint user cannot hear a page.	If an IP endpoint cannot acquire the IP resources required for a page, the user will not hear the page.	Reserve more IP resources for IP endpoint usage or dedicate IP resources for a particular IP endpoint.
IP endpoint user does not receive any calls even though their endpoint is not busy.	In order for an IP endpoint to ring, it must first be allocated the required IP resources for the call. If no resources are available, the IP endpoint camps on and does not ring until resources become available.	Reserve more IP resources for IP endpoint usage or dedicate IP resources for a particular IP endpoint.
User cannot make IP networking calls even when IP private networking resources are available.	The number of networking calls is limited by the number of IP private networking channels in the license.	Upgrade the IP private networking portion of the license.

Persistent Music-On-Hold Selection

Table 17-29 contains troubleshooting information for Music-On-Hold for Call Routing Tables.

Table 17-29. *Persistent Music-On-Hold Troubleshooting Issues*

SYMPTOM	POSSIBLE CAUSE	CORRECTIVE ACTION
No Music-On-Hold (external music source connected).	The external music source is turned off or inoperative.	Check the external music source for proper operation.
	There is a programming error.	Make sure the following fields are programmed correctly: <ul style="list-style-type: none">• Music-On-Hold settings for CO Trunk Groups• Music-On-Hold Profiles for CRTs
	There is a defective cable between the music source and the Music-On-Hold port on the back of the chassis.	Repair or replace the cable. Check to see that a 1/8-inch, 2-conductor (mono), mini-phone plug was used.
	There is a defective Music-On-Hold port.	Replace the defective chassis.

Phantom Devices

Table 17-30 summarizes the troubleshooting strategies recommended for resolving discrepancies with phantom devices.

Table 17-30. Phantom Devices Troubleshooting Strategies

Symptom	Possible Cause	Corrective Action
Endpoint displays INVALID FEATURE CODE and DND does not disable.	The user accessed remote programming to take a phantom out of DND.	As designed, a phantom device cannot be taken out of DND.
Endpoint displays INVALID EXTENSION NUMBER and swap endpoint fails.	An endpoint administrator accessed the swap endpoint operation for a phantom device.	As designed, a phantom device cannot swap endpoints because it does not have a physical hardware address.
When an endpoint administrator is scrolling through a list of endpoints, the endpoint displays CIRCUIT NONE.	An administrator is accessing administrator features for a phantom device.	As designed, there is no device number for a phantom device because it does not have a hardware address.
A phantom cannot forward to the public network.	A phantom does not have access to forward to the public network.	Enable the phantom's Manual Forward to Public Network flag.
	The phantom is not in the CO trunk group's outgoing access list.	Assign the phantom's outgoing extension to the corresponding outside access CO trunk group.
A phantom cannot forward off-node.	The phantom is not in the node trunk group's outgoing access list or node IP connection group.	Assign the phantom's outgoing extension to the corresponding outside access node trunk group or IP connection group.
	The local node does not recognize the off-node device.	Create the off-node device on the local node.
A phantom hunt group member cannot forward to the public network.	Like other forwarded endpoints, hunt group members cannot forward to the public network.	Phantom hunt group members cannot forward to the public network.
When adding more phantoms, the system slows down.	Adding too many phantoms in the current database configuration. Phantoms, though they do not use physical hardware, still use similar processor resources as a physical endpoint.	Remove some phantoms from the system.
Mitel 5000 v2.1 (or Axxess v9.x) or earlier nodes cannot call a Mitel 5000 v2.2 phantom.	The off-node device for the phantom does not exist on the earlier node.	On the earlier node, create an off-node device for the Mitel 5000 v2.2 phantom extension. This will allow the older node to recognize the phantom extension and call it.

Table 17-30. *Phantom Devices Troubleshooting Strategies (Continued)*

Symptom	Possible Cause	Corrective Action
The user cannot add more phantoms.	The default phantom value is too low for the current system.	<p>If additional phantoms are necessary, Mitel recommends increasing the phantoms value in Online Monitor (OLM) mode so the combined TDM/IP devices and the phantoms value does not exceed the system's license capacity. There are three ways to tell how many devices you have in your system:</p> <ol style="list-style-type: none"> 1) Dump the System Device Information to Message Print via an administrator endpoint. 2) Use Diagnostics Monitor/System Monitor (v3.2.1 or later) to dump the System Device Information. 3) Use DB Studio to view the System Device Information (View/System Device Information). <p>If the system needs more phantoms that the system's licensable capacity, contact Mitel Technical Support.</p> <p>The system may run slower by increasing the default phantom value.</p> <div> <div>NOTE</div> <div>Do not use OLM mode unless you are instructed to do so by Mitel support personnel.</div> </div>

Processor Module (PM-1)

To determine extent of catastrophic hard drive error:

1. Set up a RS-232 connection or keyboard/monitor connection and reset the PS-1.
2. Capture the power-up events and determine if the PS-1 is able boot up.
 - a. If the PS-1 offers a log-in account, this is not a catastrophic hard drive error. In this situation, Mitel may need remote access to log into the PS-1 to diagnose the problem further.
 - b. If the PS-1 does not offer a log-in account, this may be a catastrophic hard drive error. Send the power-up events to Mitel before proceeding any further.
3. With assistance from Mitel Technical Support, create an PS-1 recovery CD by using an “ISO” image, or Mitel Technical Support can provide a PS-1 recovery CD.
4. With authorization and guidance from Mitel Technical Support, place the PS-1 recovery CD into the PS-1 optical drive and reset the system.
5. Use an RS-232 connection or keyboard-and-monitor connection to confirm that the installation wiped the previous contents from the PS-1 hard drive and reformatted it based on the CD contents.

Table 17-31 summarizes the troubleshooting strategies recommended for resolving Processor Module (PM-1) discrepancies.

Table 17-31. *Processor Module (PM1) Modem Troubleshooting Strategies*

Symptom	Possible Cause	Corrective Action
Users cannot connect to the modem	The Force Minimum Bit Rate flag is enabled, and the connection speed is below the specified minimum.	Disable the Force Minimum Bit Rate flag.
	Poor line quality or other external factors are affecting the connection rate.	Set the Minimum Bit Rate field to 9600 or lower.
An incoming CO call is disconnected when the modem is disabled.	The primary attendant endpoint is not set.	Make sure the primary attendant endpoint is set in the Endpoint-Related Information field so that the call is sent to the attendant when the modem is disabled.

Processing Server (PS-1)

Table 17-32 summarizes the troubleshooting strategies recommended for resolving PS-1 operational discrepancies.

Table 17-32. Processing Server Troubleshooting Strategies

Symptom	Possible Cause	Corrective Action
The PS-1 does not connect with the Base Server	Software version mismatch.	Ensure that both the Base Server and the PS-1 are running the same release of v2.x software and that they comply with the requirements identified in the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	The Base Server is not running in Gateway mode.	Use the LCD panel to configure the Base Server in Gateway mode.
	The PS-1 does not have the Base Server connection IP address.	Log into DB Programming on the PS-1 and configure the Base Server connection IP address in <i>both</i> of the following folders: <ul style="list-style-type: none"> System\IP Settings\Base Server IP Settings System\IP Settings\Base Server/Processing Server Connection Settings
	The PS-1–Base Server connection IP address does not match the Base Server address.	Verify that the Base Server is using a static IP address. If the Base Server is using DHCP, a new IP address may prevent a successful PS-1–Base Server connection.
	The PS-1 and Base Server do not have the same password and/or port number.	The CP system log file can be used to determine which port the PS-1–Base Server is using for the connection. This information resides in the latest /usr/local/intl/etc/cp/cp_system_log*. file. Configure the PS-1 password/port numbers in OLM on the PS-1 and the Base Server or in DB Programming.
The PS-1 and Base Server lose communication.	Something prevents the PS-1 and Base Server from communicating with each other.	Ensure that the PS-1 and Base Server are configured on the same switch.
	The PS-1–Base Server connection IP address does not match the Base Server IP address.	Use the PS-1 diagnostics to determine when/if the system started having packet loss. Attempt to associate this with a network impairment issue or a condition where the physical LAN connection was either moved or unplugged.
The PS-1 does not boot up or function due to a catastrophic hard drive error.	The PS-1 hard drive may be severely corrupted.	To determine the extent of the problem, perform the steps in paragraph 10.4.

Retry ARS Call If Call Rejected

Table 17-33 summarizes troubleshooting strategies recommended for resolving discrepancies related to the Retry ARS Call If Call Rejected feature.

Table 17-33. *Retry ARS Call If Call Rejected Troubleshooting Strategies*

Symptom	Possible Cause	Corrective Action
An ARS-routed ISDN call rejected by the local telco causes the system to cycle through all the ISDN channels before disconnecting.	The Retry ARS Call If Call Rejected flag is set to No in DB Programming.	From the DB Studio main screen go to System – Communication Server – Bay n: <BRM-S; T1/PRI; E1/PRI> and set the flag to Yes .
	The Retry ARS Call If Call Rejected flag is set to Yes , but the cause for rejection by the telco is other than those listed in the feature options. For more information, refer to the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.	Verify that the number dialed is correct and valid. Try calling the rejected number from another endpoint.


Scheduled Backups – Warnings and Error/Failure Reasons

The following types of events are recorded in the Event Viewer or the Session Manager Scheduled Backups Summary:

- “[Information](#)” below
- “[Warning](#)” below
- “Error/Failure” on [page 17-60](#)

Information

When a Scheduled Backup completes successfully, the following event is recorded in the Event Viewer.


 Information 11/7/2008 10:19:59 PM CS5000 ...

Descriptions:

Scheduled backup for <session name> completed successfully.

Warning

When a Scheduled Backup does not complete successfully, the following event is recorded in the Event Viewer or the Session Manager Scheduled Backups Summary.

 Warning 11/7/2008 10:19:59 PM CS5000 ...

Descriptions:

- “[Voice Data Backup Failed](#)” below
- “Scheduled Backup Delayed” on [page 17-60](#)
- “Retry Scheduled” on [page 17-60](#)
- “Warning Recorded” on [page 17-60](#)
- “Scheduled Backup Is Not Yet Complete” on [page 17-60](#)—displayed in the Session Manager Scheduled Backups Summary only

Voice Data Backup Failed

This warning description is recorded when the system database save completes successfully, but the voice data save does not complete successfully.

Scheduled backup for <session name> completed successfully only for the system database. The voice data backup failed: <reason>.

Table 17-34 shows various Voice Data Backup Failed reasons and troubleshooting tips.

Table 17-34. Voice Data Backup Failed Reasons

Warning Message	Possible Cause	Corrective Action
"The Voice Data Path is empty."	There is a problem with the registry. The Voice Data Path cannot be empty to save voice data.	Type the proper path in the Location tab.
"The Voice Data Path is invalid."	A character in the path is either invalid, does not exist, is not accessible, is read-only, or in use.	Verify that the path is valid in the "Location Tab" on page 3-19 .
"The Voice Data Hostname is empty."	When saving voice data in PS-BVM, the host name must be included in the Voice Data Path.	Type \\<host name>\<path> in the Path box in the "Location Tab" on page 3-19 .
"The Voice Data Hostname is invalid."	A character in the host name is invalid, the host name cannot be found, or the host is not accessible or online.	Verify that the host name is properly programmed in the Path box in the "Location Tab" on page 3-19 , and that the indicated server is accessible and online
"The drive indicated in the Voice Data Path is not ready."	The storage media is missing from the drive or the drive is malfunctioning.	Make sure the storage media is in place and that the drive is functioning properly.
"The Voice Data Path points to a removable drive requiring a user to insert multiple disks. Because a user is not typically present to insert disks, this is supported for Scheduled Backups."	A floppy drive cannot be used for Scheduled Backups.	Make sure the path points to a drive that can hold all of the data.
"A write error occurred when attempting to save voice data."	An exception occurred while writing to the media. There may be a problem with the server or drive.	Resolve the problem if possible, and verify that you can write to the server/drive manually. If this problem persists, contact Technical Support.
"Voice data cannot be saved because the object specified in the Voice Data Path is in use."	The destination media is busy.	Resolve the problem if possible, and verify that you can write to the server/drive manually. If this problem persists, contact Technical Support.

Table 17-34. Voice Data Backup Failed Reasons (Continued)

Warning Message	Possible Cause	Corrective Action
(Exception) <description>	An unhandled exception occurred during the save of the voice data. The <description> of the exception is provided by Microsoft Windows.	Contact Technical Support.

Scheduled Backup Delayed

This warning description is recorded whenever a Scheduled Backup is delayed due to too many simultaneous backup sessions.

```
Scheduled backup for <session name> has been delayed due to  
simultaneous sessions limit.
```

Retry Scheduled

This warning description indicates that a Scheduled Backup has failed and the system will attempt a retry. The backup is logged as a warning until the last retry. If the last retry attempt fails, it will be logged as a failure.

```
Scheduled backup for <session name> failed, but a retry has been  
scheduled for HH:MM AM/PM. DETAILS: <error message>.
```

Warning Recorded

This warning description is recorded when a discrepancy is detected during a backup. A discrepancy could be something regarding extension conflicts in DB Programming, a hardware connection problem, etc. Monitor the Service Log to identify the problem.

```
Scheduled backup for <session name> completed successfully, but  
warnings were recorded. DETAILS: See Service Log.
```

Scheduled Backup Is Not Yet Complete

This warning description indicates that the scheduled backup is still in progress. It may also indicate that the computer rebooted during the backup and the backup failed to complete. This warning is recorded only in the Session Manager Scheduled Backups Summary. If the computer reboots during a scheduled backup, this is the only warning indication. There is no event log posting, no e-mail is sent, and a retry is not scheduled.

```
The Scheduled Backup is not yet complete.
```

Error/Failure

Whenever attempted backups fail or the last retry attempt fails, the following event is recorded in the Event Viewer or the Session Manager Scheduled Backups Summary.

```
❌ Error 11/7/2008 10:19:59 PM CS5000 ...
```

Descriptions:

```
Scheduled backup for <session name> failed: <reason>.
```


Table 17-35. Error/Failure Reasons and Troubleshooting Tips (Continued)

Error Message	Possible Cause	Corrective Action
"Unable to locate the database file."	The database schema file is missing.	Reinstall DB Programming.
"Unable to copy empty database for remote session. The disk may be full or the remote directory path may be invalid."	The message is self-explanatory.	Make sure the file is accessible, not read-only, and not in use. If necessary, reinstall DB Programming.
"Unable to copy database schema. The disk may be full, the file may be locked, or the local directory path may be invalid."	The message is self-explanatory.	Make sure the file is accessible, not read-only, and not in use. If necessary, reinstall DB Programming.
"Unable to locate the database schema file."	The registry is corrupted.	Reprogram the IP address or host name for the session in the Session Manager, and then try again.
"Unable to locate session information for <session name>."	The session no longer exists. This can only happen if you manually alter the registry, deleting or renaming a session, or if you edit a Scheduled Backup task in the Windows Task Scheduler.	Delete the task from the Windows Task Scheduler, or reprogram the session. If this problem persists, contact Technical Support.
"Could not write file to <path>."	The path is invalid, inaccessible, unavailable, or read-only.	Make sure the path is correct, that you have access to the path, and that it is not read-only or in use. If this problem persists, contact Technical Support.
"Archive of database file to <path> failed."	The last step of the database save failed. It could not be inserted into an archive.	Make sure the path is correct, that you have access to the path, and that it is not read-only or in use. If this problem persists, contact Technical Support.
"Could not open file <path>."	The path is invalid, inaccessible, unavailable, or read-only.	Make sure the path is correct, that you have access to the path, and that it is not read-only or in use. If this problem persists, contact Technical Support.
"The Save system database to folder plus filename is too long. The limit for the length is 60 characters."	The path to a system database save file must be 60 characters or less. To allow for the 17-character file name: YYYYMMDDHHMM.intl, the folder name must be less than 43 characters.	Change the destination folder for the system database in the Save system database to folder box so that it is less than 43 characters.

