553-3001-102/555-4001-135

Meridian 1 and Succession Communications Server for Enterprise 1000/
Meridian SL-100

Meridian Integrated Conference Bridge

Service Implementation Guide

MICB 3 Standard 01.06 June 2002

NORTEL NETWORKS™

Meridian 1 and Succesion Communications Server for Enterprise 1000/
Meridian SL-100

Meridian Integrated Conference Bridge

Service Implementation Guide

Publication number: 553-3001-102/555-4001-135
Product release: MICB 3
Document release: Standard 01.06
Date: June 2002

Copyright © 2002 Nortel Networks,
All Rights Reserved

Printed in the United States of America.

NORTEL NETWORKS CONFIDENTIAL: The information contained in this document is the property of Nortel Networks. Except as specifically authorized in writing by Nortel Networks, the holder of this document shall keep the information contained herein confidential and shall protect same in whole or in part from disclosure and dissemination to third parties and use same for evaluation, operation, and maintenance purposes only. Changes or modifications to the Meridian switch without the express consent of Nortel Networks may void its warranty and void the user's authority to operate the equipment.

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

*Nortel Networks, the Nortel Networks logo, MAP, Meridian, Meridian 1, MSL, Nortel, Northern Telecom, NT, SL-1, SL-100, Succession, and SuperNode are trademarks of Nortel Networks.

Publication history

June 2002

Version 01.06, MICB 3, Standard. Additional upgrade procedures added.

May 2002

Version 01.05, MICB 3, Standard. First standard version for MICB 3.

May 2002

Version 01.04, MICB 3, Preliminary. Updated with internal additional review comments.

March 2002

Version 01.03, MICB 3, Preliminary. Updated with internal additional review comments.

March 2002

Version 01.02, MICB 3, Draft. Updated with internal review comments.

February 2002

Version 01.01, MICB 3, Draft. This is the first draft for MICB Release 3 for internal review purposes. This version combines the following two MICB 2 documents into a single guide:

- **Meridian 1** – *Meridian Integrated Conference Bridge Description, Installation, Administration, and Maintenance*, 553-3001-102
- **Meridian SL-100** – *Meridian Integrated Conference Bridge Reference Manual,* 555-4001-135

Contents

About this document xi

Product description 15

Purpose 15
MICB description 15
Conference administration 15
System overview 16
MICB conference feature summary 17
Hardware overview 18
MICB hardware design characteristics 19
External equipment 23
MICB operation 24
Join the conference using the direct meeting access method 25
Join the conference using the single DN access method 26
Expand the conference 29
End the conference 29

Engineering guidelines 31

Purpose 31
System requirements 31
Software 31
Hardware 32
System compatibility 33
Meridian 1 and Option 11 33
CSE 1000 33
Meridian SL-100 system compatibility 33
Automatic call distribution resource allocation 33
LAN configuration 35
Global internet access 35
LAN/intranet access only 37
Notes 39
Summary of LAN installation information 40

Installation and configuration 41

Purpose 41
Getting started 41
Unpack and inspect the equipment 41
Take inventory 42

Verify IPE Slot(s) 42
Determine the access method 42
Meridian 1 and CSE 1000 configuration 42
Summary 43
Assign ACD DNs 43
Define Phantom TN blocks 44
Configure DNs for a dual-card conference 47
Meridian SL-100 configuration 50
Single-card configuration 50
Dual-card configuration 55
MICB installation and configuration procedures 60
MICB Installation Wizard 67
Overview 67
Step 1 – Basic Card Settings 67
Step 2 – Access Numbers 70
Step 3 – Define First User 71
Step 4 – Dual Card Meetings 71

Browser user interface 75

Purpose 75
Overview 75
User types 76
Log into the BUI 76
Login password change 78
Customize the BUI home page and title bar 79
Fixed title frame 79
Scheduling BUI 81
Meetings List window 81
Scheduling window 84
Chairperson operations 91
Meeting Control window 91
Administration BUI 96
Introduction 96
MICB Dashboard 98
Settings 99
E-mail template 101
Customize greetings 102
Company images upload 105
Upgrades 107
Users 107
Call-out Groups 113
Permanent Conferences 120

Telephone user interface 125

Purpose 125
Overview 125
Active conference 125
Scheduling and recording features 125
TUI operation during an active conference 126
Chairperson features 126

Features available to all participants 133
Conferee features 135
TUI services 136
Schedule a conference 136
Record a brandline greeting 137
Record a conference-specific greeting 138

Maintenance 141

Purpose 141
Maintenance overview 141
Problem solving 143
Diagnostic tools 143
MICB status LED indicator 143
Self-test 144
Sanity monitoring 145
Diagnostic commands 145
TCP/IP connectivity test 146
CLI command summary 147
Using CLI commands 147
MICB CLI commands 148
MICB fault isolation and correction 150
Card replacement 151
Error message handling 151
Error messages format 152
Error message procedures 153
Advanced troubleshooting 155
Backup and restore procedures 155
Backup 156
Restore 159
Backup and restore process log 160

Reports 161

Purpose 161
Overview 161
BUI Report Viewer 162
Short Connection Report 163
BUI Short Connection Report 163
CLI Short Connection Report 163
Meetings Log Report 164
BUI Meetings Log Report 164
CLI Meetings Log Report 165
Overbooking Report 166
BUI Overbooking Report 166
Overbooking Report (.CSV) 167
Billing Report 168
Introduction 168
BUI Billing Report 169
Billing Report (.CSV) 169
Meridian 1 Call Detail Recording 173
CDR example scenarios 175

Maintenance (Error) Report 175
BUI Maintenance (Error) Report 175
CLI Maintenance (Error) Report 176

Upgrades 177
Purpose 177
Overview 177
Keycode security 179
Planning for an upgrade 179
Managing the user community during an upgrade 180
Upgrade procedures 180
Card upgrade 180
Port Upgrade 181
Firmware Upgrade 182
Upgrade to the single DN access method 184
Upgrade from a stand-alone to a dual-card MICB 185

Appendix A: Password security 187
Purpose 187
Access permissions 188
Unsuccessful login attempt handling 189
Password parameters summary 190
Reset passwords 191
CLI Password Editor editing session 193

Appendix B: Product integrity 195
Environmental specifications 195
Regulatory standards 196
Safety 196
Electro-magnetic compatibility (EMC) 197

List of terms 199

About this document

Purpose and audience

This document instructs system administrators and installers how to install, configure, operate, and maintain the Meridian Integrated Conference Bridge (MICB) as a part of the overall Meridian system. In this guide, Meridian system refers to either the Meridian 1, Succession Communications Server 1000 (CSE 1000), or the Meridian SL-100 switch. The MICB card allows you to schedule and configure multiple simultaneous conferences.

You can install the MICB card in either the Meridian 1, CSE 1000, or Meridian SL-100. In the majority of places the MICB operates the same way regardless of the system in which you install it. When the information differs between the systems, this guide contains separate sections for the Meridian 1 and CSE 1000, and the Meridian SL-100 (for example, configuration information).

Structure

This document contains the following sections:

- **“Product description” on page 15** – describes how the MICB operates and the conference features it provides, as well as the card hardware and software characteristics.
- **“Engineering guidelines” on page 31** – describes MICB system resource allocation, and software and hardware requirements.
- **“Installation and configuration” on page 41** – describes how to prepare the Meridian SL-100 equipment, install the MICB into the Intelligent Peripheral Equipment (IPE) module, connect the MICB to the administration terminal, and configure the MICB. This chapter contains separate configuration sections for the Meridian 1 and CSE 1000, and the Meridian SL-100.

- **“Browser user interface” on page 75** – describes how to use the browser user interface (BUI), a web-based server, for conference administration and scheduling, as well as user administration and maintenance of the MICB.
- **“Telephone user interface” on page 125** – describes how to use the telephone user interface (TUI) for simple conference reservation, as well as lists commands available to participants during an active conference.
- **“Maintenance” on page 141** – shows how to perform maintenance and troubleshooting operations. Includes a description of the Command Line Interface (CLI).
- **“Reports” on page 161** – introduces the reports that the MICB can generate and describes billing.
- **“Upgrades” on page 177** – provides procedures for upgrading to MICB 3 from previous releases.
- **“Appendix A: Password security” on page 187** – describes MICB password protection and access restrictions.
- **“Appendix B: Product integrity” on page 195** – provides environmental specifications and shows regulatory standards.
- **“List of terms” on page 199** – describes the terms used in this guide.

How to check the version and issue of this document

The version and issue of the document are indicated by numbers (for example, 01.01).

The first two digits indicate the version. The version number increases each time the document is updated to support a new software release. For example, the first release of a document is 01.01. In the next software release cycle, the first release of the same document is 02.01.

The second two digits indicate the issue. The issue number increases each time the document is revised, but re-released in the same software release cycle. For example, the second release of a document in the same software release cycle is 01.02.

FOR MORE INFORMATION

To determine whether you have the latest version of this document and how documentation for your product is organized, check the release information in the *Meridian 1 Library Navigator* or the *Meridian SL-100 Master Index of Publications*.

References in this document

Meridian 1

If you are installing the MICB in a Meridian 1, see the following documents for additional information:

- *Hardware Replacement,* 553-3001-520
- *General Maintenance Information,* 553-3001-500
- *Fault Clearing,* 553-3001-510
- *System Engineering,* 553-3001-151
- *Capacity Engineering,* 553-3001-149
- *Power Engineering,* 553-3001-152
- *Summary of Transmission Parameters,* 553-2201-182
- *Call Detail Recording*, 553-2631-100

Meridian 1 and CSE 1000

If you are installing the MICB in a Meridian 1 or a CSE 1000, see the following documents for additional information:

- *Input/Output Administration,* 553-3001-311
- *Features and Services,* 553-3001-306

CSE 1000

If you are installing the MICB in a CSE 1000, see the following documents for additional information:

- *Application Guide*, 553-3023-110
- *Planning and Installation Guide*, 553-3023-210
- *Maintenance Guide*, 553-3023-510

Meridian SL-100

If you are installing the MICB in a Meridian SL-100, see the following documents for additional information:

- *IPE Reference Manual,* 555-4001-129
- *Alarm Clearing Procedures,* 555-4031-543
- *Routine Maintenance Procedures,* 555-4031-546
- *Card Replacement Procedures,* 555-4031-547
- *Log Report Reference Manual,* 555-4031-840

End user documentation

The following documents apply to all platforms:

- *Meridian Integrated Conference Bridge User Guide,* P0989944 – shows end user how to schedule and manage a conference using either the Telephone User Interface or the Browser User Interface.
- *Meridian Integrated Conference Bridge Quick Reference Card, P0989945* – provides a list of Telephone User Interface commands; comes in a package of 20.