Table 17-35. Error/Failure Reasons and Troubleshooting Tips (Continued)

Error Message	Possible Cause	Corrective Action
"Could not write to or remove file <path>. (Exception = <description>)"	An exception occurred when trying to overwrite or write to the path.	Make sure you have access to the path, and that it is not read-only or in use. If this problem persists, contact Technical Support.
"Could not initiate the session due to not enough memory."	There is a serious shortage of memory on the computer.	Try resetting the computer. If this problem persists, contact Technical Support.
"Unable to read database path from registry."	Installation information in the registry is corrupted.	Reinstall DB Programming. If the problem persists, contact Technical Support.
"Unable to read session path from registry."		
"Unable to update startup data in registry."	Session information in the registry is corrupted.	Contact Technical Support.
"Unable to read session data from registry."		
"Unrecognized product type and/or version in database. Contact Technical Support."	There is a problem with the database itself.	Try restoring a recent backup to the system. If none is available or this does not solve the problem, contact Technical Support.
"Unable to locate the language database <path>."	The language database is missing for this DB Programming version.	Reinstall DB Programming.
"Unable to locate the flavor database <path>."	The flavor package database is missing for the DB Programming version.	Reinstall DB Programming.
"Needed Voice Processor information is missing from the database. Restore the last saved database, or use DBTest to repair this database. You may need to Contact Technical Support."	There is a problem with the database.	Restore the last saved database, or use DB Test to repair this database. If this problem persists, contact Technical Support.
"The CP node for the connection has been programmed to have a Voice Processor attached. The connection to the Voice Processor has failed. This must be resolved before this service mode task can complete successfully."	The message is self-explanatory.	Manually resolve the problem with the Voice Processor connection, or manually start up DB Programming to indicate that you wish to run DB Programming without a Voice Processor connected. After performing either of the above, the backup should complete. If the Voice Processor is disconnected, voice data is saved.

Table 17-35. Error/Failure Reasons and Troubleshooting Tips (Continued)

Error Message	Possible Cause	Corrective Action
"You are attempting to connect with a system that is not a Mitel 5000 product. To connect with this system, please use the appropriate Session Manager."	The message is self-explanatory.	Verify that the IP address or host name programmed for the session in the Session Manager is correct. Make sure it matches the system to which you are trying to connect.
"Unable to locate the session database."	You have attempted to run DB Programming via command line.	Do not run DB Programming via command line. If you have not attempted to run DB Programming via command line and you get this error, contact Technical Support.
(Exception) <description>	An unhandled exception occurred during the save of the voice data. The <description> of the exception is provided by Microsoft Windows.	If it is not obvious what to do from the description, contact Technical Support.

Scheduled Backups – Error Messages

This section summarizes the troubleshooting strategies recommended for resolving scheduled backups programming issues and discrepancies.

Table 17-36 shows possible programming error messages and troubleshooting tips for Scheduled Backups. If the following information does not address the concern, see [page 17-65](#) for additional troubleshooting tips.

Table 17-36. *Scheduled Backups Error Messages and Troubleshooting Tips*

Error Message	Possible Cause	Corrective Action
General Error Messages		
"Unable to schedule backups: <i>reason</i> . If this problem persists, contact Technical Support."	As described in "reason."	Resolve the problem if possible. If this problem persists, contact Technical Support.
"You have made changes that are not yet saved. Are you sure you want to close this dialog without saving changes?"	Some changes have not been saved.	None. Click Yes to continue (cancelling all unsaved changes) or No to return to the Scheduled Backups dialog box.
"You have changed the Scheduled Backups configuration but have not scheduled a test. Would you like to schedule a test of the Scheduled Backup configuration?"	You have not scheduled a Scheduled Backup configuration test.	Go to the Test tab and schedule a test.
"You have changed the Scheduled Backups configuration but have not scheduled a test. Would you like to schedule a test of the Scheduled Backup configuration?"	You have not scheduled a Scheduled Backup configuration test.	Go to the Test tab and schedule a test.
Scheduling Tab (see page 3-25)		
"Invalid monthly schedule. At least one month must be checked."	A month not selected.	Select at least one month.
"Invalid monthly schedule. The day of the month does not occur in one or more of the months specified."	The selected day (date) is invalid for any of the selected months.	Select a valid day (date) of the months.
"Invalid weekly schedule. Week frequency must be greater than zero."	Zero is not a valid number.	Type a different number (up to 99).
"Invalid weekly schedule. At least one day must be checked."	A day of the week not selected.	Select at least one day.

Table 17-36. Scheduled Backups Error Messages and Troubleshooting Tips (Continued)

Error Message	Possible Cause	Corrective Action
"Invalid daily schedule. Day frequency must be greater than zero."	Zero is not a valid number.	Type a different number (up to 999).
Location Tab (see page 3-19)		
"You have changed the Scheduled Backups configuration but have not scheduled a test. Would you like to schedule a test of the Scheduled Backup configuration?"	You have not scheduled a Scheduled Backup configuration test.	Go to the Test tab and schedule a test.
"The Save system database to folder is not unique. You must enter a folder that is different from that assigned to any other session."	Two sessions have the same folder path name.	Change one of the sessions with a different folder path name.
"You must enter a Save system database to folder."	The Save system database to folder box is blank.	Type the folder name.
"The Save system database to folder is invalid."	The folder name is invalid.	Type the valid folder name.
"There might not be enough space on the chosen drive to hold the system database file. Please free up at least 50 MB or choose a different drive for the Save system database to folder."	The folder specified is on a drive that has less than 50 MB available.	Select a different drive.
"To save voice data, you must enter a Path."	The Path box is blank.	Type the valid path in the Path box.
"The voice data Path is invalid."	The Path holds an invalid folder name.	Type the valid folder name in the Path box.
Authorization Tab (see page 3-23)		
"You must enter a Username."	The Username box is blank.	Type the valid user name in the Username box.
"You must enter a Password for the Username."	The Password box is blank.	Type the valid password in the Password box.
Notification Tab (see page 3-24)		
"You must enter at least one Recipient."	The Recipient(s) box is blank.	Type one or more recipients. Or, disable E-mail Notification.
"You must enter a Server/Port Number."	The Server or Port Number box is blank.	Type the server or port number. Or, disable E-mail Notification.

Table 17-36. *Scheduled Backups Error Messages and Troubleshooting Tips (Continued)*

Error Message	Possible Cause	Corrective Action
"You have changed Notification parameters, but you have not sent a test message. Click OK to continue, or Cancel to remain on the Notification tab and send a test message"	You have not sent a test message to verify that the Notification programming is valid.	Click Send Test Message to test the changes.
"Unable to send e-mail: <i>reason</i> ."	There is a problem sending the message.	Address the problem before Notification can work properly.
Test Tab (see page 3-27)		
"Unable to schedule a test of Scheduled Backup configuration: < <i>error message</i> >. If you cannot resolve this issue and this problem persists, contact Technical Support."	As described in the error message.	Follow the directions in the error message. If this problem persists, contact Technical Support.

Scheduled Backups – General Troubleshooting Tips

Table 17-37 summarizes the troubleshooting strategies recommended for resolving scheduled backups discrepancies.

Table 17-37. Scheduled Backups Troubleshooting Tips

Symptom	Possible Cause	Corrective Action
Scheduled Backup E-mail notification was not received when expected.	E-mail Notification is not enabled.	Make sure the Notification Enabled check box is selected (see “Notification Tab” on page 3-24). Also check to see if the Notify only when Scheduled Backups fail to complete check box is selected. When selected, you receive an e-mail notification only when backups fail.
	Notification parameters are not properly programmed.	Type the correct server and address (see “Notification Tab” on page 3-24). Click the Send Test Message button to send a test message, and verify success status is returned and that the e-mail message is received. If the test fails, take corrective action (see below).
	There is a problem with the e-mail server at either end. (Determine this by trying to send e-mail manually from the DB Programming computer to the programmed server and address.)	Troubleshoot internet connection and e-mail server at both ends. Contact Technical Support if needed.
	The DB Programming computer was powered down.	Make sure the DB Programming computer is always powered up whenever backups are scheduled.
No Scheduled Backup event was posted in the Windows Event Log when expected.	The DB Programming computer was powered down.	Make sure the DB Programming computer is always powered up whenever backups are scheduled.
	A component needed for event logging is missing.	Reinstall DB Programming.
Backups keep failing because they run too slow or long.	There are too many simultaneous sessions allowed, and too many are running at once. The interaction is too slow, or because they simply take too long due to decreased bandwidth per session.	Reduce the number of Simultaneous sessions allowed (see “Setting Scheduled Backups for All Sessions” on page 3-30).

Table 17-37. Scheduled Backups Troubleshooting Tips (Continued)

Symptom	Possible Cause	Corrective Action
Backups keep failing because they run too slow or long.	There are too many simultaneous sessions allowed, and too many are running at once.	Reduce the number of Simultaneous sessions allowed (see “Setting Scheduled Backups for All Sessions” on page 3-30).
	The interaction is taking too long due to decreased bandwidth per session.	
	The Time before Retry value programmed is too short.	Increase this parameter to an appropriate value (see “Setting Scheduled Backups for All Sessions” on page 3-30).
Backup files are not found where expected.	The Save system database to folder box is not programmed correctly.	Type the correct path (see “Location Tab” on page 3-19).
	Scheduled Backups programming is not configured correctly.	Verify that the backup took place by checking e-mail notification, the Windows Event Log, and the Service Log (see “Scheduled Backup Diagnostic Logs” on page 3-31). If the backup did not take place, verify that the backups are scheduled correctly (see “Scheduling Tab” on page 3-25).
	The programmed Username does not have permission to write to the programmed location.	Verify that the Username programmed, has access to the backup save location (see “Authorization Tab” on page 3-23). If not, give the Username access or program a different Username to be used that does have access. See “Error/Failure Reasons and Troubleshooting Tips” on page 17-61 for various reasons for failures.

Single Line Endpoints

Table 17-38 summarizes the troubleshooting strategies recommended for resolving discrepancies occurring with single line endpoints.

Table 17-38. *Single Line Endpoint Troubleshooting Strategies*

Symptom	Possible Cause	Corrective Action
Single line endpoint does not work	Defective endpoint	Replace the single line endpoint.
	Defective cabling	Check the endpoint and system cabling. For more information about hardware connections, refer to the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Defective SLA	Replace the associated SLA.
	Defective Digital Endpoint Module (DEM-16)	Replace the associated module.
	Defective processor module	Replace the module if faulty.
	Defective onboard single line ports	Replace the chassis.
Single line endpoint does not work; talk battery present	Defective set	Replace the single line endpoint.
	Defective DEM-16 or Single Line Module	Replace the associated defective module.
	Defective processor module	Replace the module if faulty.
	Defective onboard single line ports	Replace the chassis.
Single line endpoint does not work; calls ring in; talk battery is present	Defective endpoint	Replace the single line endpoint.
	Defective SLA	Replace the associated SLA.
	Defective digital endpoint module	Replace the associated module
	Defective processor module	Replace the module if faulty.
	Defective onboard single line ports	Replace the chassis.
A group of single line endpoints is inoperative; all are on the same SLA or the T1M or T1M-2 expansion module	Defective cabling	Ensure connector or cable is securely attached to the SLA or the T1M or T1M-2 expansion module.
	Defective SLA, T1M, or T1M-2 expansion module	Replace the module.
Single line endpoint will not ring for CO or intercom calls; talk battery is present; calls can be placed	Single line endpoint ring jumper strap not set for correct ringing	Set the ring jumper strap of the single line endpoint for AC ringing. For more information, refer to the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Defective endpoint	Replace the endpoint.
	Defective SLA	Replace the associated SLA.
	Defective digital endpoint module	Replace the associated module.
	Defective processor module	Replace the module if faulty.
	Defective onboard single line ports	Replace the chassis.

Table 17-38. Single Line Endpoint Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
Ring trip is not provided to a group of single line endpoints; outgoing calls are not affected	Defective cabling of the onboard single line ports.	Using a voltmeter, measure the input at the block. For more information, refer to the "Installation" chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Proper voltage absent from SLA.	Defective connection or incorrect installation of SLA. Using a voltmeter, measure the voltage at the digital expansion block. For more information, refer to the "Installation" chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Proper voltage absent from digital endpoint module	Defective connection or incorrect installation of the digital endpoint module. Using a voltmeter, measure the voltage at the digital block.
	Defective digital module	Replace the associated module.
A group of AC ringer-equipped single-line sets will not ring for CO or intercom calls; talk battery is present; calls can be placed; all endpoints are on the same SLA or digital endpoint module	Defective SLA	Replace the associated SLA.
	Defective digital endpoint module	Replace the associated module.
	Defective processor module	Replace the module if faulty.
	Programming error	Make sure the Extended Ring Cadence flag is enabled.
No AC ringer-equipped single line endpoint rings for CO or intercom calls; talk battery present; calls can be placed	Defective processor module	Replace the module if faulty.
	Defective digital endpoint module	Replace the associated module.
	Defective SLA	Replace the associated SLA.
	Programming error	Make sure the Extended Ring Cadence flag is enabled.
	Either a DTMF decoder, voice channel, or tone generator is not available	Single line endpoint user will hear busy tones when any of the necessary resources are not available. User may camp on.
Cannot obtain intercom dial tone; no sound is heard	Defective set	Replace the single line endpoint.
	Defective SLA	Replace the associated SLA
	Defective digital endpoint module	Replace the associated digital endpoint module.
	Defective processor module	Replace the module if faulty.
Cannot place intercom call; dial tone present, but reorder tone heard	User error	Try the call again. User may have dialed an invalid number.
	Defective set	Replace the single-line set.
	Defective processor module	Replace the module if faulty.
Cannot break CO dial tone	Defective endpoint	Replace the single line endpoint.
	Defective SLA	Replace the associated SLA.
	Defective digital endpoint module	Replace the associated digital endpoint module.
	Defective processor module	Replace the module if faulty.
	Defective onboard single line ports	Replace the chassis.

NOTE

See also CO trunk problems.

Chapter 17: Troubleshooting

Single Line Endpoints

Table 17-38. Single Line Endpoint Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
Cannot place off-hook voice announce calls	Programming error	Ensure that the system option for off-hook voice announce is enabled that the endpoint is programmed to transmit OHVA calls. Also, Ensure the Ring Intercom Always feature is disabled.
	User error	Called endpoint is a single-line set or an endpoint that is not equipped with a secondary voice path.
	Defective processor module	Replace the module if faulty.
Single line endpoints not receiving audio message waiting indications	Programming error	Audible Message indication for SL Sets flag must be enabled in the database. See the “System Flags” on page 10-19 chapter.
Audio distortion. Talker and/or listener hears brief, noticeable changes in volume that do not sound normal.	Some analog single line endpoints transmit at abnormally high levels.	Use an analog single line endpoint that meets industry-standard transmit levels.
	The talker may be speaking loudly.	Reduce the volume of the incoming audio.
Single-line set does not receive caller ID information.	Single line endpoint flags may be programmed incorrectly in DB programming.	Set the Caller ID-IC and Extended Ring Cadence flags to Yes .
	The single line device may not support the shortened number of an extension.	Replace the device with a single-line device that supports the shortened number of an extension number and the split ring of an IC call.
	The single line device may stop collecting data at the second IC ring burst.	

System Health Report

Table 17-39 lists troubleshooting information for the System Health Report feature.

Table 17-39. System Health Report Troubleshooting Issues

Symptom	Possible Cause	Corrective Action
Email message are never sent by the Mitel 5000 system.	The feature is not enabled in the license.	Enable the feature in the system license.
	The system is not configured to send status emails.	Configure the feature in DB Programming.
	The e-mail gateway is not configured.	Configure the e-mail gateway in DB Programming.
Email messages are sent by the system, but are not received by the recipient. This is evident in the error messages of the /var/log/mail.mainlog showing that e-mails were rejected,	The Mitel 5000 does not have outgoing network access.	Configure the customer's network to allow the 5000 to send status emails to the recipient.
	The e-mail gateway is not configured to relay the Mitel 5000 e-mail.	Configure the e-mail gateway to allow relaying the Mitel 5000 e-mail.

System Features

Table 17-40 summarizes the troubleshooting strategies recommended for resolving system features discrepancies.

Table 17-40. System Features Troubleshooting Strategies

Symptom	Possible Cause	Corrective Action
Feature does not work correctly	User error	Refer to the applicable endpoint user guide for feature instructions. Also, ensure that the feature is available on the software package installed.
	Programming error	Check feature code programming. Also, check user-programmable feature key programming.
	Defective endpoint	Replace the endpoint and/or perform the endpoint self-test as described in the "Installation" chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Defective digital endpoint module	Replace the associated module.
	Defective processor module	Replace the module if faulty.
Cannot transfer CO or intercom calls to other endpoints	User error (for example, wrong feature code)	Refer to the applicable endpoint user guide for feature instructions
	Called endpoint is in Do-Not-Disturb	An endpoint in Do-Not-Disturb cannot receive transferred calls.
Cannot transfer calls to outside numbers	User error (e.g., wrong feature code)	Refer to the applicable endpoint user guide for feature instructions
	Programming error	Check trunk access and toll restriction.
	Defective processor module	Replace the module if faulty.

Table 17-40. System Features Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
Cannot transfer incoming CO calls or place them on hold	User error	Refer to the applicable endpoint user guide for feature instructions.
	User error (trunk button being pressed after initial connection is made)	Set the CO Reseize timer to a higher value. Default value is 3 seconds. Or, program the endpoint to disallow CO Reseize. See “Timers and Limits” on page 10-24 and “Endpoint Flags” on page 7-22 .
	Programming error	Check user-programmable feature button programming.
Cannot initiate a conference	User error	Refer to the applicable endpoint user guide for feature instructions.
	System capacity exceeded	See the maximum system capacities in the “Specifications” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Defective endpoint	Replace the endpoint and/or perform the endpoint self-test as described in the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Defective digital endpoint module	Replace the associated digital endpoint module.
	Defective processor module	Replace the module if faulty.
Last number redial feature inoperative	User error	For feature information, refer to the “System Features” chapter in the <i>Mitel 5000 Reference Manual</i> , part number 580.8007. Endpoint may be programmed for last number saved.
	System speed-dial number identified as non-display	A System Speed Dial number identified as non-display cannot be redialed.
	Defective endpoint	Replace the endpoint and/or perform the endpoint self-test as described in the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Defective processor module	Replace the module if faulty.
Cannot initiate a page	User error	Refer to the applicable endpoint user guide for feature instructions.
	All endpoints in the paging zone are busy, or a voice channel is not available	Reorder tone is heard. Wait several seconds and then attempt to place the page again. Paging requires a voice channel.
	All endpoints in the paging zone are in Do-Not-Disturb	Reorder tone is heard if all endpoints in the zone are in Do-Not-Disturb and if external paging for the zone is disabled.
	No endpoints are programmed to receive pages	Reorder tone is heard. Check paging assignment. See “Page Zones” on page 10-15 .
	Defective endpoint	Replace the endpoint and/or perform the endpoint self-test as described in the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Defective processor module	Replace the module if faulty.

Table 17-40. System Features Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
House Phone is not working properly or is inoperative	User error	Incoming calls take precedence over outgoing calls. For more information, refer to the “System Features” chapter in the <i>Mitel 5000 Reference Manual</i> , part number 580.8007.
	Programming error (data base)	Ensure that the endpoint is designated as a House Phone. Also, make sure the endpoint has been assigned the correct COS and trunk access. See “Programming Endpoint Options” on page 7-50 .
	Programming error (data base or speed-dial)	Ensure that the correct numbers are in appropriate day number and night number (Speed Dial) locations.
Cannot initiate a call forward	User error	Refer to the applicable endpoint user guide for feature instructions.
	User attempting illegal forward	Endpoints are not allowed to set call forward if it forms an unconditional loop, the receiving endpoint is in Do-Not-Disturb, or an invalid intercom number is dialed. COS and outgoing access are checked when a call is forwarded to an outside telephone number. Also, ARS cannot be used to forward to an outside number.
	Defective endpoint	Replace the endpoint and/or perform the endpoint self-test as described in the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Defective processor module	Replace the module if faulty.
Calls will not forward	User error	Refer to the applicable endpoint user guide for feature instructions.
	Illegal forward	Conditional forwards (e.g., if busy, if unanswered) may form an undetected loop. If a call forward request forms a conditional loop, the call returns to the first endpoint.
	Defective digital endpoint module	Replace the associated module.
	Defective processor module	Replace the module if faulty.
Endpoint is not receiving hunt group calls	User error	Hunt group calls may have been halted using the Hunt Group Remove feature code. Or, the endpoint may be in Do-Not-Disturb.
	Programming error	Check hunt group programming. See “Hunt Groups” on page 8-32 .
Endpoint is not receiving pages	User error	Pages may have been halted using the Page Remove feature code. Or, the endpoint may be in Do-Not-Disturb.
	Programming error	Check page zone programming for the endpoint. See “Page Zones” on page 10-15 .

Table 17-40. System Features Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
Endpoint cannot be placed in Do-Not-Disturb mode	User error	Refer to the applicable endpoint user guide for feature instructions.
	Programming error	Endpoint is programmed to disallow Do-Not-Disturb. See the “Programming Endpoint Options” on page 7-50 .
	Defective endpoint	Perform the endpoint self-test as described in the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
The supervisor cannot silent monitor a call	The supervisor is not in the member’s hunt group.	Program the appropriate endpoint as the hunt group supervisor in DB programming.
	The agent is on a peer-to-peer (P2P) call.	Program the agent in a network group that does not allow P2P calls.
	The agent is on a conference call.	The agent must terminate the conference call.
	The agent is receiving agent help.	Wait until the agent help hangs up the call.
	Another supervisor is currently joining the hunt group member’s call.	Wait until the other supervisor hangs up the call.
A supervisor’s silent monitor terminates	The hunt group member has requested agent help.	None. The supervisor has terminated the call.
	The hunt group member puts the call on hold.	None. The supervisor has terminated the call.
	Another supervisor was silent monitoring and joined the call.	None. Only one supervisor can join a call per call.
	The call was transferred.	None. A silent monitor on a transfer announcement call terminates after the system completes the transfer.
The user cannot access feature code 320.	The Audio Diagnostics endpoint flag is not enabled.	Enable the Audio Diagnostics endpoint flag (under System\Devices and Feature Codes\Endpoints\<Node>\<endpoint>\Flags).
The user does not see the Record-A-Call menu after activating the Audio Diagnostics feature.	The Record-A-Call application does not exist.	Create a Record-A-Call application if one does not exist.
	The Record-A-Call application is not active.	Make sure the Record-A-Call feature is enabled in DB programming.
	A supervisor is silent monitoring a call.	None. The Record-A-Call feature cannot be used on certain calls (such as Agent Help, Station Monitor, Conferences, Paging, etc.).

System-Level Issues

Table 17-41 summarizes the troubleshooting strategies recommended for resolving discrepancies that may occur at the system level.

Table 17-41. System-Level Troubleshooting Strategies

Symptom	Possible Cause	Corrective Action
<p>Repeated occurrence of all calls in progress dropping</p> <p>NOTE The central office (CO) must provide a minimum of 18 mA loop current.</p>	AC line is not isolated and dedicated	Have isolated, dedicated line installed. For more information, refer to the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Defective power supply	Replace the chassis if the power supply is faulty.
	Equipment chassis located near a strong magnetic field or other potential source of interference (copy machines, power transformer, etc.)	Relocate the equipment chassis a minimum of 20 ft. (6 m) from any equipment that is a potential source of interference.
	IC-CO/CO-CO Disconnect timer(s) need(s) adjustment	See the <i>dialed digits</i> field in SMDR. Refer to the “System Features” chapter in the <i>Mitel 5000 Reference Manual</i> , part number 580.8007. Set timer(s) to a higher value. See “Timers and Limits” on page 10-24 .
	Defective Processor Module	Replace the module if faulty.
	Open or loose connection in the cable between the power supply and the chassis backplane, or a defective cable	Turn off the AC power. Check to see that the backplane-to-power supply interface cable is properly connected. Repair or replace the cable and/or the backplane if the connection is faulty. Repair or replace the chassis if the power supply is faulty.
All endpoints in the system are inoperative; no LED indication when a trunk or call button is pressed	Defective power supply or connector	Replace the chassis.
	Defective module	Replace the faulty module.
	Defective chassis backplane	Check the system voltages on the chassis backplane. Replace the chassis assembly or the chassis backplane if necessary.
Database restore aborts before finishing	Computer's power saver feature shuts down the computer and severs the communications link	Disable the computer power saver feature.
DISA does not work	User error	For procedure instructions, refer to the “System Features” chapter in the <i>Mitel 5000 Reference Manual</i> , part number 580.8007
	Endpoint not compatible	User must dial in from a DTMF telephone.
	Programming error	Ensure that the trunk group is identified correctly as a day or night DISA trunk group. See “Trunk Programming Options” on page 6-11 .
	Defective trunk module	Replace the associated module.
	Defective processor module	Replace the module if faulty.

Table 17-41. System-Level Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
NOTE Due to the natural characteristics of the CO trunk, the volume level of DTMF tones transmitted over the trunk may be substantially reduced before reaching the system. This natural degradation in tone volume may adversely affect the reliability of the DISA feature. Other factors which can affect DISA performance are CO trunk noise and the quality and strength of the DTMF tones generated by the off-premises endpoint itself.	Equipment being called is defective	Ensure that the called equipment is functioning correctly.
	DTMF digit duration/pause specifications of called equipment is incompatible with Mitel system	Check with the equipment manufacturer for DTMF digit duration/pause specifications. Adjust DTMF Digit Duration/Pause timer. Default value is .06 sec. See "Timers and Limits" on page 10-24 .
	CO trunk is designated for dial-pulse signaling	CO trunk must be designated as DTMF. See "Programming CO Trunk Group Options" on page 8-10 .
	Defective trunk module	Replace the associated trunk module.
	Defective processor module	Replace the module if faulty.
No Music On Hold/ Background Music (external music source connected)	External music source turned off or inoperative	Check the external music source for proper operation. For more information, refer to the "Installation" chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Programming error	Make sure the Music-On-Hold option for the affected device is programmed correctly. Refer to the "System Features" chapter in the <i>Mitel 5000 Reference Manual</i> , part number 580.8007.
	Defective cable between music source and the music on hold port on the back of the chassis	Repair or replace the cable. Check to see that a 1/8-in., 2-conductor (mono), mini-phone plug was used.
	Defective MOH port	Replace the defective chassis.

Table 17-41. System-Level Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
RFI/EMI present over conversations	AC power source or grounding incorrect	Verify that the AC circuit is isolated and dedicated and check for adequate grounding. For more information, refer to the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Grounding point is source of RFI/EMI	While the system is running on AC power, temporarily remove the grounding wire to see if it is the source of the RFI/EMI. For correct grounding requirements, refer to the “Installation” chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	AC power source is causing RFI/EMI	If an external battery back-up power source is installed, switch system operation to battery back-up power by unplugging the power source's AC power cord (with grounding wire connected to chassis). If RFI/EMI stops, the AC power source is the cause. Install an RFI/EMI filter or equivalent on the AC outlet.
	Trunk from central office is picking up interference	At the CO block, remove the bridging clips for the trunk. On the telco side of the block, use a test set to check for interference. Also, move the CO trunk to a known good CO circuit. If the problem follows the trunk, contact the telco.
<div> <div>NOTE</div> <div> <p>For further RFI/EMI troubleshooting assistance <i>while on site</i>, certified technicians should contact Technical Support with the following information:</p> <ol style="list-style-type: none"> 1. Modulation (AM, FM, or other) and frequency of the interfering station (in Hz) 2. Broadcast power and distance between equipment chassis and broadcast antenna 3. Who hears RFI: <ul style="list-style-type: none"> – Outside call - inside party only? – Outside call - outside party only? – Outside call - both parties? – Intercom call - one or both parties? 4. Type of instrument(s) on which RFI is heard </div> </div>		
Faulty DID numbers displayed at attendant endpoints	User error (after dialing the correct 3- or 4-digit “base” number, the user entered in correct or incomplete “start” digits)	Only valid DID “start” digits can be processed by the system.
	Programming error	Ensure that all valid DID numbers have been programmed to ring in to the appropriate locations.
	Defective T1M or T1M-2 expansion module	Replace the T1M or T1M-2 expansion module.
	Defective SLA or digital endpoint module	Replace the SLA or digital endpoint module.

Table 17-41. System-Level Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
DID numbers routed before all digits are dialed	Non-programmable system timer expiring before CO completes digit transmission	The system allows seven seconds for DID input. After seven seconds, the system routes the call based on information received to that point. The Central Office must complete DID digit transmission within seven seconds.
The traceroute command always displays “no reply.”	The routers or destination host on the network are programmed to ignore ICMP Echo requests or to not send ICMP Time Exceeded messages.	Contact the network administrator to enable these ICMP messages.
With the diagnostics mode enabled, the endpoint administrator cannot access the dump from his or her endpoint. The endpoint administrator sees “Invalid Extension Number.”	The endpoint administrator has not enabled the diagnostics mode.	Make sure the endpoint administrator has enabled the diagnostics mode (9900 in the U.S. and 9100 in Europe).
	The user has not entered the correct digits.	Verify the correct diagnostics code is used (9933 for U.S., 9133 for Europe). Also, verify that the correct digits are used for the dump.
The administrator endpoint is not displaying Alarm 128.	The Audio Diagnostics Suppression System flag is enabled.	Disable the Audio Diagnostics Suppression flag (under System\Flags).
Alarm 128 displays on an administrator endpoint.	A user completed the Audio Diagnostics feature.	Collect the Freeze which contains Message Print entry and other diagnostics data to submit to Technical Support for analysis.

T1/E1/PRI Modules

Table 17-42 summarizes the troubleshooting strategies recommended for resolving discrepancies that may occur with T1/E1/PRI (T1M) or Dual T1/E1/PRI (T1M-2) modules and trunks.

Table 17-42. T1/E1/PRI Troubleshooting Strategies

Problem	Possible Cause	Corrective Action
Dual T1/E1/PRI Module does not come online.	Hot-swap lever is not in the “on” position.	Make sure the module is properly installed in the bay. The lever is spring-loaded and should normally automatically move to the “on” position once the module is properly installed.
	Incorrect software.	Install the latest software on the Mitel 5000 system's Web page. The Dual T1/E1/PRI Module is supported in version 2.3 and later. Also make sure you have the latest Dual T1/E1/PRI package installed.
	Incorrect license.	Although the Dual T1/E1/PRI Module itself is not licensable, the second port is. Watch Message Print as you insert the module in the bay. If the board comes online, but the second port does not, you do not have a correct license. Otherwise, there is a different problem.
	Defective module.	If all of the above suggestions do not help, you may have a defective module. Please contact Mitel technical support.

Table 17-42. T1/E1/PRI Troubleshooting Strategies

Problem	Possible Cause	Corrective Action
A Dual T1/E1/PRI port does not come online.	Wrong license.	The second port on the T1M-2 has a separate license, named Additional T1/E1/PRI Ports. Regardless whether you first program port 1 or port 2, the second port you program requires a license. Make sure you have uploaded the correct license by looking at the License Information option in DB Programming. If the port is T1/PRI or E1/PRI, also make sure you have enough PRI Licenses.
One port or channel is always unavailable.	The port/channel has been busied out.	A channel, a port, or an entire module can be busied-out by a user. These can be unbusied either in DB Programming or in the DMU. You may also check the busyness status on the web page.
T1 trunks have frequent “Controlled Slip” and “Out-Of-Frame” errors	Line Build-Out (LBO) setting incorrect	Use T1 Diagnostics to determine the current LBO status. Then use T1 Programming to change the setting. For more information, refer to the “Diagnostics” chapter in the <i>Mitel 5000 Reference Manual</i> , part number 580.8007.
	Defective T1M or T1M-2 module	Check for inadequate connection. If the problem persists, contact the T1 provider or replace the module if faulty.

Upgrade Process

Table 17-43 summarizes the troubleshooting strategies recommended for resolving discrepancies that may occur when executing the upgrade process.

Table 17-43. Upgrade Process Troubleshooting Strategies

Problem	Possible Cause	Corrective Action
Upgrade action requested, but nothing happens	TFTP server has been incorrectly configured.	Check TFTP server configuration. Ensure files requested are present.
Download of upgrade component completes, but fails install	Checksum on one or more of the files will cause install to quit. The system will not be corrupted. Dependency checks may fail. Compact flash-type memory card space requirements could be exhausted.	Each of the above problems will result in a message at the web browser console (in addition to messages in the system logs). For a checksum failure, check the file on the server, and replace if a checksum failure. Attempt to download again and observe results.
		Log in as Sys Admin MB to check the disk space usage statistics and verify there is sufficient space on the compact flash-type memory card to complete the download.
System is running, but “system unavailable message” displays when connecting to the web browser	Web server is not running.	Enable the Web server through DB programming and browse to the network address.
No description or version information available for any of the components.	The package database has been corrupted.	In the Web interface, select Update to refresh the browser to retrieve the current package information, then reinstall all packages.
Upgrade action requested but nothing happens.	TFTP server has been incorrectly configured.	Check TFTP server configuration and verify requested files exist.
Download of upgrade component completes but fails install.	Checksum on one or more of the files will cause install to quit. The system will not be corrupted. Dependency checks may fail. compact flash-type memory card space requirements could be exhausted.	Each of the problems will result in a message at the Web browser console (in addition to messages in the system logs). For a checksum failure, check the file on the server, and replace if a checksum failure. Attempt to re-download and observe results.
Failure during install process.	There may be a power failure or a technician could inadvertently reset the system during the upgrade process.	If an install was aborted for either of the possible causes cited, the install process can be restarted and the system should restore correctly. However, for NOR flash components or FPGA this action could be fatal, resulting in the system having to be returned to Mitel for repair.
System is running but a “system unavailable” message appears on the Web browser	Web server is not running.	Enable the Web server through Database programming and browse to the CS-5X00 network address.
No description or version information available for any of the components.	The package database has been corrupted.	Either reinstall all packages or restore the package database.
System fails to boot.	<ul style="list-style-type: none"> Power lost during upgrade. T1M-2 installed with systems running v2.2 or earlier system software. 	<ul style="list-style-type: none"> Return power to system and reboot system. Refer to Knowledge Base Center (www.intel.com/knowledgebasecenter) KB3921 and, if necessary, contact Mitel Technical Support for direction.