Product description

Purpose

This chapter describes the functional and physical characteristics of the Meridian Integrated Conference Bridge (MICB) Release 3. Technicians can install the MICB Intelligent Peripheral Equipment (IPE) card in either a Meridian 1, Succession Communications Server 1000 (CSE 1000), or Meridian SL-100. This guide uses the term “Meridian system” to refer to either the Meridian 1, Meridian SL-100, or CSE 1000.

The chapter contains the following sections:

- **“MICB description” on page 15** – describes the MICB card and the role it plays in conference calls. Summarizes MICB features and services.
- **“Hardware overview” on page 18** – describes the hardware components of the MICB system.
- **“MICB operation” on page 24** – shows how MICB conferences operate.

MICB description

Conference administration

The MICB card allows users to schedule and administer multiple simultaneous conferences. Schedule conferences based on time-of-day, duration of each conference, and number of individuals (conferees) participating in, or ports allocated, for each conference. Schedule a conference using either of the following:

- Browser user interface – point and click web-page application
- Telephone user interface – telephone keypad entries

The MICB card provides announcements and tones that relate to specific events during conferences. These events include the following:

- advising the chairperson and conferees of the status of the conference connection
- indicating when a conferee joins or leaves the conference, and

- warning the chairperson and the conferees when the conference is about to expire.

Technicians can install multiple MICB cards into a single Intelligent Peripheral Equipment (IPE) module, Option 11 shelf, or CSE 1000 Gateway slot. Each MICB card can operate independently, providing up to 32 ports for a single conference. The MICB card can support up to ten simultaneous, separate conferences.

When users establish a single-card conference, they use the 32 ports on the card. If two conferences are held at the same time, they need to share the 32 ports. For example, if one user sets up a 10-port conference, the other can set up a 22-port conference.

Technicians can connect two MICB cards to provide up to 62 ports for a single conference. In dual mode, there can be only one dual-card meeting per pair of cards.

The MICB supports several simultaneous conferences. The number of conferences depends on the number of MICB ports available and the number of participants (conferees) in each conference. The MICB supports the following:

- maximum number of participants as follows:
  - single-card: 32 participants
  - dual-card: 62 participants (unless Chairperson Control over a Dual-card Meeting is activated, in which case it is 60 participants)
- any number of conferences (up to 10) with one or more participants in each conference

The MICB communicates with the system software by emulating a digital line card, which allows existing software to control the operation of the MICB. Configure each MICB port as an Automatic Call Distribution (ACD) M2616 digital telephone set.

System overview

The MICB comes as a single card, or a pair of cards if additional ports are required to support a dual-card meeting. Each card stands alone, even in the dual-card configuration. For dual-card meetings, the primary card uses ports on the secondary card. The following rules apply:

- Each card (that is, the primary and secondary) has its own set of users. There is no “common list” for both cards.

- To schedule a conference, the user logs into the card in which their account is defined. If the user has two accounts, one on each card, they must try each card separately to find available resources for the conference. There is no automatic pooling between cards.
- A user or super-user can have accounts on many cards at a company (that is, a customer can have one person who administers multiple bridges for their company).
- Dual-card conferences can only be scheduled by users on the primary card.

MICB conference feature summary

The MICB:

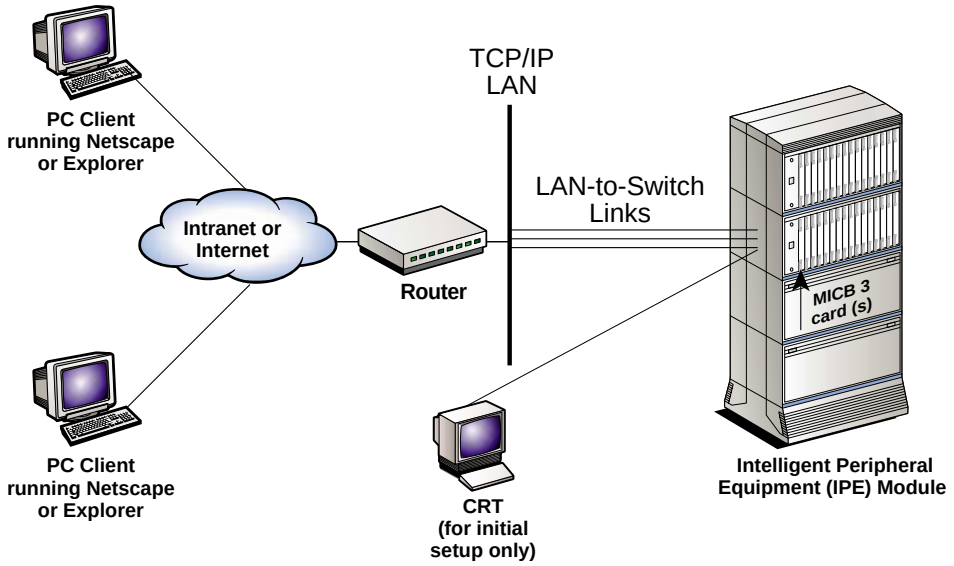
- Allows volume control by conference participants.
- Offers customized conference-specific greetings.
- Enables users to acquire and release chairperson control while in a conference.
- Delivers pre-meeting and post-meeting participants notifications.
- Allows one chairperson per conference.
- Offers optional chairperson control on the secondary card of a dual-card conference.
- Provides for one or more permanent bridge configurations.
- Supports multiple conferences simultaneously.
- Provides chairperson commands during an active conference.
- Provides conferee commands during an active conference.
- Allows conference extension beyond the scheduled time.
- Issues a 10-minute warning, before the conference termination.
- Supports multiple languages, including N.A. English, Spanish, French, Brazilian Portuguese, L.A. Spanish, Mandarin, Japanese, Korean, U.K. English, French, German, and Italian.
- Provides conference password security, requiring the chairperson and/or the conferees to enter a Dual-Tone Multifrequency (DTMF) password before entering the conference.
- Automatically starts and terminates conferences based on reservations scheduled in advance.
- Provides Group Call with smart retry.
- Provides the ability to reserve a port in each conference for the chairperson.

- Provides “Block scheduling” for recurrent conferences, up to one year in advance and up to 30 iterations of recurrent conferences.
- Offers an over-booking option, enabling the administrator to allocate up to 125% of port resources (based on the idea that most conferences are scheduled with more ports than are required).
- Provides an emergency bridge option, which creates a permanent bridge that automatically dials a pre-determined list of DNs when someone dials the emergency bridge DN. The emergency bridge does not support the dual-card configuration.
- Provides automatic conference expansion, allowing additional conferees to join the conference. For the expansion to work, the ports hosting the additional conferees must be both unassigned and available.
- Provides entry and exit indications – provides four options to indicate the entry and exit of a conference participant:
  - entry by name, exit by name
  - entry by name, exit by tone
  - entry by tone, exit by tone
  - silent entry and exit
- Allows the first conferee joining the conference to turn off and turn on conference music.
- Controls access to the conference in progress by monitoring the maximum number of scheduled attendees at each conference.
- Manages time and date for scheduled conferences and reserves ports for each conference.
- Provides recorded announcements to conferees who attempt to enter a meeting too early or after a meeting has ended.
- Issues audible responses to conferees based on the conference activity.
- Allows recording of a brand line (custom) greeting to replace standard greeting.
- Provides a scheduling display that indicates meeting reference number and whether a custom greeting has been created.
- Provides scheduling receipts e-mailed to users (receipt includes the direct meeting access DN or the single DN access DN.

Hardware overview

Figure 1 on page 19 shows MICB system composition.

Figure 1
MICB system composition



1. You install up to six MICB 3 cards in an IPE shelf of the Meridian 1/SL-100. Each MICB card serves a specific set of users.
2. You connect cards to the corporate Intranet/Internet through a TCP/IP Ethernet LAN, which is a 10BaseT physical connection.
3. You connect a CRT or Terminal Emulator directly to the serial port of the MICB 3. You require this terminal for initial installation only. You perform all administration and maintenance activities remotely.
4. Users and administrators access the cards from their desktops, which can be on the global internet behind a firewall.
5. MICB 3 can co-exist with MICB 2 on the same switch, with or without the MICB 2 server. There is no interaction between MICB 2 and MICB 3.

G100014

MICB hardware design characteristics

The MICB occupies one slot in an IPE module (Option 11 shelf or Gateway slot in the CSE 1000). The MICB card has the following hardware interface characteristics:

- uses the microprocessor unit (MPU) based on the 25MHz MC68EN360 Integrated Communications Controller
- uses standard interface buses and personal computer memory card international association (PCMCIA) cards and handles files that are compatible with MS-DOS operating system on the PCMCIA storage device

- accesses all 32 DS-30X voice/signaling timeslots
- provides echo cancelling and automatic gain control
- supports both the A-law and the m-law signal coding/decoding.
- Emulates an M2616 digital telephone set on each MICB port
- supports Card-LAN interfaces
- performs X12 signaling protocol messages for input/output
- uses digital signal processor (DSP) for conferencing and DTMF detection
- The DSP firmware:
  - Analyzes the loudness off all received signals continuously and selects the two loudest signals to be the active speakers.
  - Handles two-way conversation in conferences with three to 62 conferees.
  - Normalizes the pulse code modulation (PCM) input samples.
  - Provides gain control on all output samples.
  - Provides software upgrades using a PCMCIA Flash card.
- provides self-tests of internal hardware components and allows card monitoring and maintenance through the maintenance port; provides enable/disable capabilities similar to existing Meridian cards
- provides one RS-232 serial port for administration and maintenance access
- provides enhanced Call Detail Recording (CDR – Meridian 1 only) and billing options.
- provides an optional Ethernet interface over a Maintenance interface
- provides a Command Line Interface (CLI) accessible by direct connection, modem, telnet, or BUI emulation for performing OA&M functions.
- enables the reservation of one port on each card for TUI-only interaction.
- provides an embedded web-based server
- provides a customized MICB BUI login window.
- offers automatic backup. Backup configurations can be e-mailed to a predefined e-mail address.

Table 1 describes each hardware component of the MICB application. These components connect the MICB to the local or remote maintenance terminal.