UPS Monitoring

Table 17-44 summarizes the troubleshooting strategies recommended for resolving discrepancies in the UPS Monitoring feature that may occur when upgrading to v2.2.

Table 17-44. *Troubleshooting Strategies for UPS Monitoring Issues*

Symptom	Possible Cause	Corrective Action
UPS not detected	UPS unit not connected properly and/or not supported.	Verify that the UPS unit is connected correctly and is a supported model. The <code>upsmmon</code> command, available in the OLM shell, can be used to verify if the UPS is detected.
System does not shut down when the UPS runs out of battery power.	Error in UPS configuration	Verify that the system has been set to shut down upon receiving a low battery event from the UPS. See “System Flags” on page 10-19 .

Voice Processing

Table 17-45 summarizes the troubleshooting strategies recommended for resolving discrepancies with voice processing systems.

Table 17-45. *Voice Processing Troubleshooting Strategies*

Symptom	Possible Cause	Corrective Action
Phone system unable to communicate over voice channels with voice processing computer	Programming error	Make sure the appropriate time slot group (number of voice processing voice channels) is assigned to each voice processing application. Voice channels are used for processing calls between the phone system and the voice processing computer. See “Time Slot Groups” on page 11-27 .
	Loose or defective cabling between the phone system and the voice processing computer.	Check the cabling connecting the system to the computer.
System programming computer unable to communicate with voice processing computer (the monitor may display a message about being unable to communicate with or losing its connection with the voice processing computer)	Programming error	External voice processing programming cannot be accessed until a voice processing communications port has been established. Make sure Basic Voice Mail is disabled and enable the Voice Processor Connection flag.
	Defective processor module	Replace the defective module.
	The ASAI connection is bad.	The ASAI connection comes from the IP network. Verify the network configuration settings in DB programming and the Avdap Configuration Utility.
Basic Voice Mail files are corrupted.	Not running the most current software release.	Upgrade the system files to the latest release. If BVM files are still corrupted, refer to the Knowledge Base for additional information. Contact Technical Support for assistance, if needed.

Table 17-45. Voice Processing Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
Monitor and keyboard unable to communicate with voice processing computer	Loose or defective cabling between the voice processing computer and the monitor or keyboard	Check the cabling connecting the computer to the monitor or keyboard.
	Monitor is wrong type for the Monitor Card installed in the computer	Make sure the monitor is the correct type (generally VGA) for the Monitor Card installed in the computer.
	Defective monitor or keyboard	Replace the defective monitor or keyboard.
	Defective Monitor Card or computer Motherboard	Replace the defective card.
Automated attendant not responding properly	User error	The caller must use a DTMF endpoint to enter digits.
	DTMF tones not being interpreted correctly (see NOTE below)	If numbers appear to be misdialed frequently, due to trunk noise or other problems, use the Digit Translation feature. See “Using Digit Translation” on page 11-33 .
	Programming error	Automated attendant endpoint(s) must be designated in the database. See “Auto Attendant” on page 11-30 .
	Defective VPC or hard disk	Replace the defective computer component.
<div style="display: flex; align-items: center;"> <div style="background-color: #d9e1f2; padding: 5px; margin-right: 10px; width: 100px; text-align: center;">NOTE</div> <div> <p>Due to the natural characteristics of the CO trunk, the volume level of DTMF tones transmitted over the trunk may be substantially reduced before reaching the system. This natural degradation in tone volume may adversely affect the reliability of the automated attendant feature. Other factors which can affect automated attendant performance are CO trunk noise, the quality of the recording device, and the quality and strength of the DTMF tones generated by the calling endpoint itself.</p> </div> </div>		
Automated Attendant is not receiving incoming calls. Callers are routed to primary attendant instead	Programming error	Ensure that the desired trunks (in day and/or night mode) are programmed to ring in directly to the correct automated attendant extension number. See “Trunk Programming Options” on page 6-11 .
	Loose or defective cabling between the phone system and voice processing computer	Check the cabling connecting the system to the computer.
Automated Attendant says you have pressed an invalid button when no button was pressed	Talk off is occurring from the recording	Remove that recording and play the application to see if it transfers improperly. Re-record the message that is causing talk-off.
Automated Attendant indicates that an extension number is invalid even though it exists on the system	The extension does not have an assigned mailbox or an extension ID number	Extension ID numbers provide the Automated Attendant application a means for transferring calls to extensions which do not have mailboxes. See “Extension IDs” on page 11-47 .
Automated Attendant transfers calls directly to voice mail without trying the extension number first	Programming error	Make sure the mailbox is associated with a corresponding extension number. See “Programming Mailbox Options” on page 12-8 .

Table 17-45. Voice Processing Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
Unable to access desired voice processing application (intercom callers hear reorder tones and see a CALL CANNOT BE COMPLETED display; outside callers are rerouted to the primary attendant)	Voice processing has slowed down and call processing has timed out	If the problem continues to occur, even during periods of low activity, reboot the voice processing computer.
Unable to access desired voice processing application (intercom callers see a XXXXX IS BUSY display and camp on until a voice channel is available; outside callers hear ringing until a voice channel is available)	All programmed voice channels are currently busy	Make sure the appropriate time slot group (number of voice processing voice channels) is assigned to each voice processing application. Voice channels are used for processing calls between the phone system and the voice processing computer. See “Time Slot Groups” on page 11-27 .
		Disable Basic Voice Mail and add an external voice processing application for additional ports.
Unable to access desired voice processing application (intercom callers hear reorder tones and see a XXXXX IS UNAVAILABLE display; outside callers are rerouted to the primary attendant)	A database save or restore is in progress, the computer is being reset, or the computer is starting up for the first time	Try again within five or 10 minutes.
Unable to access desired voice processing application (intercom callers hear reorder tones and see a XXXXX IS UNPLUGGED display; outside callers are rerouted to the primary attendant)	The voice processing computer power switch is off, the cabling between the system and the computer is disconnected or defective, or the voice processing computer is inoperative	Check to make sure the voice processing computer power switch is on, and check the cabling connecting the phone system to the computer. Also, verify IP addressing and network connectivity for ASAI connection.
	The Basic Voice Mail Application got hung up	Reset call processing.
Voice processing applications are slow (e.g., voice prompts are slow and display messages are delayed)	The voice processing computer high-speed (turbo) processor mode is turned off	For optimal performance, the voice processing computer is configured with the high-speed (turbo) mode <i>always</i> enabled. Do <i>not</i> disable the turbo mode setting.
Voice processing computer is programmed with 12–40 voice channels, but no more than eight calls at a time are accepted	The number of programmed voice channels is less than the available hardware	Make sure the appropriate time slot group (number of voice processing voice channels) is assigned to each voice processing application. See “Time Slot Groups” on page 11-27 .
	Loose/defective cabling between the voice processing device AIC and the chassis	Check the AIC-to-CS-5000 base server cabling.

Table 17-45. Voice Processing Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
When power is turned on, the voice processing computer does not boot up properly	Diskette in floppy drive	Ensure that the computer is not trying to boot off a diskette in the floppy drive.
	The two-pin AIC-to-reset switch cable is not connected properly	Be sure that pin 1 marked on each end of the cable matches pin 1 on the AIC and computer Mother board. (If connected incorrectly, the computer will be reset continuously or will not boot up at all.)
	The voice processing computer's high-speed (turbo) processor mode is turned off	The voice processing computer boots up much faster in turbo mode. Before shipping, the computer is configured with the high-speed (turbo) mode <i>always</i> enabled. Do <i>not</i> disable the turbo mode setting.
When power is turned on, the voice processing computer beeps once (for two seconds) and does not boot up properly.	Incorrect DIP switch or jumper strap settings on the Audio Interface Card (AIC)	Ensure that the AIC DIP switches and jumper straps are set in the correct positions. For more information, refer to the "Voice Processing Features" chapter in the <i>Mitel 5000 Reference Manual</i> , part number 580.8007.
	Software problem	The computer should be used for voice processing applications only. If necessary, delete any unneeded peripheral software and re-install the voice processing applications software as outlined in the "Installation" chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Incorrect CMOS settings	Refer to the diagnostic materials generally included in a plastic sleeve attached to the inside of the chassis cover.
Both internal and remote users have no message notification after receiving voice messages in their mailboxes	The Message Notification/ Retrieval application has not been set up	The system must be programmed with the Message Notification/Retrieval application in order to allow voice mail message notification and quick mailbox access. See "Message Notification/Retrieval" on page 11-37 .
Audio volume levels from voice processing applications (such as voice mail and Automated Attendant) are too low or too high	Programming error	Adjust the volume level for all of the voice channels used by the voice processing computer. See "Voice Processor System Settings" on page 11-16 .
No audio from voice processing applications, such as voice mail or Automated Attendant	Loose or defective cabling between the AIC and the chassis	Check the cabling.
	Invalid or missing prompt files One or more ports are blocked	When Basic Voice Mail starts up, if the prompt or menu files (english.pmt, english.ini, & menuinit.dat) are not valid (missing, defective, or the wrong version), the message "Faking an active language" will appear in the log file. You must reinstall the prompt and menu files as described in the "Installation" chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	Defective AIC in the EM	Replace the defective card.
	Improper drivers are loaded	Load the correct drivers. See if the fax ports are listed in the <code>summary.txt</code> (in the Avdap folder).

Table 17-45. Voice Processing Troubleshooting Strategies (Continued)

Symptom	Possible Cause	Corrective Action
Fax-On-Demand feature not working properly	Programming error.	User group 1 and the home area code tables must be programmed before using the Fax-On-Demand feature. A fax library must also be established. See the "Fax-On-Demand" on page 11-69 .
	Incorrect switch or jumper settings on the Fax Card.	Ensure that the switches and jumpers are set in the correct positions.
	Defective Fax Card	Replace the Fax Card.
	Improper drivers are loaded	Load the correct drivers. See if the fax ports are listed in the <code>summary.txt</code> (in the Avdap folder).
Unable to record any voice mail greetings or messages and/or unable to hear any voice prompts	Loose/defective cabling between the external voice processor and the chassis	Check the cabling.
Japanese language voice prompts unavailable	Japanese voice prompts not installed	Install the Japanese voice prompts as outline in the "Installation" chapter in the <i>Mitel 5000 Installation and Maintenance Manual</i> , part number 580.8000.
	User and/or programming error	Refer to the "System Features" chapter in the <i>Mitel 5000 Reference Manual</i> , part number 580.8007

VoIP Echo Canceller Troubleshooting

[Table 17-46](#) lists VoIP Echo Canceller troubleshooting scenarios.

Table 17-46. VoIP Echo Canceller Troubleshooting Tips

Scenario	Cause	Possible Solution
A customer complains about echo.	The system may still be configured to use the Basic VoIP Echo Canceller setting.	Configure the system to use the Advanced VoIP Echo Canceller setting and monitor the site for feedback.
A customer is using the Advanced VoIP Echo Canceller setting and complains about loud, clear echo throughout calls.	The echo has a delay of more than 64 ms.	Configure the system to use the Specialized VoIP Echo Canceller setting and monitor the site for feedback. Determine the source of the long echo, because this does not occur regularly with trunks that are operating normally.

VPIM Networking

Table includes additional troubleshooting information for VPIM networking issues. In general, you can review the following log files to help troubleshoot VPIM issues:

- **Avdap.log**: Shows the voice mail processes as they pertain to conversion and sending of messages.
- **Mail.mainlog**: Contains messages from the component used to route VPIM messages (EXIM), and includes the source and destination mailbox extensions and any relay errors.

Table 17-47. VPIM Troubleshooting Strategies

Symptom	Probable Cause	Corrective Action
A message did not arrive at the remote node.	The domain name is not correct.	Modify the Domain field in DB Programming to match the FQDN for the VPIM node (see “VPIM Domain Name” on page 11-10).
	The destination e-mail username is not correct.	Contact the administrator of the remote node and verify that the E-mail Username field is programmed correctly.
	SMTP server isn't configured for open relaying.	Contact the administrator at the remote node and advise him or her to configure the SMTP server for open relaying.
	The Mitel 5000 server's hostname is programmed incorrectly or an alias was used. When a VPIM message arrives, the system cannot resolve the hostname and deliver the message.	To receive and send e-mail messages using VPIM, you must program the hostname for the Mitel 5000 Base/Processing server under System\IP Settings identically to the hostname you program under Voice Processor\Devices\ Nodes\<node>\System Number/Domain . Verify the FQDN and ensure an alias is not used by looking up the entries in DNS.
A message did not arrive at the local node.	A firewall may be blocking port 25. This port is required to be open for VPIM networking.	Verify that you can ping the system on the appropriate port from an address outside the firewall and network.
	The domain of the sending voice processing platform is not a safe domain.	Be sure that you have added the sending voice processing platform as a remote VPIM node with the correct FQDN.
The network settings are configured correctly on both VPIM nodes, but messages are not being exchanged.	The VPIM peer is not fully VPIM-compliant.	Capture the e-mails that are being sent between the VPIM peers and compare them against the RFC 2421 Specification .

Customer Support

Mitel provides access to comprehensive technical support in accordance with the criteria and processes described in this section.

Technical Support

For additional information and/or technical assistance in North America, certified technicians may contact:

Technical Support Department (U.S.)

Mitel Networks Corporation.

7300 West Boston Street

Chandler, AZ 85226-3224

1-888-777-EASY (3279)

For information on how to contact Mitel Technical Support outside of North America, please refer to your Channel Support Agreement.

Emergency Assistance

After office hours and on weekends, call 1-888-777-3279 and leave your message with the voice mail service. A Technical Support Product Specialist will return your call as soon as possible, usually within an hour. As a backup (e.g., the main number does not answer or you do not receive a call back within an hour), you can call 480-961-0277. Please remember that this is an emergency number for *critical system problems only*. Sales questions, equipment orders, and so on, can only be handled during normal business hours.

Defective Equipment Return Policy

For complete information on returning equipment, refer to the current *Repair and Return Policy*, part no. 835.1065. This document includes specific information on the following subjects: warranty, procedures to follow when returning equipment, equipment damaged in shipment, insurance, repair policy, and advance replacement policy.

Index

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

Symbols

911, programming 5-21
 99 Nodes Support 17-11
 99 Nodes Support Troubleshooting Issues 17-11

A

Abandoned Call Timer 10-24
 Absorbed Digits 8-17
 Absorbed digits 8-17
 programming 8-16
 Absorbed Patterns 8-17
 AC impedance, loop start 6-33
 Access rights, programming 3-5
 Account Codes 7-69, 7-70
 forced 7-69
 standard 7-69
 ACD Agent ID 8-33
 ACD Agent ID extension lists 8-4
 ACD Agent No Answer – DND Message Additional Text 8-42
 ACD Agent No Answer – DND Message Number 8-43
 ACD Hunt Groups
 extension lists 8-40
 flag 8-44
 wrap-up timer 8-42
 Adding 6-10
 Administrative Web Session 17-12
 Administrative Web Session *See AWS*
 Administrative Web Session Troubleshooting Strategies 17-12
 Administrator, e-mail address 11-63
 Administrator E-Mail Address 11-62
 Administrator Feature Codes 10-41
 Administrator feature codes 10-41
 Administrator phone/endpoint flag 7-23
 Advanced IP Settings 9-15
 Advanced IP Settings Fields 9-15
 Agent Help 7-51, 7-58
 tone interval timer 10-24
 Agents 8-38
 Alarms, clearing 16-36
 description 16-33
 major 16-48
 major, responding to 16-36
 minor 16-48
 queue 16-35
 system
 #203 11-5
 Allow International Calls 11-71
 Allow Transfer Method Programming 11-47, 12-23
 Allow User to Configure Settings 12-13
 Allowed Answer
 programming 8-9, 8-12, 8-13, 8-14, 8-15, 8-16, 8-18,
 8-19, 8-20, 8-21, 8-22, 8-23, 8-24, 8-26, 8-
 27, 8-30, 8-31, 8-56
 Allowed Numbers COS (Europe) 5-6
 All-Ring Hunt Group 8-40
 Alternate Hold Timer 10-28
 Alternate Hold Timers endpoint flag 7-23
 Alternate Keymap 7-48
 Alternate Keymap endpoint flag 7-23
 Alternate Message Source
 programming 7-51
 Alternate Tone Detection 11-19
 Analog Voice Mail, hunt group flag 8-44
 Analog Voice Mail Hunt Group 8-44
 Announce Only 12-27
 Announcement and Overflow Endpoints 8-45
 Announcement Endpoints 8-42, 8-45
 Announcement Timer 8-42
 Answer Recognition timer, E&M trunks 6-15
 Answer Supervision Types
 E&M trunks 6-15
 loop start trunks 6-15
 Application Attributes 11-29
 application diagnostic commands 16-47
 Application-Related Information 11-53
 Applications 11-28

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

- Area codes 5-4
 - allowed/denied 5-5
 - extended 5-26
 - flags 5-4
 - restricted 5-26
 - user group 5-26
 - Area flags 5-4
 - ARS (Automatic Route Selection)
 - ARS Only option for COS (Europe) 5-6
 - ARS Only option for COS (USA) 5-5
 - description 5-10
 - dial rules
 - Europe systems 5-12
 - programming 5-12
 - USA systems 5-12
 - facility group report 15-3
 - facility groups 5-14
 - route group report 15-3
 - route groups 5-16
 - audio settings 5-20
 - creating 5-17
 - dial groups
 - programming 5-18
 - facility groups, adding 5-19
 - ASR
 - See Automatic Speech Recognition
 - Associated Devices and References 7-17
 - Associated devices and references 16-38
 - Associated Extensions 7-22
 - Associated Gateway, MGCP 6-21
 - Associated Mailboxes, test 14-11
 - Attached Device 7-64
 - Attachment Format for Inbound Faxes 11-61
 - Attachment Format for Mobile Devices 12-13
 - Attendant 11-44
 - Attendant endpoint flag 7-23
 - Attendants 7-78
 - primary 7-79
 - programming 7-51
 - Audio, Direction 16-21
 - Audio Diagnostics Sampling Period 9-27
 - Audio Diagnostics Samplings 9-27
 - Audio for Calls
 - camped onto this device 7-65, 8-50, 11-44
 - holding for this device 7-65
 - ringing this device 7-66, 8-46
 - Audio for Calls Camped onto this Device 7-65, 8-45, 11-44
 - node programming 4-5
 - Audio for Calls Holding for this Device 7-65
 - Audio for Calls Ringing this Device 7-66, 8-46
 - Audio for Camped-On Announcement Calls 8-46
 - Audio Frames/IP Packet 9-28
 - Audio Quality 17-35
 - Audio RTP and Data Types of Service 9-18
 - Audio RTP Type of Service 9-18
 - Audio RTP Type Of Service And Data Type Of Service 9-18
 - Audio RTP Type of Service and Data Type of Service 9-18
 - Audio Stream Receive Port 9-19
 - Audio Stream Receive Port Ranges and Default Values 9-19
 - Auditex recordings, saving and restoring 13-6
 - Auditex Recordings 11-51
 - Auto Attendant Transfer Prompt 12-24
 - Auto-Answer modem 2-10
 - Automated Attendant
 - information 11-30
 - transfer prompt 11-47, 12-24
 - Automatic Answer endpoint flag 7-23
 - Automatic Fax Detection 11-41
 - Automatic Header Reduction 11-70
 - Automatic NAT Detection 9-40
 - Automatic Report Generation 15-8
 - Automatic Route Selection, route group dial patterns, USA 5-18
 - Automatic Speech Recognition
 - feature description 11-23
 - programming 11-24
 - Automatic Speech Recognition (ASR) Enabled 11-24, 12-28
 - Automatic Speech Recognition (ASR) Setting 11-24, 12-28
 - Average Connect Time Per Call 8-42
 - AWS (Administrative Web Session)
 - description 16-37
- ## B
-
- Backup database
 - forcing 3-14
 - saving 3-14
 - Backup database
 - enable periodic save 3-13
 - periodic save time 3-12
 - save retry attempts 3-13
 - Base Server/Processing Server Connection Settings 9-11
 - Base Server/Processing Server Connection Settings Fields 9-11

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

Basic Rate Module

Busy Out

Manager 16-4

statuses 16-5

Basic Voice Mail 17-12

Basic Voice Mail Troubleshooting Strategies 17-12

Batch Extension Change 8-8, 8-36, 10-33, 11-28

Trunks 6-4

Bit rate modem 4-25

Boards, test 14-12

Daylight Saving Time 10-3

Broadcast Alarms to All Administrators 10-20

BS-BVM System Recording Codec 11-26

Busy Out

Manager, programming 16-4

statuses, programming 16-5

Busy Signal

instead of camp-on DID/E&M 7-24

Busy Tone Cycle Detect 11-54

Button Assignments 7-72

BVM (Basic Voice Mail)

data, saving and restoring (CS-5600) 13-19

data, saving and restoring (to NFS) 13-20

play only mailbox 12-25

C

Cadences

alerting 7-24

ring 7-25

ringback 7-24

Call Configuration 9-39

Call configurations

trunks 6-20

Call Cost 3-36, 8-17

adjustments 3-38

trunk groups 8-16

Call Flow 17-8

Call Flow Troubleshooting Considerations 17-8

Call For Each New Message 12-20

Call Forwarding

no answer timer 10-28

timer 10-28

Call Logging 7-54

option fields 7-54

Call Processing

resetting 3-3, 3-44

Call Progress Delay 11-54

Call Progress Detection 11-54, 12-22

Call Routing announcement, nodes 11-32

Call routing reports 15-3

Call routing patterns

adding 6-26

batch creating 6-27

copying 6-27

deleting 6-26

description 6-24

editing 6-25

options 6-25

viewing 6-26

Call Routing Table 7-56, 8-25

Call routing tables

description 6-22

keys 6-23

Call Screening 11-48

Callback (Queue)

timer 10-30

Caller ID

propagate original 8-26

timers 10-28

wait for ISDN 8-27

Caller ID Forwarding

troubleshooting 17-13

Caller ID Propagation 17-14

Caller ID Propagation Support Troubleshooting Issues 17-14

Caller Information 7-25

Calling Party Name 7-63

endpoints 7-63

for trunk groups 8-26

for voice processing applications 11-46

Calling Party Number 7-63, 7-64

endpoints 7-64

for trunk groups 8-26

for voice processor applications 11-46

Call-in-Progress Dial Tone 11-54

Camp On Allowed 8-57

Camp-On

hunt groups 8-47

timer 10-24

tone enable/disable 7-25

tone timer 10-24

Camp-On Indications endpoint flag 7-24

Camp-Ons Allowed 8-23, 8-31, 8-47, 8-57

Canceling fax selections 11-33

Cascade Levels 12-21

Category D licenses 3-7

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

Change log, database 16-6

Channel Statistics 15-7

Characters, dialing pattern 5-24

Class of Service 7-55

Classes of Service

- report 15-3

Classes of Service (COS) 8-16, 11-37

- trunk groups 8-16

Cleanup test 14-13

Clear mailbox messages 12-5

CO Recall 7-56

CO Reseize Timer 10-24

CO Transfer/AA/VM 7-56

CO Trunk Group 8-4

CO Trunk Groups 8-7

CO trunk groups

- assigning trunks to 6-5
- report 15-3

CO Trunk Troubleshooting Strategies 17-16

CO/IC Reseize Timer 7-24, 10-24

CO-CO Disconnect Timer 10-29

Codes

- area (used as office) 5-4
- diagnostics feature 16-43
- endpoint feature 10-34
- home area 5-22
- office 5-4
- trunk access 10-33

Communication Timeout 6-21

Company Directory 11-33

Configuring a 99-Node Network 4-2

Connected to CO 6-17

Conversions

- database, description 14-23

Converting Inter-Tel to Mitel IP Endpoints 7-17

Converting Usernames to Mixed Case 7-18

Copy and Paste Application Attributes 11-29

Copy and Paste Applications 11-29

Copy and Paste Attributes 11-29

Copy Fax to Sender 12-14

Copy Mailbox 12-6

Copying

- call routing patterns 6-27
- trunks 6-5

Copying Endpoint Programming 7-16

COS (Classes of Service)

- Allowed Numbers (Europe) 5-6
- ARS Only (Europe) 5-6
- ARS Only (USA) 5-5
- day and night lists 5-7
- Denied Numbers (Europe) 5-6
- Deny Area/Office (USA) 5-5
- Deny Equal Access (USA) 5-5
- Deny International (Europe) 5-6
- Deny International (USA) 5-5
- Deny Local Calls (Europe) 5-6
- Deny Local Calls (USA) 5-5
- Deny Operator (Europe) 5-6
- Deny Operator (USA) 5-5
- Deny Toll Access (Europe) 5-6
- Deny Toll Access (USA) 5-5
- description 5-5
- descriptions, adding or changing 5-7
- dialing patterns

 - adding 5-8
 - allowing or restricting 5-8
 - deleting 5-8
 - moving 5-8

Cost

- call adjustments 3-38
- calls, description 3-36

CP History 6-20

Creating and Managing a Group List 11-49

Current Fax-On-Demand Library Size And Percentage Of Maximum Currently Used 11-70

Customer Care Remote Configuration

- enabling with endpoint 3-56
- IP Port settings 2-6

Customer Support 17-88, 17-89

D

Data, mailbox statistics, saving and restoring 13-6

Data Type of Service 9-18

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

- Database
 - backup
 - enable periodic save 3-13
 - forcing 3-14
 - parameters 3-12
 - save retry attempts 3-13
 - saving 3-14
 - change log 16-6
 - default 3-34
 - operations 16-41
 - query options 16-39
 - scheduled backups 3-15
 - Test and Repair 14-20
 - menus 14-8
- Database Change Log, troubleshooting 17-20
- Database Programming See DB Programming
- Database utilities
 - Database Coverter
 - description 14-23
 - Mitel 5000 DB conversions 14-24
 - notes 14-23
 - Database Test and Repair
 - Associated Mailbox 14-11
 - Boards 14-12
 - Cleanup 14-13
 - common errors 14-10
 - description 14-7
 - Devices 14-13
 - Dynamic Enumerations 14-15
 - Enumerations 14-16
 - Extensions Conflict 14-16
 - guidelines 14-9
 - Hardware Addresses 14-17
 - icons 14-8
 - Miscellaneous 14-18
 - options 14-9
 - DB Test
 - Miscellaneous 14-19
 - Static Records 14-20
 - viewing 14-2
- Databases
 - CS-5600 BVM, saving and restoring from remote computer 13-15
 - EM, saving and restoring 13-11
 - testing and repairing 14-7
- Date, programming 10-2
- Day and Night Class of Service 7-55
- Day and Night Classes of Service 11-37
- Day and Night Lists, COS 5-7
- Day/Night Emergency Outgoing Access 8-56
- Day/Night list
 - user group 5-27
- Day/Night Outgoing Access 8-56
- Days of the Week 11-73
- Days Of The Week, Message Notification 12-20
- DB (Database) Programming
 - Session Manager
 - connection options 2-9
 - Connection tabs 2-7
 - description 2-4
 - IP Port settings 2-6
 - language, selecting 2-6
 - network connections 2-6
 - Session menu 2-5
 - session, starting 2-8
 - Settings menu 2-6
- DB Studio
 - File menu 2-13
 - Help menu 2-14
 - Options menu 2-13
 - Toolbar icons 2-14
 - Tools menu 2-14
 - View menu 2-13
- DDI (Direct Dialing Inward) trunks
 - Number of Digits to Receive 6-18
- Default
 - database 3-34
- Default Application 11-40
- Default Echo Profiles for Devices 10-7
- Default Keymap 7-27
- Default Network Group 8-52
- Defective Equipment Return Policy 17-89
- DEI Troubleshooting Strategies 17-20
- Delay Dial Start Type 6-14
- Deleted Message Hold Duration 11-54
- Deleting an ACD Agent ID 8-34
- Deleting Hunt Groups 8-35
- Deliver Hangup Message (When ANI Is Available) 12-24
- Deliver Hangup Message (when ANI is available) 12-24
- Denied Numbers COS (Europe) 5-6
- Deny Equal Access COS (USA) 5-5
- Deny International COS (Europe) 5-6
- Deny International COS (USA) 5-5
- Deny Local Calls COS (Europe) 5-6
- Deny Local Calls COS (USA) 5-5
- Deny Operator COS (Europe) 5-6
- Deny Operator COS (USA) 5-5
- Deny Toll Acces COS (USA) 5-5

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

- Deny Toll Access COS (Europe) 5-6
- Deny/Area Office COS (USA) 5-5
- Desktop Interface 10-33
- Detailed Endpoint report 15-3
- Device IP, status 9-4
- Device Baseline Extensions 5-9
- Devices
 - database test 14-13
 - nodes, importing and exporting 4-19
 - system information 16-37
- Diagnostics
 - Administrator endpoint 16-43
 - automatic delivery 16-37
 - external resources 16-49
 - feature codes 16-43
 - other features 16-43
 - periodic 16-40
 - raw commands 16-49
 - system 16-48
 - system alarms 16-33
 - System Manager 16-49
 - voice processing
 - description 16-42
- Diagnostics and Troubleshooting 16-1, 17-1
- Diagnostics feature codes 16-43
- Diagnostics Mode Default Feature Codes 10-42
- Diagnostics Mode Feature Codes 10-42
- Dial Initiation Timer 10-22, 10-24
- Dial Patterns/Strings, ARS 5-18
- Dial rules
 - European systems 5-12
 - programming for ARS 5-12
 - USA systems 5-12
- Dial Tone Start Type 6-14
- Dial-0 Destination 11-18, 12-18
- Dial-0 Destinations 11-18, 12-18
- Dialed Pause Duration 11-54
- Dialing patterns
 - adding 5-8
 - allowing or restricting 5-8
 - deleting 5-8
 - digits, programming 5-8
 - moving 5-8
 - special characters 5-24
- Dialing Timers 10-24
- DID Start Types 6-14
- DID (Direct Inward Dialing) trunks
 - Number of Digits to Receive 6-18
- DID trunks
 - Disconnect Timer 6-14
 - Start Type 6-14
- DID/E&M Receive Busy Instead Of Camp On endpoint flag 7-24
- DID/E&M Receive Busy Instead of Camp-On 7-24
- Different Alerting Cadence Intercom/CO Call 7-24
- Digit Translation 11-33
 - nodes 11-36
 - programming 11-33
- Digital Equipment Interface (DEI) 17-16
- Digits
 - dialing pattern 5-8
- Direct Inward Dialing (DID)
 - disconnect recognition timer 10-24
 - inpulse-dial inter-digit pause recognition timer 10-24
 - off-hook debounce timer 10-25
 - on-hook debounce timer 10-25
 - post-seize delay timer 10-25
 - post-signal delay timer 10-25
 - pre-signal delay timer 10-25
 - ready timeout timer 10-25
 - seizure recognition timer 10-25
 - signal hold timer 10-25
 - timers 10-24
- Direct Inward System Access (DISA) 7-56, 8-25
 - invalid extension failure limit timer 10-25
 - security code failure limit timer 10-25
 - transfer tone 10-20
- Direct Station Select/Busy Lamp Field Unit
 - keymaps 7-39
 - populating a DSS keymap 7-44
- Directories, reports 15-7
- Directory
 - company 11-33
 - information 12-9
 - sort order 15-7
- Directory Information 12-9
 - setting flags 12-9
- Disable Confirmation Tone to Trunks 10-20
- Disconnect Timer
 - DID trunks 6-14
 - E&M trunks 6-14
- Disconnect Wait after Dialing Timer 10-25
- Disk Usage Statistics 11-18
- Display "T" for Two B-Channel Transferred Calls 3-52
- Display Caller ID Name and Number 10-21

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

Distributed 4-5
 trunk group 8-18
 Domain name 9-9
 Do-Not-Disturb
 override 7-24
 permission 7-24
 Drop Incomplete Calls 10-21
 DSS or IDS DSS 7-39
 DSS/BLF Button 7-43
 DTMF (dual-tone multi-frequency)
 trunk signaling 6-13
 DTMF Digit Delay Off 11-58
 DTMF Digit Delay On 11-58
 DTMF Digit Detect Off 11-58
 DTMF Digit Detect On 11-58
 DTMF Digit High To Low Twist (Play and Idle) 11-58
 DTMF Digit In To In Ratio (Play and Idle) 11-60
 DTMF Digit In To Out Ratio (Play and Idle) 11-58
 DTMF Digit Low To High Twist (Play and Idle) 11-58
 DTMF Generation Information 11-59
 Dual-Tone Multi-Frequency (DTMF) Signaling
 digit timers 10-26
 Dual-tone multi-frequency *See DTMF*
 Dynamic Enumerations test 14-15, 14-16