Table 1
MICB hardware list

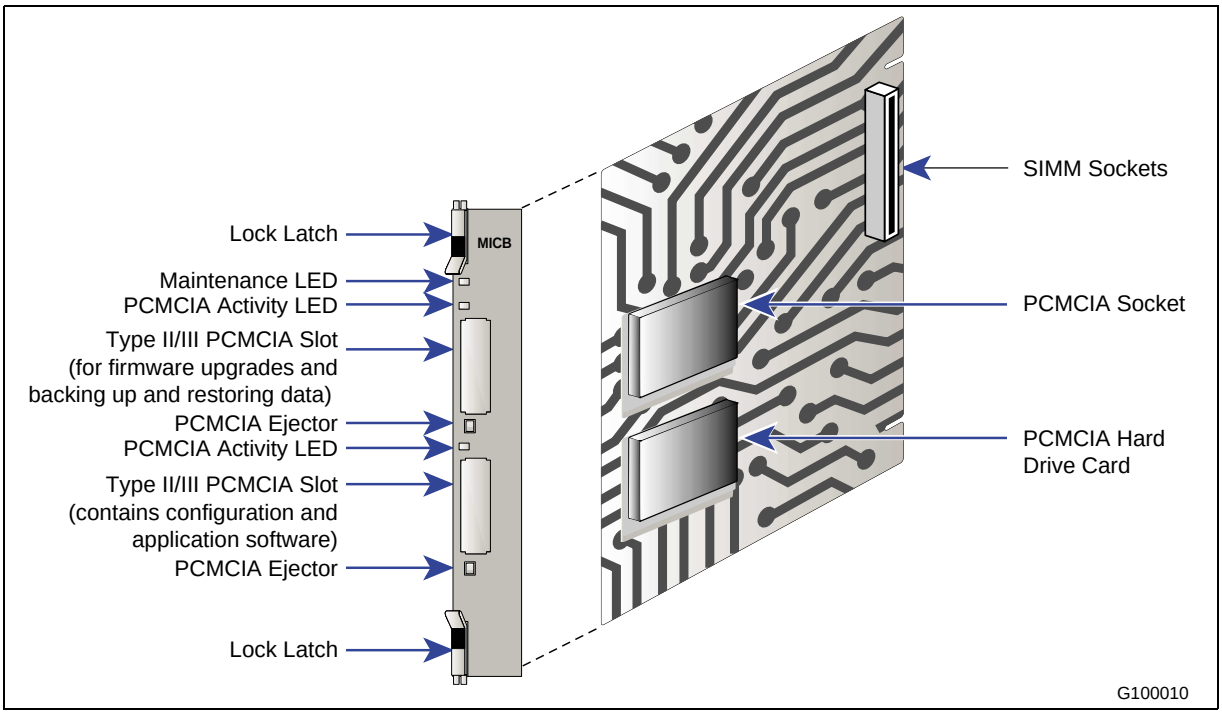
Component	Description
NT5D51AC or higher MICB card	An IPE card that provides bridge and conference scheduling for up to 10 simultaneous conferences.
NT5D62FA or later PCMCIA hard drive card	This PCMCIA card contains the MICB software and configuration. Install the PCMCIA card in the lower PCMCIA drive.
NT5D52AC Ethernet Adapter card (for IPE module installation)	Install this adapter card on the IPE module I/O panel only if connecting the MICB to Ethernet. ***Note:*** NT5D52BC for Option 11 and CSE 1000.

MICB card description

The MICB card has two PCMCIA sockets. PCMCIA hard drive cards store the MICB voice prompts and firmware code. The MICB comes with the PCMCIA hard drive. The bottom socket houses the PCMCIA hard drive card that contains the current firmware and customer data. Use the top socket to upgrade the firmware, and to backup and restore customer data.

Figure 2 on page 22 shows the component side of the MICB card and the faceplate. The component side shows the DRAM and the PCMCIA socket locations. The faceplate shows the card LED and the PCMCIA activity light-emitting diode (LED) indicators and the slot locations for PCMCIA cards.

Figure 2
MICB card



The MICB faceplate provides the following:

Maintenance LED – The MICB faceplate provides a red LED to indicate the enabled/disabled status of the card and to indicate the self-testing result during power up or card insertion into an operating system. This LED indicates the following:

- The LED is lit when the MICB card is disabled.
- The LED is off when the MICB card is enabled and ready for use.
- The LED blinks three times, runs software from the PCMCIA, then blinks three times again and stays on. The LED remains on until the software is enabled when the MICB card successfully completes the self-test.

PCMCIA activity indicator LEDs – These LEDs are next to the PCMCIA slots and indicate the following:

- The LED is lit when the PCMCIA card is disabled.
- The LED is off when the PCMCIA card is enabled and ready for use.
- The LED blinks when the PCMCIA card is in use.

Type II/III PCMCIA slots – The MICB faceplate provides two Type II/III PCMCIA card slots. These slots house the PCMCIA cards. Install the PCMCIA hard drive card that stores voice prompts and firmware code in the lower slot. Use the upper slot for upgrading the firmware, and backing up and restoring customer data.

External equipment

VT100 type terminal

Use a VT100 terminal for initial card configuration. After initial card configuration, use the BUI to perform operations, administration and maintenance (OA&M). Connect the terminal to the MICB RS-232 interface using one of the following methods:

- Direct connections:
  - — directly to the IPE module I/O panel
  - — directly to the DB-9 connector on the NT5D52 Ethernet Adapter card installed on the I/O panel
- Remote connections:
  - — to the IPE module I/O panel through a modem connection

The terminal interface must be set at 9600 baud, 8 data bits, 1 stop bit, and no parity. The flow control is hard wired (do not use XON/XOFF flow control).

Ethernet application

MICB Ethernet use has the following characteristics:

- The MICB Ethernet connection is separated from the external LAN traffic by a firewall.
- The Ethernet Adapter connection for MICB is NT5D52AA for the IPE module application.
- The Ethernet provider assigns the IP address for the MICB. Enter the IP address from the Maintenance terminal.
- To access the MICB CLI over the Ethernet, use a TELNET client on a PC workstation or in the LAN.

MICB operation

The MICB provides flexibility in configuring conferences. Configure conferences as follows:

- pre-scheduled conferences with a fixed number of ports and start/stop times
- pre-scheduled conferences with a variable numbers of ports, where ports are added when required (if available) and subtracted by the system automatically as conferees leave the conference
- permanent bridges with fixed numbers of ports that can be used without pre-scheduling the conference

The minimum duration of a conference is 15 minutes and the maximum duration of a time-limited conference is 12 hours. The conference starting time and duration can be scheduled in increments of 15 minutes.

The MICB card continuously monitors the audio signal level received from each conferee and selects the two loudest signals for transmission. The two loudest signals are summed and inserted into the PCM sample prior to their transmission to other conferees. This implementation of the two loudest signals improves the interrupting capability of a conference connection and allows normal two-way conversation that all conferees can hear.

In addition to the conferee timeslots, the MICB provides a timeslot between the MPU and the DSP. This timeslot transmits message prompts, entry and exit tones, or both that the system broadcasts to all conferees when requested by the MPU.

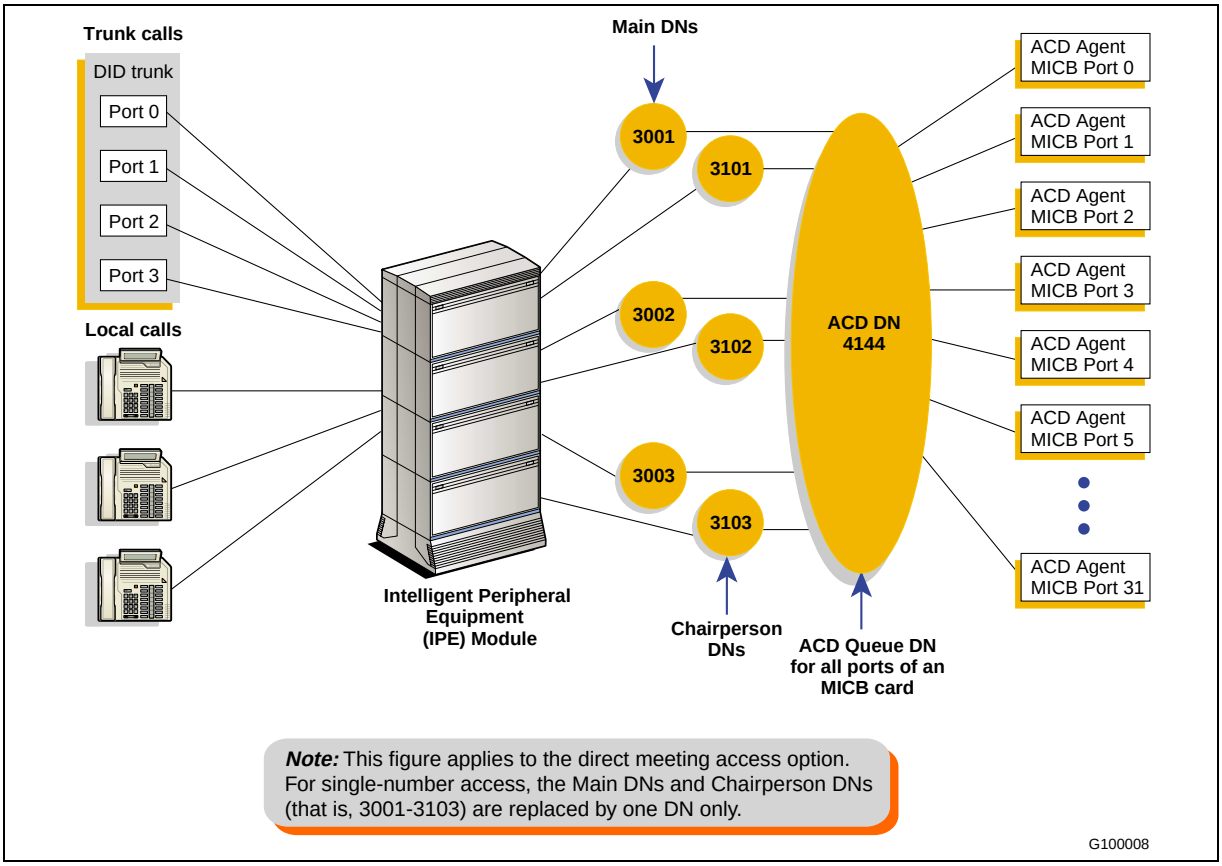
The MICB uses ACD features to route external incoming trunk and local line conferees to their appropriate conferences. The ACD features provide queuing, chairperson features, and event reporting for each conference.