E

E&M (Ear and Mouth) trunks
 Answer Recognition timer 6-15
 Answer Supervision Types 6-15
 Disconnect Timer 6-14
 Off-Hook Debounce Timer 6-15
 Start Type 6-14
 E&M Transmit Handshake Delay 10-27
 E&M Trunks
 receive busy instead of camp-on 7-24
 timers 10-26
 Echo Cancellor 10-8
 Echo Profile 7-67, 9-20
 Echo Profiles 17-3
 system 6-16, 10-5
 EM Server IMAP Connection Timeout 11-61
 E-mail Account Folder for Synchronization 12-13
 E-mail Account Password 12-13
 E-mail Account Username 12-13
 E-Mail Address 11-63
 E-mail Address for Fax Delivery 12-14
 E-mail Address for Voice Messages 12-13
 E-mail Client Message Format 12-14
 E-Mail Gateway 11-66
 administrator e-mail address 11-63, 11-64, 11-65
 gateway password 11-65
 E-Mail Gateway for SMTP 11-67
 E-Mail Gateway on the CS-5600 11-66
 E-Mail Gateway Programming Options 11-62
 E-mail Reader Profile 12-17
 E-mail Reader Profiles 12-17
 E-mail Reader Profiles, Message Notification 12-17
 E-Mail Real Name 11-63
 E-Mail Retrieval (minutes) 11-25
 E-mail Server 12-13
 E-Mail SMTP Port 11-64
 E-Mail SMTP Server 11-64
 E-Mail System 11-64
 E-Mail Username 11-65
 Emergency
 extension 9-36
 numbers, programming 5-21
 outgoing access 9-36
 Emergency Assistance 17-89
 Emergency Outgoing Access 8-56
 node IP connection groups 8-56
 Emergency Party Calling Number 7-64
 Enable Auto Schedule 13-2
 Enable Delivery of Incomplete/Failed Inbound Faxes 11-61
 Enable Diagnostics 13-2
 Enable Hookflash 8-22
 Enable IMAP Login for EM Server 11-61
 Enable Notification 12-22
 Enable Shutdown On Low Battery 10-21
 Enable SSL for E-mail Server Connection 12-13
 Enabling a Socket 9-34
 Encoding Settings
 fax transmission 9-32
 Music-On-Hold 8-55
 speech 9-34
 End Fax Selections 11-34
 Endpoint
 database programming password 7-76
 feature codes 10-34

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

Endpoint Associated Extensions

- Agent Help 7-51
- Agent Help User-Keyed Extension 7-51
- Alternate Message Source 7-51
- Attendant 7-51
- Emergency Extension 7-51
- Message Center 7-51
- Outgoing Extension 7-52
- Transfer Recall Destination 7-52
- Voice Mail 7-52

Endpoint Flags 7-22

Endpoint Troubleshooting Strategies 17-21

Endpoints 17-21

- attendants 7-78
- caller information 7-25
- Calling Party Name 7-63
- Calling Party Number 7-64
- converting Inter-Tel to Mitel 7-19
- creating from CSV files 7-8
- DB Programming password 7-76
- flag report 15-3
- handsfree enable/disable 7-25
- headset connect tone 7-25
- message centers 7-77
- messages 7-72
- MGCP
 - creating 6-10
 - on the local node 7-22
 - outgoing trunk access 7-52
 - primary attendants 7-79
 - system forwarding paths 7-74
 - system speed dial 7-75
 - transient call indication 7-26

Endpoints on the Local Node 7-22

Enterprise Messaging System Fields 11-53

Envelope Settings 12-10

Equal Access wildcard 5-23

Error information 3-15

Error information 16-41

Error reporting 16-48

Errors, Database Test and Repair 14-10

Example of Get IP Device Status Window 16-42

Exempt from ARS 8-16, 8-17

Expansion Module Troubleshooting Strategies 17-27

Expansion Modules 17-27

Extended area codes 5-26

Extension ID 11-47

Extension IDs 11-47

Extension Lists

- in ACD hunt groups 8-40
- in hunt groups 8-40

Extension lists, ACD Agent ID 8-4

Extensions

- conflict test 14-16
- Device Baseline 5-9

External voice processor, saving and restoring 13-4

External diagnostics resources 16-49

F

Facility group dialing rules, programming 5-14

Facility groups

- Europe systems 5-13
- planning 5-13
- trunk groups 5-15
- USA systems 5-13

Failed Connection Retry Interval 11-13

Failed Connection Timeout 11-13

Favorites menu 2-14

Fax

- delivery reports 15-7
- documents
 - saving and restoring 13-6

Fax Control-Messages Redundancy Count 9-31

Fax Delivery Destination 12-14

Fax detection 11-41

Fax Detection Sensitivity 9-31

Fax Documents 11-71

Fax Documents Usage report 15-7

Fax Encoding Setting (Fax Transmission) 9-32

Fax Format 11-73

Fax Maximum Connection Speed 9-32

Fax Page-Data Redundancy Count 9-31

Fax Retransmission Timer 11-69

Fax Retry Timer 11-69

Fax Tone Wait Timer 11-70

Fax-On-Demand 11-32, 11-69

- allow international calls 11-71
- digit translation 11-34
- fax documents 11-71
- fax format 11-73
- outgoing access 11-72
- timers and limits 11-69

Fax-on-Demand Timers and Limits 11-69

Feature Buttons 7-43

Feature Codes 10-2, 10-33

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

Feature codes

diagnostics 16-43

endpoint 10-34

File-Based Music-On-Hold 10-9

troubleshooting 17-28

Firmware, uploading through a TFTP connection 14-21

Flags 10-19

agent help tone 10-19

allow green LEDs 10-19

alternate IP/digital endpoint menu display 10-19

area 5-4

audio for camped-on announcement calls 8-46

Barge-In notification tone 10-20

broadcast alarms to all administrators 10-20

date display format 10-20

DISA transfer tone 10-20

drop incomplete calls 10-21

house phone mode 10-21

insufficient bandwidth alarm 10-21

Music-On-Hold for IC calls 10-22

OHVA enable 10-22

play pre-Record-A-Call display 10-22

receive network alarms 10-22

Record-A-Call tone 10-22

restart ACD idle time upon login 8-48

ring flash on DSS lamps 10-22

send network alarms 10-22

single idle time for all hunt groups 10-22

system speed dial override toll restriction 10-23

time display format 10-23

UCD/ACD station-monitor indications 10-23

use green LEDs for direct rings 10-23

validate network mailboxes 11-15

validate voice mailbox number 10-23

validate voice mailbox numbers 10-23

wrap-up mode for ACD calls 10-23

Flags for Endpoints

Administrator 7-23

Alternate Hold Timer 7-23

Alternate Keymap 7-23

Attendant 7-23

Automatic Answer 7-23

Camp-On Indications 7-24

DID/E&M Receive Busy Instead Of Camp On 7-24

Different Alerting Cadence Intercom/CO Call 7-24

Force reset if not idle 3-45

Force Trunk Group Calling Party Name and Number 8-27

Forced – Local Toll Calls Validated 7-69

Forced Account Codes 7-69

validated 7-69

Forced reset, major 3-45

Forwarding

call types 7-56

path 7-56

Forwarding Paths 7-56

Four-Port Single Line Module 17-29

G

Gateway Password 11-65

Gateways

MGCP

address, changing 6-10

creating 6-9

SIP

description 6-6

placing behind a NAT device 6-7

supported 6-6

viewing 6-6

General Connection Issues 17-37

General Endpoint report 15-3

General IP Settings 9-6

General IP Settings Fields 9-7

Greeting 12-26

Greetings, Mailbox 12-26, 12-28, 12-29

Ground start trunks

Hybrid Balance Test 6-17

Ground Start Trunks Timers 10-28

Group Call Pick-Up 8-47

Group Lists 11-49

programming 11-49

Group lists, voice processor, saving and restoring 13-6

Group Page Breaks 15-4

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

Groups

facility

- dialing rules, programming 5-14
- European systems 5-13
- programming 5-13
- trunk groups 5-15
- USA systems 5-13

route

- creating 5-17
- dial groups, programming 5-18
- European systems 5-17
- facility groups, adding 5-19
- USA descriptions 5-16

route, description 5-16

user 5-25

- planning 5-25

Guidelines

- voice processor, saving 13-5

H

Handsfree, enable/disable 7-25

Hangup Message 12-24

Hardware addresses test 14-17

Hardware Upgrade 8-52

Headsets, connect tone 7-25

Hidden Entries in the Voice Mail Directory 7-22

Hold

- alternate hold timer 10-28
- timer 10-28

Home area codes 5-22

Hookflash timers 10-29

Hot-Swapping an Expansion Module 17-7

House Phone 10-21

- day/night numbers 7-62

House Phone Day/Night Numbers 7-62

Hunt Group-Related Information 8-32

Hunt Groups

- ACD agent ID 8-32
- all-ring 8-40
- button 7-43
- camp on 8-47
- camp-on tone 7-25
- capacity 8-32
- extension number 8-32
- linear 8-49

local hunt groups 8-35

members 8-4

remote hunt groups 8-51

station lists 8-32

station monitoring 10-32

supervisor 8-41

using extension lists 8-40

Hunt groups report 15-3

Hybrid Balance, test all loop start interfaces 16-28

Hybrid Balance Test 16-26

loop start and ground trunks 6-17

I

IC-CO Disconnect Timer 10-29

Icons

Database Test and Repair 14-8

DB Studio toolbar 2-14

Identification Prompt 11-21

IMAP IDLE Timeout 12-15

IMAP Polling Timeout 12-15

IMAP Synchronization Method 12-14

Immediate Start Type 6-14

Import Endpoints from CSV Files, troubleshooting 17-30

Inactivity Timer 10-28

Information

error 3-15

Initializing Mailboxes 12-23

Intelligent Directory Search (IDS) Support 7-15

Intercom (IC) Button 7-43

Intercom Calls 7-56

ringback cadence 7-24

Interdigit Long Timer 10-28

Interdigit Short Timer 10-28

CS-5600 Connection Wizard 17-16

ITP Default Feature Codes 10-40

Introduction 7-4, 17-3

IP

devices, status 9-4

resources

reservation, configuring 9-43

Reserved by Device 9-47

Reserved by Function 9-44

Shared Resource Summary bar 9-49

resources, reserving 9-42

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

IP (Internet Protocol) 6-18

- address, Proxy server 3-55
- Communication Timeout 6-21
- connection, creating new 4-8
- devices
 - status 16-42
- Manufacturer, MGCP 6-21
- networking
 - existing node 4-6
- Proxy Server IP Port 3-55
- trunks, call configurations 6-20

IP Call Configuration 8-55**IP Connection Groups 4-4****IP Connection Groups, Node 8-54****IP Connections 9-34**

- local node 9-17
- remote node 9-21

IP Device Audio 17-35**IP Device Audio Troubleshooting Strategies 17-35****IP Device Connection 17-36****IP Device Connection Troubleshooting Strategies 17-36****IP Device Echo 17-38****IP Device Echo Troubleshooting Strategies 17-38****IP Device VLAN Tagging 17-40****IP Device VLAN Tagging-Related Troubleshooting Strategies 17-40****IP Devices 17-32****IP Devices Troubleshooting Strategies 17-32****IP Endpoints 8-53****IP Networking 17-41****IP Networking Troubleshooting Strategies 17-41****IP Port Session Manager 2-7****IP Resource Application (IPRA) 17-32****IP Resources**

- Sharing Log file 16-25
- sharing statistics 16-24

IP Terminal General Purpose UDP Port 9-19**IP Terminal TCP Call Control Port 9-19****IP/Digital Endpoint 8-4****IP/Digital Endpoint Database Programming Password 7-76****IPRA Troubleshooting Strategies 17-32****ISDN Data Calls Allowed 8-24, 8-31****ISDN PRI Two B-Channel Transfer 6-34****J****Japanese language**

- Mitel IP endpoints 7-60, 7-61

Japanese Prompts and Displays

- language selection 7-60, 7-61, 11-36

K**Key (Button) Assignments Folder 7-72****Key Assignments 7-72**

- see* Button Assignments

Keymaps 7-48

- alternate 7-23, 7-48
- DSS 7-39
- report 15-3

Keystroke Summary 2-18**Keystrokes for Navigating a Laptop Without a Mouse 2-18****L****Language 7-60**

- selection 7-60, 7-61, 11-36
- trunks, selecting 6-18

Languages

- for reports 15-2
- primary and secondary, programming for system 10-3

Last Number Dialed/Saved 7-26**Latency Time 11-8****LCD panel, description 16-47****License**

- Category D 3-7
- Mitel endpoints 3-7
- software
 - comparing and uploading 3-11
 - uploading 3-10

Licensing Issues 17-45**Licensing Troubleshooting Strategies 17-45****Linear 4-5**

- hunt group 8-49

Lists

- extension 8-40
- group 11-49
- hunt group station 8-32
- trunk 8-7, 8-28

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

Local

- hunt groups 8-35
- modems 4-25
- node 4-2
- page zones 10-16

Local 7/10 digit dialing 5-4

CO 17-16

Local Fax ID 11-73

Local Hunt Groups 8-35

Local Node 4-2, 9-17

Local nodes 4-2

Local Page Zones 10-16

Logo Document 11-73

Logs, database change 16-6

Loop Loss Measurement

- troubleshooting 17-45

Loop Loss Measurement Test

- description 6-31
- options 6-32
- starting 6-32
- troubleshooting 17-30, 17-45

Loop Start AC Impedance 6-33

Loop Start Trunks

- connected to paging 8-14, 8-15
- timers 10-28

Loop start trunks

- Answer Supervision Types 6-15
- Hybrid Balance Test 6-17
- Polarity reversal 6-15
- Send Digits En Bloc 6-16
- Valid Call Timer 6-15
- Valid Call Timer with Polarity Reversal 6-15

M

Mailbox Greetings 12-26, 12-28, 12-29

Mailbox Initialized 12-20

Mailboxes 7-57, 7-59

- initialization 12-23
- message limits 12-15
- passwords 12-4
- play only 12-25
- programming
 - create an associated mailbox 11-47, 12-4
 - mailbox number 12-5
- receive only 12-4

subscriber statistics 12-16

swap 7 and 9 keys 12-25

user-keyed extension 7-59

Mailbox-Related Information 7-57

Maintenance, system 3-36

Major alarms 16-48

Major reset

- parameters 3-44
- scheduling 3-44

Major reset, forced 3-45

Manual Report Generation 15-10

Maximum

- deleted message space 11-55
- fax delivery attempts 11-69
- fax selections 11-70
- Fax-On-Demand library size 11-70
- Fax-On-Demand ports 11-70
- greeting length 11-55
- mailbox message capacity 12-15
- messages per network call 11-13
- network call attempts 11-13
- network calls 11-14
- network inbound connections 11-14
- network message length 11-14
- network outbound connections 11-14
- non-subscriber message length 12-15
- number of deleted messages 11-55
- outgoing calls 11-55

Medial Gateway Control Protocol *See MGCP*

Members 8-40

Menus

- Database Test and Repair 14-8
- DB Studio
 - File 2-13
 - Help 2-14
 - Options 2-13
 - Tools 2-14
 - View 2-13
- Favorites 2-14

Message Center 7-72

- programming 7-51

Message Centers 7-72

Message Limits 12-15

Message Notification

- endpoint 12-27

Message Notification Endpoint 12-27

Message Notification/Retrieval 11-37

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

Message Print

- description 3-48
- output active 3-49
- output device line width 3-49
- print options 3-49
- queues 3-35

Message Threshold 11-8**Message Threshold for AMIS 11-8****Message, Hangup 12-24****Messages 7-72**

- message wait timer 10-30
- new
 - saving and restoring 13-6
- saved
 - saving and restoring 13-6

Methodology 17-3**MGCP 6-21****MGCP (Media Gateway Control Protocol)**

- Associated Gateway 6-21
- ateways
 - creating 6-9
- endpoints
 - creating 6-10
- gateway
 - address, changing 6-10
 - trunks, Send Digits En Bloc 6-16
- gateway port 6-20
- Manufacturer 6-21
- names 6-21
- Receive Port 9-20