The ACD features used by the MICB card provide the following:

- easy software configuration
- incoming calls, announcement on arrival, call management, and reporting queues
- operational statistics reports
- enhanced call routing

Figure 3 shows the call routing for three conferences and shows the conference chairperson access DN for each conference. The figure also shows the ACD DN for the ACD queue that controls the path of all ports on an MICB card. The right-hand side of the figure shows the distribution of MICB ports as ACD agents.

Figure 3
Call routing with chairperson access



Join the conference using the direct meeting access method

Assign a main DN and a chairperson DN, for each conference. The main DN is the number the conferees dial to get into the conference and the chairperson DN is the number the chairperson dials. Configure the DNs in the Meridian system when installing the MICB card. The total number of DNs is equal to two times the number of simultaneous conferences. For example, 10 simultaneous conferences require 20 DNs: 10 main DNs and 10 chairperson DNs.

When several conferences occur simultaneously in the same MICB card, the conferee dials the DN assigned to a specific conference. The MICB card identifies the dialed DN and routes the conferee to the appropriate conference represented by that specific DN. The system assigns all ports on the MICB card to the appropriate conference through the ACD DN assigned to that MICB card. The chairperson dials the chairperson DN to a specific conference. This number is different from the DN dialed by the conferees for the same conference.

The MICB performs DTMF detection on MICB ports identified as chairperson ports. DTMF detects when conferees enter a conference password. A conference can start without the chairperson. If all allocated ports for a conference are taken up with conferees, the chairperson cannot join the conference, unless a port is specifically reserved for the chairperson. The chairperson can also join if the system allows conference expansion and there are free, un-scheduled (floating) ports available.

The first conferee joining the conference hears an announcement indicating that no other conferee has joined the conference, followed by 60 seconds of music. The system repeats the announcement with 60 seconds of music, until another conferee joins the conference.

Join the conference using the single DN access method

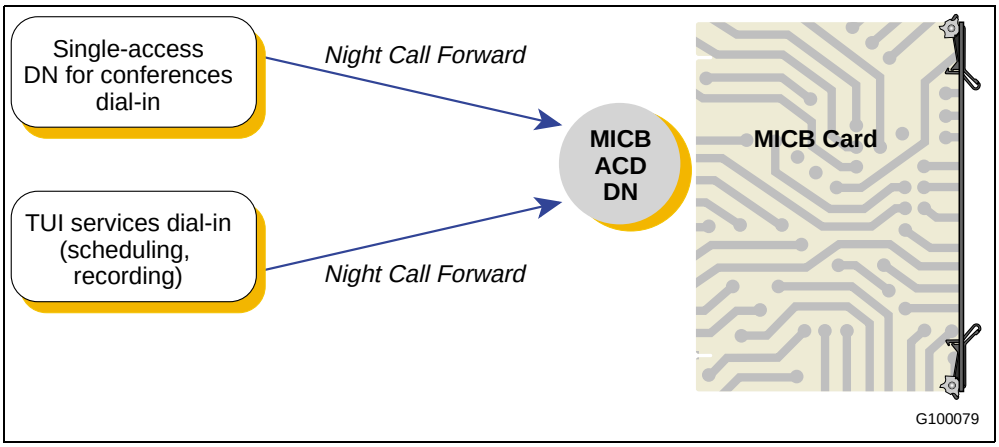
The single DN access method to all meetings provides users with a alternative method of accessing the MICB. This feature reduces the amount of Direct Inward Dialing (DID) numbers that have to be configured in the switch and provides the following benefits:

- Saves 20 DID numbers from the customer's DID range.
- Saves 20 ACD or Phantom DNs in the Meridian system thereby providing a cost savings.
- Simplifies installation as there is no DN pair configuration.
- Saves work if a change the numbering plan is required in the Meridian system.

The only trade-off is that callers have an additional step when accessing a meeting (that is, after dialing the single-access DN, they must enter the chairperson, or meeting, DN of their specific meeting).

Figure 4 on page 27 shows the DN configuration for single DN access with one MICB card.

Figure 4
Single DN access method (one MICB card)



The DNs on the left in Figure 4 can be Phantom DNs or CDNs, instead of ACD DNs. The DNs must be DID numbers.

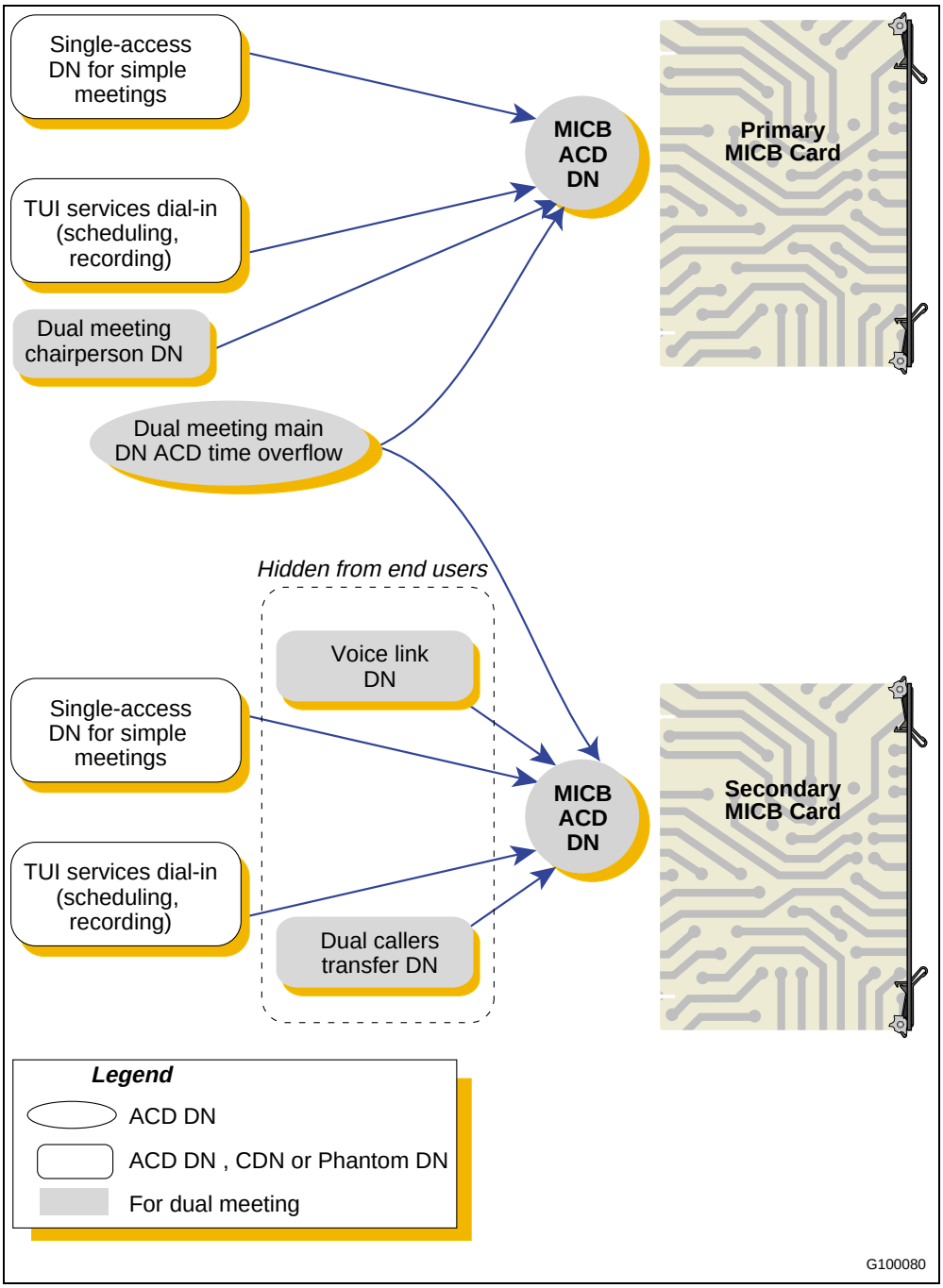
In a dual-card system, each card requires its own single-access DN. In a dual-card set, conferences that span the two cards do not support the single DN access method. However, in a dual-card set, simple conferences that use only one card support the single DN access method.

Figure 5 on page 28 shows the DN configuration in a Meridian system for the single DN access method when the system uses two MICB cards. Single DN access requires one DN, instead of the separate 10 DNs required with direct meeting access.

The figure shows a configuration that supports the following:

- Simple conference contained in the primary MICB – participants dial the single-access DN at the top of the figure.
- Simple conferences contained on the secondary MICB – participants dial the single-access DN at the bottom of the figure
- Meetings spanning both cards – participants dial the “Dual meeting main DN” in the middle of the figure and the chairperson dials the “Dual meeting chairperson DN”. The figure shows that dual-card meetings do not use the single-access DNs.

Figure 5
Single DN access method (two MICB cards)



Note: All DNs on the left side of the figure must be DID numbers.

Single DN access is mutually exclusive from the direct meeting access method in a MICB card or card pair. Configure the card for one access method; the system does not support combinations on the card or card pair.

Callers to all meetings access the MICB by dialing one common fixed number. The MICB prompts the caller for the meeting or chairperson DN to enter the required meeting. In this mode of operation, configure the single-access DN in the Meridian system and MICB only. Access DN pairs are pre-coded in the card.

Expand the conference

Conference expansion allows the system to increase the number of conferees if there are remaining MICB ports that are both unassigned and unused. Allow or deny conference expansion for each conference using the browser user interface (BUI) (see the “Add ports as needed field” in the “Scheduling window” on page 84).

When reserving the MICB ports for each simultaneous conference, the system does not tag ports for a specific conference. The MICB counts the number of reserved ports and compares these against the total number of ports provided by the MICB card. The MICB then makes sure that the reserved ports do not exceed the total number of ports provided by the MICB card.

If additional (non-scheduled) callers try to join a conference, but there are no floating ports, or the system locks out additional conferees, the MICB card issues an overflow tone. The system then disconnects the call.

If the system releases un-scheduled (floating) ports from a conference, they are immediately available to be used by other conferences that have the expansion feature enabled.

End the conference

When scheduling a conference, indicate the number of ports, start time, and duration of that conference. The conference ends based on the start time and conference duration. Ten minutes before the end of a conference, the MICB card issues an announcement warning the conferees that the conference terminates in 10 minutes.

When the conference time expires, the MICB card issues the final warning to the conferees. The MICB sends a release message to the Meridian system for all associated MICB ports. These ports become available for the next planned conference. If there is no other scheduled conference, they become floating ports which the system does not reserve for any conference. Floating ports are available to expand conferences in progress.

Conferees can exit a conference at any time. The MICB detects when a conferee exits the conference. If enabled, the MICB announces the conferee's name. When one conferee is on the conference, the system issues an announcement that only one conferee is present, followed by 60 seconds of music. The system repeats this announcement and the music, until at least one more conferee joins in, or the MICB terminates the conference.

Note: A conference can begin and end two minutes before the defined time. This feature allows the system to close all terminating conferences two minutes earlier and start all scheduled conferences immediately after closing the terminating conferences. This feature is important when terminating and starting conferences use some of the same DNs.

Engineering guidelines

Purpose

This chapter provides guidelines for engineering MICB Release 3. Engineering guidelines can vary depending on the system platform. The chapter includes the following sections:

- **“System requirements” on page 31** – outlines the software and hardware requirements for the Meridian 1, CSE 100, and Meridian SL-100.
- **“System compatibility” on page 33** – lists the various compatible systems.
- **“Automatic call distribution resource allocation” on page 33** – describes the ACD DN resource requirements.
- **“LAN configuration” on page 35** – provides guidelines for configuring the LAN options.

System requirements

Software

The required system software is as follows:

- **Meridian 1** – XII Release 19 supports up to 16 MICB ports per card; XII Release 22 and later supports up to 32 ports per card.
- **CSE 1000** – Release 1 and above supports up to 32 ports per card.
- **Meridian SL-100** – MSL09 and later supports up to 32 ports per card using the FLXA feature.

The system software must contain the basic and advanced automatic call distribution (ACD) features and routing software.

Meridian 1 and CSE 1000 software packages
In addition to standard X11 software, the following software packages are required:

- ACD basic package (45)
- ACD advanced features (41)

- Digital set (88)
- End-to-end signaling (10) – required if chairperson calls locally within the same switch
- Network ACD Enhanced Overflow (178), optional, but required for the dual-card configuration
- The following packages are optional, but are required for billing:
  - Call Detail Recording (CDR) package 4
  - CDR with Charge Account (CHG) package 23
  - Charge Account/Authorization Code Base (CAB) package 24

Meridian SL-100 software packages
In addition to the standard MSL software, the following software packages are required:

- ACD Basic, ACD Routing Enhancement
- MSL Digital Phones M2000-Display
- MSL Flex LEN on IPE
- MSL Enhanced Peripheral Equipment (IPE)

Hardware

Table 2 describes the MICB hardware specifications.

Table 2
Hardware specifications

Item	Descriptions
Port capacity	12-32 ports on a single card. Up to 62 ports in a dual-card configuration, unless chairperson control is required on the second card, in which case the capacity is 60 ports.
Capacity upgrades	Upgradeable from 12 to 62 ports.
Maximum number of conferences	Up to 10 simultaneous conferences per card.
Maximum number of BUI sessions	Up to 20 simultaneous user sessions on the BUI.
PCMCIA card	PCMCIA Type II or III.
System interface	DS-30X, CE-MUX, Card LAN, Ethernet Adapter.
Maintenance terminal	Optivity, VT-100 terminal or PC with VT100 emulation.

Table 2
Hardware specifications

Item	Descriptions
Power requirements	Power is supplied by the power supply of the shelf/module where the MICB card is installed. Each MICB card requires a total maximum power of 16.5 W.
Real time impact	Comparable to that of a digital line card (DLC).

System compatibility

Meridian 1 and Option 11

MICB 3 is compatible with the following Meridian 1/Option 11 systems:

- Option 11C, 11E,11C Mini
- Option 21E
- Option 51, 51C
- Option 61, 61C
- Option 71
- Option 81, 81C
- SL-1 systems with IPE upgrade (NT and XT)

CSE 1000

MICB 3 is compatible with the following CSE 1000 system:

- Succession Communications Server for Enterprise (CSE 1000)

Meridian SL-100 system compatibility

MICB 3 is compatible with all Meridian SL-100 system configurations.

Automatic call distribution resource allocation

The ACD function routes incoming calls to the MICB, where each MICB port operates as an ACD agent. All MICB ports are part of the same ACD queue and operate as a pool of ports with equal status. The system identifies the ACD queue with an ACD DN that handles the connection of conferees (ACD agents) to the appropriate conference.

ACD resources must be reviewed in the Incremental Software Management (ISM) of the customer configuration, if applicable. Each MICB port represents an ACD agent that uses a Terminal Number (TN)/Line Equipment Number (LEN) from the system resources.

The configuration DN and the corresponding TNs on the Meridian 1, or LENs on the Meridian SL-100, are system resources. The system resources allocated to the MICB must be subtracted from the overall system resources and cannot be used for any other application, as long as they are assigned for MICB use.

> ***Note:*** If a customer uses Agent ID and the direct meeting access method, the agent IDs must be consecutive (for example, 00-31).

Each MICB card, using the direct meeting access method, requires the following:

- One ACD group for each MICB card.
- Assign ACD agent TNs/LENs and corresponding M2616 digital sets. Each configured MICB port appears as an M2616 digital set of an ACD agent. The number of TNs/LENs is equal to the maximum number of ports provided by the MICB card. For an MICB with 32 ports active, the configuration requires 32 TNs/LENs. TNs/LENs require 32 DNs for the ACD incalls key and 32 DNs for the secondary directory number (SDN) key (Key 2).
- An MICB card configured to the maximum capacity of 32 ports and 10 simultaneous conferences requires 87 ACD DNs and 32 TNs/LENs as follows:
  - one ACD DN assigned to the MICB card
  - 32 TNs/LENs assigned to the 32 ports (1 PDN and 1 SDN for each TN/LEN; these can be internal DNs – non-DID)
  - 20 ACD DID DNs (10 DN pairs) for dialing into the potential conferences

    > ***Note:*** For single-number access, replace this with 1 DN.

  - 1 DN for TUI access

Full 62-port dual-card conferencing, using the direct meeting access method, requires the following:

- Two MICB cards and six ACD groups as follows:
  - 64 ACD agents (32 for each card), non-DID
  - 64 secondary DNs for these agents, non-DID
  - 36 DNs for simple conferences (9 pairs in each card)

    > ***Note:*** For single-number access, replace this with 2 DNs (1 for each card).

— 1 DN for dual-card conference access

— 1 DN for dual-card chairperson access

— 1 DN for the link DN, non-DID

— 1 DN for the transfer DN, non-DID

— 2 DNs for TUI access (1 for each card)

This provides a total of 170 DNs, 40 of which are DID.

- Assign an Ethernet port to each MICB card with an IP address, subnet mask, and gateway during installation.

Note: On the Meridian SL-100, verify that there are enough DS30A links back to the extended peripheral module (XPM) to handle the traffic.

LAN configuration

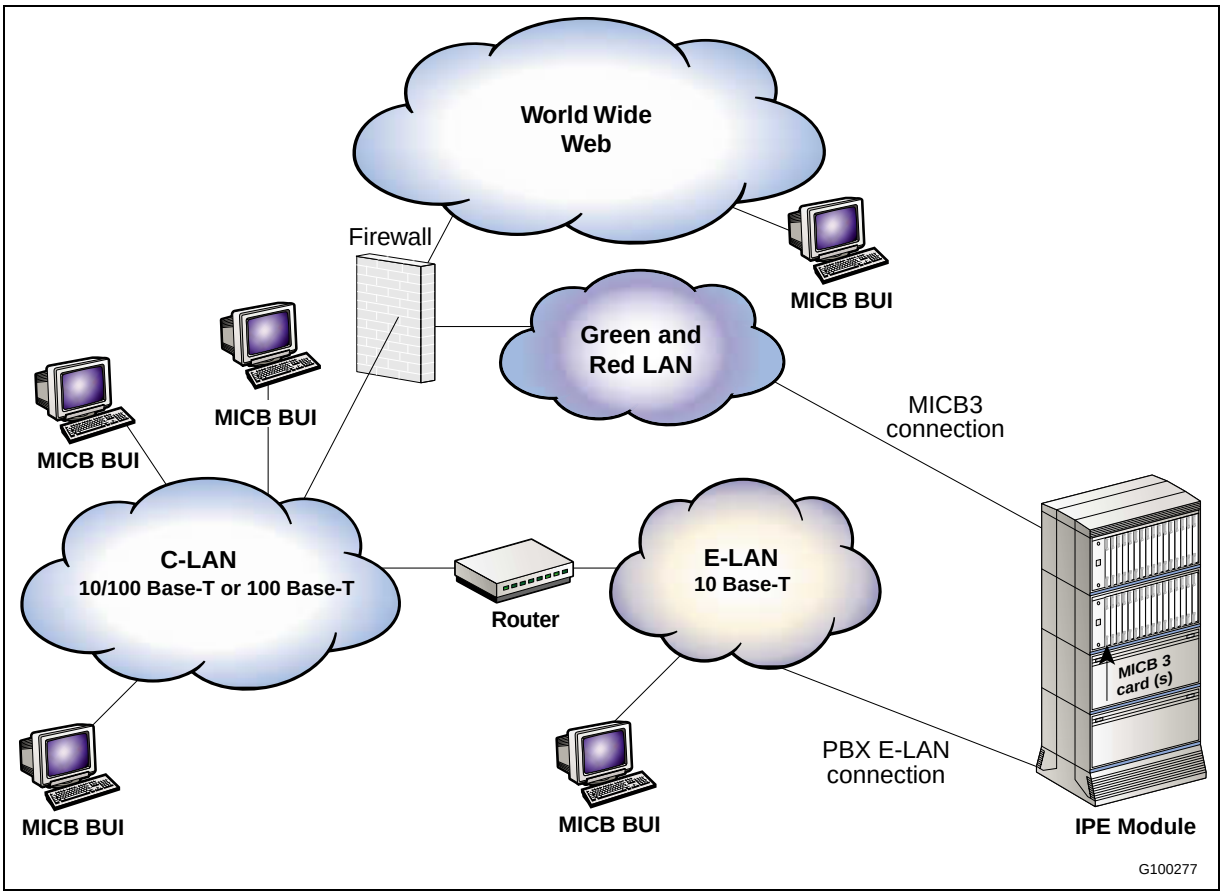
MICB customers should select one of the following alternatives for BUI access:

- users and administrators access the MICB from the global internet (the new capability of MICB3)
- users and administrators access the MICB from the customer LAN/intranet only (existing MICB2 capability)

Global internet access

Global internet access requires careful configuration of security elements. Figure 6 on page 36 shows a sample configuration.