MGCP Receive Port 9-20**Mini-DSS Unit 17-46****Mini-DSS Unit Troubleshooting Strategies 17-46****Minimum Bit Rate 4-25****Minimum Call Progress Signal Duration 11-55****Minimum Call Progress Silence Duration 11-55****Minimum Playback Time 8-55, 9-29****Minor alarms 16-48****Miscellaneous test 14-18****Mitel**

- endpoints
 - converting Inter-Tel to Mitel 7-19
 - Japanese language 7-60, 7-61
 - license 3-7
- Technical Support 2-2

Modem

- access for remote programming 2-10
- auto answer 2-10
- remote, troubleshooting 2-12
- save or restore 2-10

Modems 4-2

- local 4-25
- minimum bit rate 4-25
- off-node 4-24

Monitor Password 11-25**Monitor, Online 2-13****Mouse, using instead of a keyboard 2-18****Multilingual Capability**

- language selection 7-60, 7-61, 11-36

Multiple Ring-In 8-12**Multi-Protocol Endpoint Troubleshooting Strategies 17-47****Multi-Protocol Endpoints 17-47****Music-On-Hold**

- converter utility 14-3
- encoding setting 8-55
- file-based 10-9
- for IC calls 10-21
- parameters 11-44
- persistent 6-29

Music-On-Hold Encoding Setting 8-55**Music-On-Hold Parameters 11-44, 11-45**

N

NAT

- device, placing a SIP gateway behind 6-7
- IP Address 9-18

NAT (Network Address Translation)

- Address Type 6-19
- challenges for SIP devices

NAT Address Type 6-19, 9-40**NAT IP Address 9-18****Network**

- Session Manager connection setting 2-6
- undeliverable messages destination type 11-15

Network Address Translation See NAT**Network alarms****Network Call Failure Threshold 11-14****Network Call Retry Timer 11-14****Network Configuration 9-37****Network Diagram 17-9****Network Diagram Example 17-9****Network Group Assignment 8-52**

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

Network Groups 8-52, 9-40
 Network groups, diagnostics
 Network Node 17-51
 Network Node Troubleshooting Chart 17-51
 Network Timers and Limits 11-13
 Networking
 IP
 configuring for existing node 4-7
 existing node
 configuring 4-6
 T1
 configuring for existing node 4-7
 T1/E1/PRI 4-10
 VPIM 11-9
 No Answer Advance Timer 8-42
 Node IP Connection Group 9-22
 Node IP Connection Groups 8-54
 Node Trunk Groups 8-28
 Nodes 4-2
 Audio for Calls Camped onto this Device 4-5
 call routing announcement 11-32
 devices, importing and exporting 4-19
 import and export status descriptions 4-21
 IP Connection Groups 4-4
 local 4-2
 local node 4-2
 off-node modems 4-24
 remote 4-3
 search algorithms 4-5
 system 4-2
 trunk groups 4-4, 8-28
 Trunk/IP Connection group, adding 4-9
 Voice Processing 11-6
 Node-Spanning Hunt Groups 8-51
 Non-Validated and Validated 7-70
 Notification
 category 12-20
 destination 12-22
 destination type 12-22
 type 12-22
 Notification No-Answer Detection 11-56
 NTP Server Configuration 9-34
 NTP Server Configuration Fields 9-16
 NTP Troubleshooting 9-16
 Number Called Busy Timer 12-21
 Number Of Call Attempts 12-21
 Number of Digits to Receive, DID trunks 6-18
 Number of Voice Channels 11-60

Numbers, emergency programming 5-21

Symbols

NuPoint Messenger, description 11-4

O

Off-Hook Debounce Timer, E&M trunks 6-15
 Off-Hook Delay 11-56
 Off-Hook Voice Announce (OHVA)
 immediate transmit 7-25
 screening timer 10-30
 timer 10-30
 Office codes 5-4
 Off-Node
 device, wildcard 7-14
 mailboxes 12-7
 Off-node device 4-24
 Off-node devices
 report 15-3
 Off-Premises Extension (OPX)
 ring cadence 7-25
 transmit gain 7-25
 OHVA Enable 10-22
 OLM (On-Line Monitor)
 enabling in DB Studio 2-13
 OLM (Online Monitor) 16-47, 16-48
 diagnostics
 OLM 16-46
 system diagnostic commands 16-46
 Onboard TFTP server
 Database Programming settings 9-14
 One-Way Incoming Trunk Groups 8-22
 On-Line Monitor See OLM
 Online Monitor *see OLM*
 Operator Access wildcard 5-23
 Outgoing Access 8-30, 11-72, 12-22
 Fax-On-Demand 11-72
 node IP connection groups 8-56
 node trunk groups 8-30
 Outgoing Access Prefix 11-72, 12-22
 Outgoing Access Termination 11-72
 Outgoing Call Button 7-52
 Outgoing DTMF Digit Duration 11-56
 Outgoing Termination 12-22
 Outside Calls
 alerting cadence 7-24

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

- outgoing trunk access 7-52
- ringback cadence 7-24
- Outside Party Call Information 7-25
- Overflow 8-42
- Overflow Endpoints 8-45
- Overflow Timer 8-42
- Override Language 11-36
- Oversubscription/IP Resource Sharing Statistics 16-24
- Oversubscription/IP Resource-Sharing 17-52
- Oversubscription/IP Resource-Sharing Troubleshooting Strategies 17-52

P

- Page Zone Keys 7-43
- Page Zones 10-15, 10-17
- Pager Dial String 12-22
- Pager Notification Retry Timer 12-21
- Paging
 - remove/replace 7-26
 - timer 10-30
- Parameters
 - backup database 3-12
 - major reset 3-44
 - system, programming 10-2
- Password 12-26
- Passwords
 - extension ID 11-48
 - ip/digital endpoint database programming 7-76
 - mailbox 12-4
 - Voice Processing monitor 11-25
- Patterns
 - call routing 6-24
 - adding 6-26
 - batch creating 6-27
 - copying 6-27
 - deleting 6-26
 - editing 6-25
 - options 6-25
 - viewing 6-26
- Pause Timer 10-30
- Pause Voice Mail 11-56
- PBX 8-17
- Persistent Music-On-Hold Selection 6-29
 - troubleshooting 17-53
- Personal Number No Answer Timer 12-21
- Phantom Devices 7-67, 17-54
- Phantom Devices Troubleshooting Strategies 17-54
- Phone List report 15-3
- Pilot Numbers 8-32
- Play only mailbox 12-25
- Play Recording Instructions 12-23
- Polarity reversal
 - loop start trunks 6-15
 - trunk-to-trunk calls 6-16
- Preliminary Activities 17-5
- Primary and Alternate Message Notification 12-20
 - add a cascade level 12-21
 - delete a cascade level 12-21
 - programming cascade settings 12-21
- Primary Attendant 7-74, 7-79
- Primary Attendants 7-74
- Printing
 - manual reports 15-11
 - reports 15-5
- Priority Latency Time 11-8
- Priority Level 8-47
- Private Networking Wizard
 - starting 4-6
- Processes 17-5
- Processing Server (PS-1) 17-57
- Processing Server Troubleshooting Strategies 17-57
- Processor Module (PM-1) 17-56
- Processor Module (PM1) Modem Troubleshooting Strategies 17-56
- Programmable Fields for the Unified Messaging Folder 12-12
- Programmable Keys 7-42
- Programming 1-1, 2-1, 11-1
 - ACD hunt group flag 8-44
 - an emergency extension for IP devices 9-36
 - analog voice mail hunt group flag 8-44
 - announcement, overflow endpoints for hunt groups 8-45
 - camp-ons allowed for hunt groups 8-47
 - hunt group agents 8-38
 - hunt group members 8-40
 - hunt group priority level 8-47
 - hunt group search type 8-49
 - hunt group supervisors 8-41
 - hunt group timers 8-42
 - ip/digital endpoint database 7-76
 - use ACD agent IDs for hunt groups 8-51
- Programming a Report 15-4
- Programming an Emergency Extension for IP Devices 9-36
- Programming BVM Timers and Limits 11-54
- Programming Command and Event Ports 11-61
- Programming Description and Username Fields for Local Devices 7-15

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

Programming Keymap Buttons 7-42
Programming Local Endpoints 7-22
Programming the ACD Hunt Group 8-33
Propagate Original Caller ID 8-26
Propagate Original Caller ID on Transfer 7-26
 for voice mail applications 11-46
Propagate Original Caller ID on Transfer (Voice Mail) 11-46
Propagate Original Caller ID 8-26
Proxy Server
 Hostname/IP address 3-55
 IP Port 3-55
Proxy server, Remote Configuration 3-55

Q

Query options, database 16-39
Queue Callback Timer 10-30
Queues, Message Print 3-35
Quota Grace 12-29
Quota Warning 12-29

R

Raw commands 16-49
Recall 8-42
 hunt group timer 8-42
 timer 10-30
Recall Destination Endpoint 8-48
Receive Network Alarms 10-22
Receive Only 12-23
Record-A-Call 7-77, 10-22, 11-38
 mailbox 7-77
 tone 10-22
 tone interval timer 10-30
Record-A-Call Application 7-60
Record-A-Call Max Message Length 11-56
Record-A-Call Operation 7-58
Recording Length 12-15
Recording Silence Detection 11-56
Redialing mode 7-26
Referential Integrity
 DB Test, Referential Integrity 14-19
Referential Integrity test 14-19

Remote
 hunt groups 8-51
 IP address 9-22
 Listening Port 9-23
 page zones 10-17
 voice processor
 database, saving 13-8
Remote (Off-Node) Hunt Groups 8-51
Remote Audio Receive Port 9-23
Remote Configuration 3-54
 Customer Care utility 3-56
 enabling 3-54
 enabling 3-54
 Remote Connection 2-7
 Remote Proxy Server Timeout 2-6
 utility 3-54
 utility, on-demand connection 3-55
 View IP Port 2-6
Remote Connection
 Remote Configuration 2-7
Remote Hunt Groups 8-51
Remote IP Address 9-22
Remote Listening Port 9-23
Remote Messaging 12-19
Remote Node 8-57, 9-21
Remote nodes 4-3
Remote Page Zones 10-17
Remote programming
 modem access 2-10
 modem, troubleshooting 2-12
Remote Programming Invalid Extension Failure Limit Timer 10-30
Remote Programming Password Failed Limit 10-30
Remote Proxy Server Timeout 2-6
Replay Forward/Rewind Increment 11-56
Reports
 ARS Facility Group 15-3
 ARS Route Group 15-3
 automatically generating 15-8
 Call Routing 15-3
 Class of Service 15-3
 CO Trunk Groups 15-3
 description 15-2
 Detailed Endpoint 15-3
 directory 15-7
 Endpoint Flags 15-3
 fax delivery 15-7
 fax documents usage 15-7
 General Endpoint 15-3

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

Reports (Continued)

- generating manually 15-10
- Hunt Group 15-3
- Individual Trunk 15-3
- Keymaps 15-3
- languages used 15-2
- manual reports, selecting 15-10
- manual, printing 15-11
- Off-Node Devices 15-3
- Phone List 15-3
- print day, selecting 15-9
- print time, selecting 15-9
- printing 15-5
- programmingf 15-4
- selecting 15-8
- System Health 3-40
- System Speed Dial 15-3
- System Timers 15-3
- T1/E1/PRI 15-3
- Trunk Group 15-3
- User Group 15-3

Reseize 7-24**Reseize Timer 10-24****Reservation**

- IP resources 9-42

Reserve IP Resources 6-18**Reserve IP Resources for trunks and devices 6-18****Reserved By Device**

- description 9-47

Reserved by Function

- options 9-45

Reset

- Call Processing 3-44
- major, forced 3-45
- major, scheduling 3-44
- scheduled time 3-45
- system requires 3-45
- system, immediate 3-44

Reset system dialog box 3-47**Resetting**

- call processing 3-3

Resource Reservation Tool

- Advanced tab 9-48
- constraints 9-42
- Reserved by Device
 - description 9-47
- Reserved by Function
 - description 9-44
 - options 9-45
- resources, configuring 9-43
- Shared Resource Summary bar 9-49

Resource Reservation Tool, description 9-42**Restart ACD Idle Time Upon Login 8-48****Restoring**

- backup database 3-14
- BVM Data to an NFS-supported computer 13-20
- CS-5600 database from remote computer 13-15
- EM database 13-11
- Mitel CS-5600 BVM data 13-19
- voice processor database 13-3
- voice processor, completing 13-8

Restoring and saving

- voice processor options 13-4
- voice processor to location 13-5
- voice processor, completing 13-7

Restricted area codes 5-26**Retry ARS Call If Call Rejected 17-58****Retry ARS Call If Call Rejected Troubleshooting Strategies 17-58****Return ACD Calls to Hunt Group 8-49****Return Call Feature 11-20****Rights, programming access 3-5****Ring Cadence 7-25****Ring Flash on DSS Lamps 10-22****Ring Frequency 10-29****Ring Intercom Always 7-26****Ring Principal Once 7-56****Ring When X Calls At Extension 7-43, 7-47****Ringback Cadences 7-24****Ring-In 7-56, 8-24**

- alerting cadence 7-24
- programming 8-25
- type 6-27

Route Group Dial Patterns for European Systems 5-18**Route Group Dial Patterns for U.S. Systems 5-18****Route Groups**

- default values, international 5-17

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

Route groups

- audio settingsGroups
 - route audio settings 5-20
- creating 5-17
- description 5-16
- dial patterns, programming 5-18
- European systems 5-17
- facility groups, adding 5-19
- USA descriptions 5-16

S

Sample Speech Recognition Combinations 11-23

save and restore options 13-6

Save Message on Return Call 11-20

Save or restore using a modem 2-10

Saved messages, saving and restoring 13-6

Saving

- backup database 3-14
- BVM Data to an NFS-supported computer 13-20
- CS-5600 database from remote computer 13-15
- EM database 13-11
- Mitel CS-5600 BVM data 13-19
- voice processor database 13-3
- voice processor, completing 13-8

Saving and restoring

- voice processor options 13-4
- voice processor to location 13-5
- voice processor, completing 13-7

Scheduled backups

- database 3-15
- troubleshooting 17-58

Scheduled reset time 3-45

Schedules 1-20 11-39

Screened Transfer 12-27

SDN Data Calls Allowed 8-31

Search Algorithm 8-30

- node trunk group 4-5
- trunk group 8-30

Search algorithms, linear or distributed 4-5

Search algorithms, node 4-5

Search Type 8-49

Secondary Extension Keys

- assigning 7-43

Secondary Language 7-61

Select Fax Document 11-34

Selection wizards 2-16

Send Alert Burst to Headset 7-26

Send Camp On Notifications to Members in DND 8-50

Send Digits En Bloc, loop start and MGCP trunks 6-16

Send Network Alarms 10-22

Send Station Caller ID to Attached PBX 8-26

Send T1 OPX Disconnect Flash 7-26

Servers

Proxy

- IP address 3-55
- IP Port 3-55

Session Initiation Protocol *See SIP*

Session Manager

- connection options 2-9
- Connection tabs 2-7
- description 2-4, 2-7
- IP Port 2-7
- IP Port settings 2-6
- language, selecting 2-6
- Network Connections settings 2-6
- Session menu 2-5
- session, starting 2-8
- Settings menu 2-6

Setting a Password 9-35

Shortcut tool 2-14

Shortest Message Allowed 11-56

Single Line Endpoint Troubleshooting Strategies 17-70

Single Line Endpoints 17-70

- off-premises stations ring cadence 7-25
- off-premises stations transmit gain 7-25
- timers 10-31

Single Line Module (SLM-4) Troubleshooting Strategies 17-29

Single Ring In 8-24

Single-Line Extension Types 8-4

SIP (Session Initiation Protocol) 9-26

SIP (Session Initiation Protocol)

gateways

- description 6-6
- placing behind a NAT device 6-7
- supported 6-6
- viewing 6-6

NAT challenges

trunks

- creating 6-8
- description
- options 6-8
- viewing 6-6

SIP and ITP Default Feature Codes 10-39

SIP and ITP Mode Functions for Show IP Feature 10-39

SIP Default Feature Codes 10-39

SL Hookflash Minimum 10-31

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

SMDR (Station Message Detail Recording)

- description 3-50
- devices 3-50
- DID 3-52
- display "O/I" for operator and international calls 3-51
- display elapsed time 3-51
- display redirected station 3-52
- local backup port 3-50
- maintenance 3-50
- output active 3-51
- output port 3-50
- record calls options 3-52
- suppress digits options 3-53
- System Manager, output to 3-51