Figure 6
Global internet access example



In typical configurations, the firewall does not allow any kind of access from the World Wide Web *into* the C-LAN. Only access *from* the C-LAN hosts to the World Wide Web is allowed (for example, HTTP and FTP).

Hosts that need to be accessed from the World Wide Web must be placed in a special sub-network called the Green and Red LAN. The firewall isolates the Green and Red LAN from the C-LAN. Devices that can be accessed from the World Wide Web are put into this segregated LAN segment. Nortel Networks recommends that the Green and Red LAN be the location of the MICB connection.

On the other hand, C-LAN hosts require open access to the MICB for administration and maintenance.

Table 3 summarizes the recommended access permissions allowed by the firewall. All other paths not in the table should be denied.

Table 3
Firewall access permissions

Source	Destination	Protocol
WWW	MICB	HTTP
C-LAN	MICB	HTTP, FTP, TELNET
MICB	WWW	FTP (optional; allows upgrade from the web)
MICB	C-LAN	FTP
MICB	Mail Server	SMTP

Notes
Take the following notes into consideration:

- Technically, a firewall can be configured to enforce these access restrictions even when the MICB is in the C-LAN. However, a Green and Red LAN is usually used, because it is safer.
- Cards of a dual-MICB set must be in the same LAN segment, with no restrictions between them.
- When upgrading to this configuration from MICB2 to MICB3, MICB IP parameters will change.

LAN/intranet access only

In this configuration, the MICB is not accessible from anywhere in the World Wide Web (assuming this policy is enforced by the firewall). There are two options for this type of configuration: C-LAN connection and E-LAN connection.

Figure 7 on page 38 shows an example of the C-LAN connection.

Figure 7
LAN/intranet access only – C-LAN connection

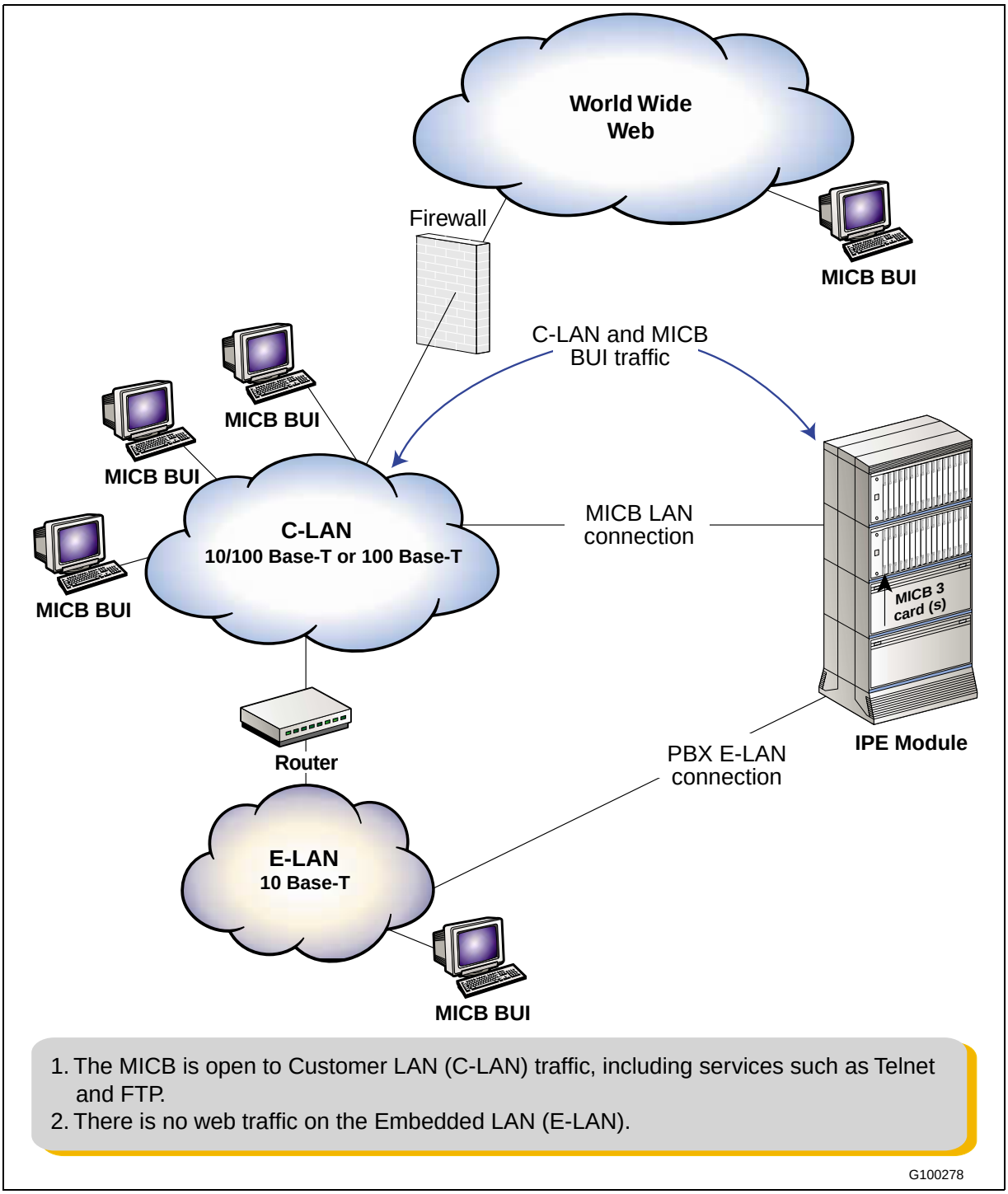
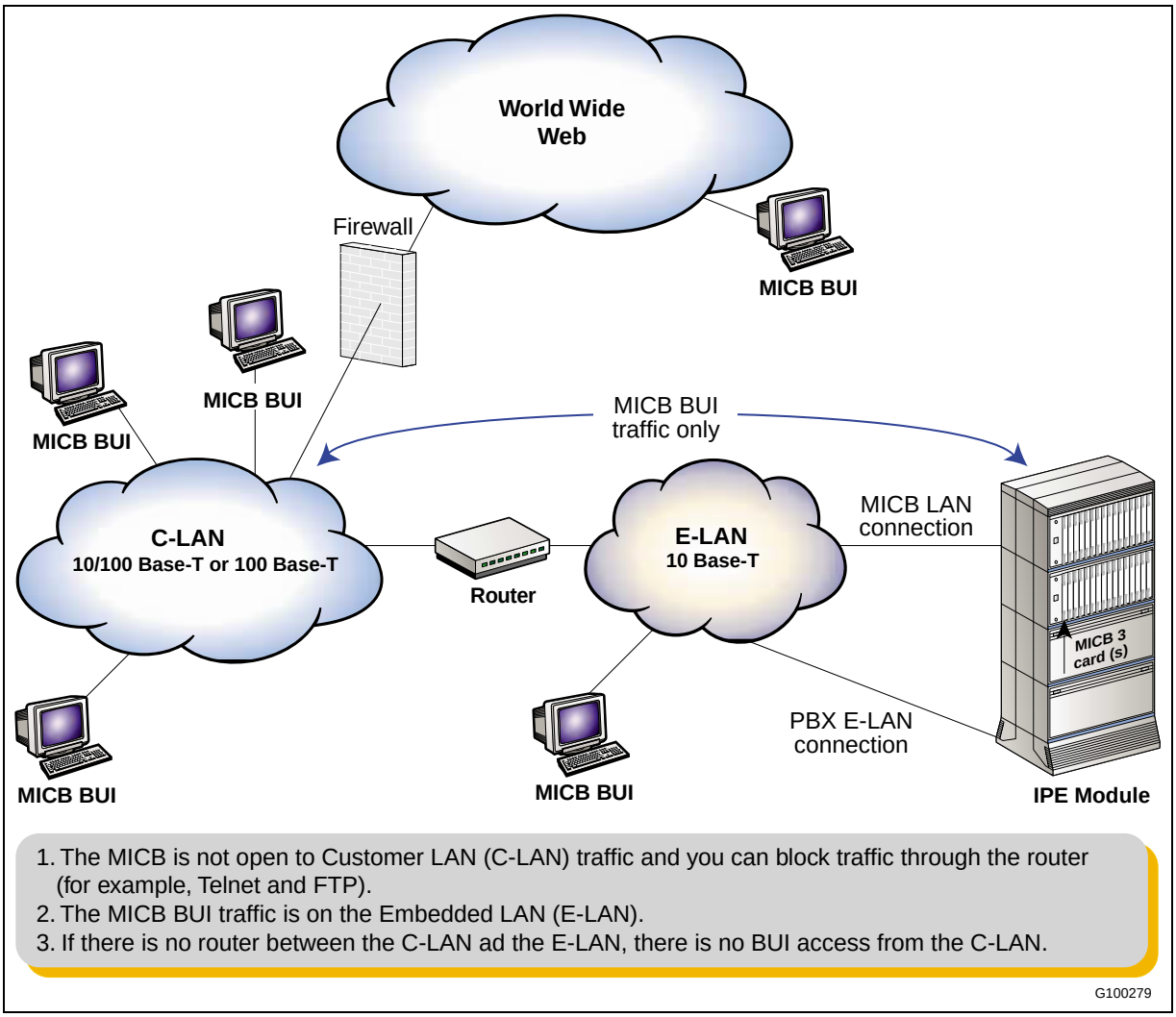


Figure 8 on page 39 shows an example of the E-LAN connection.

Figure 8
LAN/intranet access only – E-LAN connection



Notes

The following notes apply to LAN/intranet access only:

- The MICB does not interact with the Meridian system through the E-LAN, so logically there is no requirement to put it there. In addition, if the E-LAN is completely separated from the C-LAN, the MICB cannot be in the E-LAN.
- Nortel Networks recommends that customer try not to put any BUI traffic on the E-LAN if possible.
- Each site should select the most convenient option, taking into account the physical LAN endpoints available near the MICB card.

- When there are multiple MICBs (that is, more than three) and the BUI is used frequently, the BUI traffic can load the E-LAN, so it may be better to connect the cards to the C-LAN.
- The MICB has a broadcast-storm protection mechanism: it shuts off the LAN port (temporarily) when traffic is too heavy. Nortel Networks recommends that the MICB be put in a “quiet” LAN segment to get a better response time.

Summary of LAN installation information

Use the following steps when installing and configuring the LAN:

1. Determine whether the MICB is to be accessed from the World Wide Web.
2. If yes, coordinate the firewall configuration with your IS group according to Table 3 on page 37.
3. Determine what is the physical connection point of the MICB. Note these requirements: 10Base-T only, half-duplex.
4. Get the following MICB IP parameters from your IS group: IP address, gateway address, and subnet mask.
5. Get the Mail Server IP address from your IS group. Confirm that the MICB is allowed to access this server by SMTP.

Testing:

Use the following steps to test the LAN configuration:

1. After the MICB is installed and the IP parameters are configured, try to “ping” from any host in the C-LAN to the MICB or from the MICB to a host on the C-LAN.
2. In the case of World Wide Web access, try accessing the MICB from a browser (HTTP access).

Installation and configuration

Purpose

This chapter describes how to prepare the Meridian system for installation, install the MICB into the IPE module (Option 11 shelf or Gateway slot in the CSE 1000), connect the MICB to the administration terminal, and configure the card.

The chapter contains the following sections:

- **“Getting started” on page 41** – describes the steps to use when preparing for an installation.
- **“Meridian 1 and CSE 1000 configuration” on page 42** – shows how to configure the Meridian 1 and CSE 1000.
- **“Meridian SL-100 configuration” on page 50** – shows how to configure the Meridian SL-100.
- **“MICB installation and configuration procedures” on page 60** – shows how to install the card and set up the web server.
- **“MICB Installation Wizard” on page 67** – describes how to use the BUI’s Install Wiz to complete configuration.

Getting started

To begin the installation, unpack and inspect the components, take inventory, and determine which IPE card slot(s) in which to install the MICB card(s). See Table 1 on page 21 for a complete listing of the MICB hardware.

Unpack and inspect the equipment

Unpack and inspect the equipment for damage. Follow the steps in Procedure 1 on page 42, before performing the installation and configuration procedures in this chapter.

Procedure 1
Prepare for the installation

1. Remove items from the installation site that can generate static charge.
2. Use antistatic spray if the site is carpeted.
3. Ground yourself before handling any equipment.
4. Remove equipment carefully from its packaging. Save the packaging, in case the card has to be returned.
5. Inspect the equipment for faults or damage. Report any damaged component to your Nortel Networks representative and the company who delivered the equipment.

This procedure is now complete

Take inventory

After unpacking and inspecting the equipment, verify that all necessary components are on site before beginning the installation. Check the equipment received against the shipping documents. Report any missing parts to your Nortel Networks representative.

Verify IPE Slot(s)

The MICB card can be installed in any IPE card slot associated with full 50-pin I/O cables. Table 4 lists the Meridian system modules and the card slots appropriate for MICB installation.

Table 4
MICB installation into card slots

Meridian system modules	MICB card slots
NT8D37BA/EC IPE modules, and NT8D11BC/ED CE/PE modules.	All available IPE card slots.
NT8D37AA/DC IPE modules.	IPE card slots 0, 4, 8, and 12.
CSE 1000.	1, 2, or 3 of the Media Gateway, or slots 7, 8, 9, or 10 of the Media Gateway Expansion.

Determine the access method

Select the access method, single-number or direct meeting access, the system will be using. With direct access, configure 10 DN pairs. In single-number access mode, configure only the single-access DN. In both cases, the BUI provides instructions about what to do next.

Meridian 1 and CSE 1000 configuration

Prior to installing any of the MICB hardware, configure the X11 system software for the MICB card(s) through the system TTY terminal.

Summary

The following summarizes the tasks for configuring the Meridian 1:

1. LD 23 – Define the ACD DN assigned to the MICB card.
2. Define DNs using either:

   LD 23 – Define ACD DNs and assign them to the MICB card.

   or

   LD 10 – Define Phantom TNs and forward them to the ACD DN assigned to the MICB card.
3. LD 11 – Configure MICB ports as digital sets.
4. LD 23 – Configure the main DN for dual-card conferences.

Assign ACD DNs

The first step is to assign ACD DNs.

Table 5
LD 23 – Define the ACD DN assigned to the MICB card

Prompt	Response	Description
REQ	NEW	Add new data.
TYPE	ACD	ACD data block.
CUST	xx	Customer number.
ACDN	xxxx	ACD DN assigned to the MICB card.
MAXP	32	Maximum number of ACD agent positions.

Table 6
LD 23 – Assign the ACD DNs for the MICB card.

Prompt	Response	Description
REQ	NEW	New control data block.
TYPE	ACD	ACD data block.
CUST	xx	Customer number.
ACDN	xxxx	Conferee (main) or chairperson DN.
MAXP	1	Maximum number of ACD agent positions.
NCFW	xxxx	ACD DN assigned to MICB card.
Note: Repeat commands in this table for each ACD DN being configured.		

Note: The number of DNs defined for each MICB card using direct meeting access depends on the number of conferences and bridges specified on the card. A maximum of 10 conferences can be configured requiring 20 DNs, two for each conference. One DN is for the conferees to call in (the main DN) and one DN is for the conference chairperson.

Define Phantom TN blocks

Phantom TNs can be used, instead of ACD DNs, to serve as chairperson DNs, conferees DNs and TUI DNs.

Enter the Meridian 1 definitions for the Phantom TN in LD10 as follows:

1. The specific TN and DN vary by site.

   Those variables are represented by “x” in Figure 9.

2. CFXA is the Class of Service (CLS) that enables Call Forwarding.

3. The last four variables in the screen (under FTR) are the main ACD DNs in LD 23.

Figure 9
Phantom TN definitions (LD 10)

```
DES  MICB
TN   xxx   x   xx   xx       PHANTOM
TYPE 500
CDEN 4D
CUST 0
WRLS NO
DN   xxxx   x    MARP
AST  NO
IAPG 0
HUNT
TGAR 1
LDN  NO
NCOS 0
SGRP 0
RNPG 0
XLST
SCI  0
SCPW
SFLT NO
CAC  3
CLS     CTD   DTN   FBD   XFD   WTA  THFD  FND   HTD  ONS
  LPR   XRD   CWD   SWD   MWD   LPD  XHD   CCSD  LND  TVD
  CFTD  SFD   MRD   C6D  CNID   CLBD AUTU
  ICDD  CDMD  LLCN  EHTD  MCTD
  GPUD  DPUD  CFXA  ARND  OVDD  AGTD CLTD  LDTD  ASCD
  MBXD  CPFA  CPTA  HSPD  UDI   ACC  HBTD  DDGA  NAMA  MIND
  NRWD  NRCD  NROD  SPKD  CRD   PRSD MCRD
  EXRO  SHL   ABDD  CFHD  DNAA
  CWND  USRD  BNRD  OCHD  RTDD  FAXD
PLEV 02
AACS NO
MLWU_LANG  0
FTR  DCFW  12    <ACD  DN>
```

The next step is to configure MICB ports as digital sets.

Table 7
LD 11 – Configure MICB ports as digital sets

Prompt	Response	Description
REQ	NEW	Add new data.
TYPE	2616	Digital telephone set M2616.
TN	l s cu s c u	Terminal number of the MICB card, Options 51C, 61C, and 81C. For Option 11C and CSE 1000.
CUST	xx	Customer number.
CLS	FLXA VCE, WTA	FLXA = Flexible Voice/Data Allowed. VCE = Voice. WTA = Warning Tone Allowed. ACD agent (Use FLXA).
KEY	0 ACD <ACD DN> <CLI> <pos ID>	ACD DN plus CLI plus position ID.
KEY	1 SCR <any DN>	Line key.
KEY	2 NRD	Not ready key.
KEY	3 MSB	Make set busy key.
KEY	4 TRN	Call transfer key
Note: The administrator should consider chairperson dial-out restrictions through the MICB ports to prevent international dial-out.		

The number of virtual ACD agents of the ACD queue is equal to the number of MICB ports. For example, if 12 ports are enabled, define 12 ACD agents. If the TN for the MICB card is specified as 28 0 6, then TNs for the 12 agents are specified as 28 0 6 0 through 28 0 6 11.

Note: Agent IDs must be consecutive (for example, 2000-2031).

Figure 10 on page 46 shows a sample LD 20 printout of a built MICB port.

Figure 10
LD 20 MICB configuration

```
PT0000
REQ: PRT
TYPE: TNB
TN   76 0 8 0
SPWD
DATE
PAGE
DES

DES  MICB
TN   076 0 08 00
TYPE 2616
CDEN 8D
CUST 0
AOM  0
FDN
TGAR 1
LDN  NO
NCOS 0
SGRP 0
RNPG 0
SCI  0
SSU
XLST 0
SCPW
CLS  CTD FBD WTA LPR MTD FND HTD ADD HFD
     MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
     POD DSX VMD CMSD CCSD SWD LND CNDD
     CFTD SFD DDV CNID CDCA MSID DAPA BFED RCBD
CPND_LANG ENG
HUNT
PLEV 02
SPID NONE
AST
IAPG 0
AACS NO
ITNA NO
DGRP
PRI  01
DNDR 0
KEY  00 ACD 4004 0  4939210
         AGN
     01 SCN 4939250 0     MARP
        CPND
          NAME MICB CHANNEL 0
          XPLN 14
          DISPLAY_FMT FIRST,LAST
     02 NRD
     03 MSB
     04 TRN
     05
     06
     07
     08
     09
     10
     11
     12
     13
     14
```

Configure DNs for a dual-card conference

When a dual-card conference is defined, two meetings are defined on two cards. First, the meeting is booked on the primary card allocating the maximum free ports. Second, the meeting is booked on the secondary card allocating the rest of free ports for the dual-card conference. The user defines a dual-card conference only on the primary card.

When a user dials into a dual-card conference, the call can terminate either on the primary or on the secondary card. Calls to the dual-card conference main ACD DN are forwarded according to the ACD time overflow night table.

On both cards (primary and secondary), the user cannot use the dual-card conference pair DNs for a simple meeting. Therefore, nine DNs are available for simple meeting and bridges.