Sockets 9-34**Software**

- license, comparing and uploading 3-11
- license, uploading 3-10

Software license features

- analog voice mail 8-44

Speech Encoding Setting 9-30, 9-34**Speech Recognition Enabled 11-24****Speech Recognition Setting 11-24****Standard Account Codes 7-69****Standard Keymap 7-48****STAR**

- See* Scheduled Time-Based Application Routing (STAR)

Start Type, Delay Dial 6-14**Start Types**

- Dial Tone 6-14
- DID trunks 6-14
- E&M trunks 6-14
- Immediate 6-14
- Wink 6-14

Start/Stop Time 11-72

- Message Notification 12-20

Static Records

- DB Test, Referential Integrity 14-20

Static Records test 14-20**Static records, testing 14-20****Station Message Detail Recording *See* SMDR****Station Monitor Timer 10-32****Station Speed Dial Button 7-43****Stations, account codes 7-69****Statistics**

- channel 15-7
- clearing 15-8
- disk usage 11-18
- mailbox subscriber 12-16
- manual reports, clearing 15-10
- system software performance 16-40

Status

- IP device 9-4

Subject to Toll Restriction 8-16**Subscriber 11-34**

- statistics 12-16

Subscriber Statistics 12-16**Supervisors 8-41****Supports RTP Redirect 9-33****Swap 7 and 9 keys 11-21**

- mailbox 12-25

Synchronize MWI with E-mail Client 12-14**System**

- administrator mailbox 11-18
- alarm #203 11-5
- alarms
 - clearing 16-36
- backup database parameters 3-12
- date, programming 10-2
- diagnostics 16-48
- Echo Profiles 6-16, 10-5
- error reporting 16-48
- error/message printing 16-48
- force reset if not idle 3-45
- maintenance 3-36
- OLM application commands 16-47
- OLM diagnostics commands 16-46
- parameters, programming 10-2
- primary and secondary languages, programming 10-3
- prompts
 - voice processor, saving and restoring 13-6
- requires reset 3-45
- reset
 - dialog box 3-47
 - immediate 3-44
- time
 - programming 10-2
- time zone
 - programming 10-3
- voice processor
 - enabling and disabling 13-8

System Administrator

- creating an administrator endpoint 7-23

System Administrator Default Feature Codes 10-41

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

System Administrator Mailbox 11-18

System Conditions 7-56

System device information 16-37

System Features 17-73

System Features Troubleshooting Strategies 17-73

System Forwarding 7-26

- advance timer 10-31
- initiate timer 10-31
- paths 7-74
- timers 10-31

System Forwarding Paths 7-74

System Health Report 3-40

- troubleshooting 17-73

System Manager

- CA certificate, uploading 4-27
- description 4-26, 16-49
- enable connection 4-26
- IP address 4-26
- password 4-26
- port 4-26
- SMDR output to 3-51
- user name 4-27

System Reset Analysis 17-6

System Speed Dial 7-75

- report 15-3

System Speed Dial Button 7-43

System Speed Dialing 7-75

- toll restriction override 10-23

System Timers 10-24

- default values 10-24

System Timers 10-24

System-Level Issues 17-77

System-Level Troubleshooting Strategies 17-77

T

T.38 9-32

T1/E1 PRI

- networking 4-10

T1/E1/PRI

- Busy Out
 - Manager 16-4
 - statuses 16-5

T1/E1/PRI Modules 17-80

T1/E1/PRI Report 15-3

T1/E1/PRI Troubleshooting Strategies 17-80

Talk-off 11-57

TCP Call Control Port 9-20

Technical Support 2-2, 17-89

Tests

- Database Test and Repair
 - Associated Mailbox 14-11
 - Boards 14-12
 - Cleanup 14-13
 - common errors 14-10
 - Devices 14-13
 - Dynamic Enumerations 14-15
 - Extensions Conflict 14-16
 - guidelines 14-9
 - Hardware Addresses 14-17
 - menus 14-8
 - options 14-9
 - static records 14-20
- Database Test and Repair Test
 - Enumerations 14-16
- DB Test
 - Referential Integrity 14-19
 - Static Records 14-20
- Loop Loss Measurement 6-31

TFTP (Trivial File Transfer Protocol)

- uploading firmware 14-21

TFTP server

- onboard, Database Programming settings 9-14

TFTP Settings 9-14

TFTP Settings Fields 9-14

The New Key Assignments Folder for v2.4 7-40

Time

- Daylight Saving, programming 10-3
- programming 10-2
- zone, programming 10-3

Time Display

- format 10-23

Time Slot Group 11-45

Time Slot Groups 11-45, 11-52

Time Zone 12-28, 12-29

Timer 7-80

Timers 7-80, 8-42, 11-13, 11-69

- abandoned call 10-24
- agent help tone interval 10-24
- alternate hold 10-28
- AMIS 11-8
- announcement 8-42
- Answer Recognition 6-15
- camp-on tone 10-24
- CO reseize 10-24
- CO/IC Reseize 7-24, 10-24
- CO-CO Disconnect 10-29
- default values 10-24

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

Timers (Continued)

- dial initiation 10-22, 10-24
- dialing 10-24
- DID 10-24
- DID disconnect recognition 10-24
- DID impulse-dial inter-digit pause recognition 10-24
- DID off-hook debounce 10-25
- DID on-hook debounce 10-25
- DID post-seize delay 10-25
- DID post-signal delay 10-25
- DID pre-signal delay 10-25
- DID ready timeout 10-25
- DID ready timeout delay 10-25
- DID seizure recognition 10-25
- DID signal hold 10-25
- Digital/IP alternate transient display 10-25
- Digital/IP secondary extension button altering tone 10-25
- DISA invalid extension failure limit 10-25
- DISA security code failure limit 10-25
- disconnect wait after dialing 10-25
- DTMF digit duration/pause 10-26
- DTMF signaling 10-26
- E&M answer recognition 10-26
- E&M dial delay 10-26
- E&M dial delay hold 10-26
- E&M dialing wait after hookflash 10-26
- E&M disconnect flash duration 10-26
- E&M disconnect recognition 10-26
- E&M false signal debounce 10-26
- E&M handshake timeout 10-26
- E&M hookflash duration 10-26
- E&M hookflash recognition 10-26
- E&M impulse-dial inter-digit pause recognition 10-26
- E&M off-hook debounce 10-27
- E&M on-hook debounce 10-27
- E&M output-pulse-dial inter-digit pause 10-27
- E&M output-pulse-dial inter-pulse pause 10-27
- E&M post-seize delay 10-27
- E&M post-signal delay 10-27
- E&M pulse hold 10-27
- E&M ready timeout 10-27
- E&M receive handshake delay 10-27
- E&M seizure debounce 10-27
- E&M trunks 10-26
- E&M wait for dial tone 10-27
- E&M wink hold 10-27
- E&M wink timeout 10-28
- fax on demand 11-69
- forward no answer 10-28
- ground start 10-28
- GS dialing wait after connect 10-28
- GS tip-ground debounce 10-28
- GS transition delay 10-28
- hold 10-28
- hold - alternate 10-28
- hookflash 10-29
- IC-CO disconnect 10-29
- inactivity 10-28
- inactivity alarm 10-28
- interdigit long 10-28
- interdigit short 10-28
- LS dialing wait after connect 10-28
- LS/GS caller ID relay hold 10-28
- LS/GS caller ID ring idle 10-29
- LS/GS CO hookflash 10-29
- LS/GS CO-CO disconnect 10-29
- LS/GS dialing disconnect 10-29
- LS/GS dialing wait after hookflash 10-29
- LS/GS IC-CO disconnect 10-29
- LS/GS inter-ring silence 10-29
- LS/GS loop current debounce 10-29
- LS/GS output-pulse-dial inter-digit pause 10-29
- LS/GS output-pulse-dial inter-pulse pause 10-29
- LS/GS output-pulse-dial pulse hold duration 10-29
- LS/GS ring frequency - high boundary 10-29
- LS/GS ring frequency - low boundary 10-29
- LS/GS trunk ring detection 10-30
- Message Wait 10-30
- no answer advance 8-42
- Off-Hook Debounce 6-15
- off-hook voice announce screening 10-30
- OHVA 10-30
- overflow 8-42
- Page 10-30
- pause 10-30
- pause dialing digit length 10-30
- queue callback 10-30
- recall 10-30
- Record-A-Call tone interval 10-30
- re seize 10-24
- single line disconnect flash duration 10-31
- single line hookflash 10-31
- SL Inpulse-Dial Inter-Digit Pause 10-31
- SL wait for disconnect 10-31
- station monitor 10-32
- System 10-24
- system forward advance 10-31
- system forward initiate 10-31
- transfer 10-31
- transfer attendant 10-31

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

Timers (Continued)

- transfer available 10-31
- transfer busy 10-31
- transfer Voice Processing Unit 10-31
- trunk key debounce 10-32
- unsupervised CO 10-32
- update message latency period 11-14
- valid call 10-32
- Voice Processing network 11-13
- wrap-up 8-42

Timers and Limits 11-13, 11-69

Toll Digit Allowed on Toll Local Calls 5-4

Toll Digit Required on Toll Long Distance Calls 5-4

Toll Restriction 8-16

- trunk groups 8-16

Toll strings

- European wildcards 5-23
- USA wildcards 5-23
- wildcards, toll string 5-23

Tools

- shortcut 2-14

Transfer

- method 11-48
- recall destination 7-52
- timers 10-31

Transfer Method 12-27

Transfer Method, Associated Mailbox 12-27

Transfer No-Answer Detection 11-56

Transfer Recall Destination 11-45

Transfer Timers

- attendant 10-31
- available 10-31
- busy 10-31
- Voice Processing Unit 10-31

Transfer To

- collected extension 11-34
- extension 11-34
- mailbox 11-34
- node 11-34
- operator 11-35

Transient Call Indication 7-26

Transmit DTMF Level 9-30

Troubleshooting 17-3

- Caller ID Forwarding 17-13
- charts 17-10
- Database Change Log 17-20
- File-Based Music-On-Hold 17-28
- importing endpoints from CSV files 17-30

Loop Loss Measurement 17-45

Troubleshooting (Continued)

- Persistent Music-On-Hold Selection 17-53
- remote modem 2-12
- scheduled backups 17-58
- System Health Report 17-73
- Tests

- Loop Loss Measurement Test 17-30, 17-45

Troubleshooting Charts 17-10

Troubleshooting Guidelines 17-6

Troubleshooting Process Flow Diagram 17-3

Troubleshooting Strategies for UPS Monitoring Issues 17-83

Trunk,button 7-43

Trunk Group keys 7-43

Trunk Groups

- allowed answer 8-9, 8-12, 8-13, 8-14, 8-15, 8-16, 8-18, 8-19, 8-20, 8-21, 8-22, 8-23, 8-24, 8-26, 8-27, 8-30, 8-31, 8-56
- one-way incoming 8-22
- ring in 8-25
- toll restriction 8-16

Trunk groups

- Calling Party Name 8-26
- Calling Party Number 8-26
- for facility groups 5-15
- node 4-4
- report 15-3

Trunk Key Debounce Timer 10-32

Trunk List 8-7, 8-28

Trunk Service Types, descriptions 6-13

Trunks 8-53, 17-16

- access codes 10-33
- assigning to CO trunk groups 6-5
- Batch Extension Exchange 6-4
- call configurations 6-20
- call routing keys 6-23
- call routing tables 6-22
- CO reseize 7-24
- copying 6-5
- CP History 6-20
- descriptions 6-3
- extension numbers, changing 6-4
- Individual Trunk report 15-3
- IP Reserve IP Resources 6-18
- language, selecting 6-18
- Node Trunk/IP Connection group, adding 4-9
- options, programming 6-11
- outgoing access 7-52

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

SIP

- creating 6-8
- description
- options, programming 6-8
- viewing 6-6

Trunk Service Types 6-13

- descriptions 6-13

- viewing 6-4

Twist Parameters 11-57

U

UCD Station-Monitor Indications 10-23

Unannounced 12-27

Undefined Button 7-43

Undeliverable Messages 11-15

Undeliverable Messages Destination Type 11-15

Unified Messaging 11-18, 12-11, 12-18

Unified Messaging Level 12-13

Unified Messaging Levels for BVM, VPU, and EM 12-11

Unlisted Number

- private extension 11-48

Unsupervised CO Timer 10-32

Update Message Latency Period Timer 11-14

Upgrade Process 17-82

Upgrade Process Troubleshooting Strategies 17-82

Uploads, System Manager CA certificate 4-27

UPS Monitoring 17-83

USB drive, saving and restoring voice processor information to 13-5

USB Flash Drive, save and restore voice data 13-7

Use ACD Agent IDs 8-51

Use Green LEDs For Direct Rings 10-23

User group Day/Night list 5-27

User groups 5-25

- area codes, programming 5-26

- planning 5-25

User-Keyed Extension 7-52

User-Keyed Extension Examples for Agent Help 7-52

Using the Wildcard Character in Extensions 7-14

Utilities

- Customer Care Remote Configuration

- enabling 3-54

- enabling with endpoint 3-56

- Database Test and Repair

- menus 14-8

- database, viewing 14-2

- Database Converter

- description 14-23

Utilities (*Continued*)

- Mitel 5000 DB conversions 14-24

- notes 14-23

Database Test and Repair

- Associated Mailbox 14-11

- Boards 14-12

- Cleanup 14-13

- common errors 14-10

- description 14-7

- Devices 14-13

- Dynamic Enumerations 14-15

- Enumerations 14-16

- Extensions Conflict 14-16

- guidelines 14-9

- Hardware Addresses 14-17

- icons 14-8

- Miscellaneous 14-18

- options 14-9

MOH 14-3

Remote Configuration 3-54

- description 3-54

- on-demand connection 3-55

V

Valid Call Timer 10-32

- loop start trunks 6-15

Valid Call Timer with Polarity Reversal

- loop start trunks 6-15

Validate Off-Node Mailboxes 11-15

Validate Voice Mailbox Number 10-23

Validated Account Codes 7-69

Validated Flag 7-60

Version 2.4

- Database Converter Utility changes 14-18

View IP Port 2-6

Virtual Local Area Network (VLAN) Tagging Support 4-2

Voice Channels 11-60

Voice Data, save and restore to USB 13-7

Voice Mail 11-41

- extension 7-52

- information 11-52

- timers 10-32

Voice mail

- swap 7 and 9 keys 11-21

Voice Mail Application Programming Fields 11-42

Voice Mail Extension 7-52

Voice Mail Information 11-52

A - B - C - D - E - F - G - H - I - J - L - M - N - O - P - Q - R - S - T - U - V - W - X

- Voice mailbox, information, saving and restoring 13-6
- voice mails, adding to call configuration 9-26
- Voice Only 12-10
- Voice Processing 17-83
 - diagnostics
 - description 16-42
 - maintenance 7-57
 - network 11-6
 - nodes 11-6
 - number of voice channels 11-60
 - Record-A-Call 11-38
 - system-wide information
 - alternate tone detection 11-19
 - dial-0 destinations 11-18, 12-18
 - disk usage statistics 11-18
 - monitor password 11-25
 - system administrator mailbox 11-18
 - system message on return call 11-20
 - volume 11-20
 - timers and limits 11-53
- Voice Processing Troubleshooting Strategies 17-83
- Voice Processor
 - enabling and disabling 13-8
 - guidelines for saving information 13-5
 - maintenance 7-57
 - nodes 11-6
 - save and restore options 13-4
 - timers and limits 11-53
- Voice processor 13-6
 - database save and restore 13-3
 - remote mode
 - saving database 13-8
 - save and restore, completing 13-8
- Voice Processor Maintenance 7-57
- Voice Processor Nodes 11-6

- Voice Processor Timers and Limits 11-53
- Voice Processor Timers and Limits 11-54
- Voice Profile for Internet Mail (VPIM) Networking 11-9
- VOIP (Voice Over Internet Protocol)
 - Echo Canceller 10-8
- Volume 11-20
- VPIM (Voice Profile for Internet Mail)
 - home domain 11-19
 - Networking 11-9
- VPIM (Voice Profile for Internet Mail)
 - domain name 9-9

W

- Wait for ISDN Caller ID Information 8-26, 8-27
- Web Listening Port 9-20
- Web/SSH Settings 9-13
- Web/SSH Settings Fields 9-13
- Wildcards 7-14
 - Equal Access 5-23
 - European toll string 5-23
 - Operator Access 5-23
 - USA toll string 5-23
- Wink Start Type 6-14
- Wizards
 - Private Networking
 - starting 4-6
 - selection 2-16
- Wrap-Up Mode for ACD Calls 8-42, 10-23

Z

- Zones, page 10-15

Part No. 580.8006
Issue 3.0, October 2008