For a dual-card configuration, one card functions as the primary card and the other as the secondary card. Define for each card an ACD data block with an ACD DN in LD 23, as shown in Table 5 on page 43.

For the primary card, configure the following DNs:

- DN pairs (up to nine) – These pairs serve as chairperson and conferee DNs for single-card conferences (less than 32 ports) on the primary card.

  Note: If single-number access is being used, DN pairs are not required. Instead, define the single-number access DN in this step which callers use to access a simple conference on the primary card.

- TUI DN – This is the DN that users dial to set up single-card conferences on the primary card. Do not configure this DN, if the TUI is not going to be used.
- Chairperson DN – This is the DN that chairperson of a dual-card conference dials to enter a dual-card conference. This DN is required for dual-card setup.

Therefore, for the primary card, configure up to 20 DNs in LD 23 that Night Call Forward (NCFW) to the ACD DN of the primary card.

For the secondary card, configure the following DNs:

- DN pairs (up to nine) – These pairs serve as chairperson and conferee DNs for single-card conferences (less than 32 ports) on the secondary card.

  Note: If single-number access is being used, DN pairs are not required. Instead, define the single-number access DN in this step which callers use to access a simple conference on the secondary card.

- TUI DN – This is the DN that users dial to set up single-card conferences on the secondary card. Do not configure this DN, if the the TUI is not going to be used.
- Transfer DN – This is the DN that transfers dual-card conference participants from the primary card to the secondary card when the primary card reaches capacity. The primary card fills up first in a dual-card conference. Configure this DN for dual-card setup.
- Link DN – This is the DN the creates a speech path between the primary card and the secondary card for dual-card conferences. Configure this DN for dual-card setup.

Therefore, for the secondary card, configure up to 22 DNs in LD 23 that Night Call Forward (NCFW) to the ACD DN of the secondary card.

The main DN must also be configured for the dual-card conference. The main DN is the DN that conferees dial to enter the dual-card conference. When the conferees dial the main DN, the main DN forwards them to the ACD queue of the primary card. When the primary card becomes full, the transfer DN transfers further conferees to the secondary card. Use Table 8 to configure the main DN for dual-card conferences,

Table 8
LD 23 – Configure the main DN for dual-card conferences

Prompt	Response	Description
REQ	NEW	Add new data.
TYPE	ACD	ACD data block.
CUST	xx	Customer number.
ACDN	xxxx	The main DN for dual-card conferences.
MAXP	1	Maximum number of ACD agent positions.

Table 8
LD 23 – Configure the main DN for dual-card conferences

Prompt	Response	Description
Note: Carriage return to the end and start again.		
REQ	NEW	New control data block.
TYPE	NACD	Network ACD data block.
CUST	xx	Customer number.
ACDN	xxxx	The main DN for dual-card conferences.
TABL	N	Night time overflow table.
- TRGT	xxxx 0	xxxx is the ACD DN of the primary card. 0 is the time, in seconds, for an immediate transfer to the primary card.
- TRGT	yyyy 2	yyyy is the ACD DN of the secondary card. 2 is the time, in seconds, for a delayed transfer to the secondary card.

Table 9 shows a sample dialing plan for a 62-port dual-card configuration.

Table 9
Sample dialing plan for a 62-port dual-card configuration

Description of DNs	DNs for the primary card	DNs for the secondary card	Configure in...
ACD DN	7000	8000	LD 23
Pair DNs for single-card conferences	7001-7018 (NCFW = 7000 in LD 23)	8001-8018 (NCFW = 8000 in LD 23)	LD 23
TUI DNs	7019 (NCFW = 7000)	8019 (NCFW = 8000)	LD 23
Chairperson DNs	7020 (NCFW = 7000)		LD 23
Transfer DN	N/A	8021 (NCFW = 8000)	LD 23
Link DN	N/A	8022 (NCFW = 8000)	LD 23
Main DN	7021(TRGT = 7000 0)	7021 (TRGT = 8000 2)	LD 23

Note: Because of the number and variety of DNs programmed for the dual-card setup, Nortel Networks recommends creating a dialing plan chart similar to Table 9 on page 49. Refer to this chart when configuring the primary and secondary card attributes, including the dual-card settings, in the administration BUI.

Finally, configure each port on the primary and secondary cards as a digital set. See Table 7 on page 45.

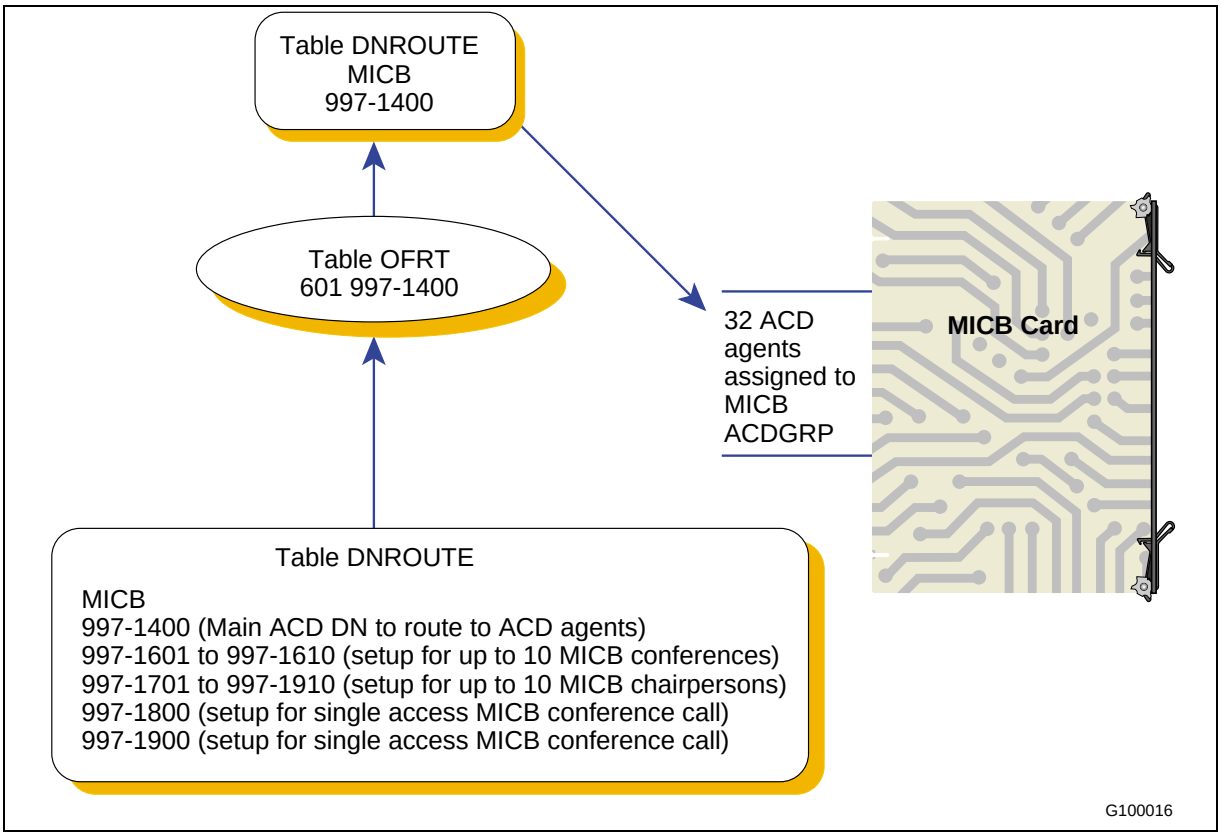
Meridian SL-100 configuration

Single-card configuration

After installing the MICB card(s) and connecting the terminal for CLI access and the server for BUI access, perform Meridian SL-100 database configuration. Figure 11 shows the tables to datafill for single-card setup.

Note: If single-number access is being used, the DN pairs are not required. Instead configure a single-number access DN.

Figure 11
Single-card conference, 10 conferences, 32 ports



Configuration procedure

Single-card installation enables up to 10 conferences on one 32-port MICB card. Each MICB card can use one MICB ACD Group to handle all the access DNs required

To configure an MICB single-card conference with direct meeting access, from a maintenance administration position (MAP) terminal follow the steps in Procedure 2.

Procedure 2
Configure a single-card conference

1 Define LENs as FLXA (MSL09 or above) in table LNINV for a 32-port conference. Refer to Figure 12 on page 52.

2 Define the MICB ACDGRP and ACD agents assigned to the MICB card. See Figure 13 on page 52, Figure 14 on page 52, and Figure 15 on page 52.

3 Define the MICB conference and chairperson bridge DNs. Refer to Figure 16 on page 53. This step provides the following:

- **a** Main DN for conference ACD groups to access the MICB agents on the card.
- **b** Conference DNs and Chairperson DNs.
- **c** TUI DN and Assistant DN.
- **d** Single number access conference and chairperson DN.

4 Define the night service route from ACDGRP NSROUTE.

The night service DN assigned in table OFRT allows conference and chairperson ACDGRPs to route to the MICB card ACD agents. Table DNROUTE defines the routes. Figure 17 on page 53 shows an example of table OFRT routing to 214 997 1400 (MICB DN) assigned in table DNROUTE.

5 Use the following tables and command interfaces (CIs) to datafill the MICB for single-card configuration:

- Table LNINV.
- Table ACDGRP.
- Table ACDSGRP.
- Table ACDLOGIN.
- Table CUSTACD (optional).
- Table ACDENLOG (optional).
- Table DNROUTE.
- Table OFRT.
- Table OFCENG.
- Service Orders.

Figure 12
LNINV example

```
LEN CARDCODE PADGRP STATUS GND BNV MNO CARDINFO
-----------------------------------------------------------------------------------
IPE1 00 0 00 00 5D51AB NPDGP WORKING N NL Y FLXA
```

Note: Cardcode can also be configured as an 8D02 digital line card.

Figure 13
ACDGRP example

```
ACDNAME CUSTGRP ACDRNGTH THROUTE NSROUTE PRIOPRO DBG
MAXCQSIZ MAXWAIT ACDMIS MSQS DISTRING OBSWTONE FRCNGTSV
OPTIONS
-----------------------------------------------------------------------
MICB BNRRCH 12 OFRT 600 OFRT 600 0 Y 2 0 N N NONE N N (ACDDISP 4)
(NONIMCUT ) $
```

Figure 14
ACDSGRP example

```
ACDGROUP SUBGROUP RECORDER
-----------------------------------------------------
MICB                1 NONE
```

Figure 15
ACDLOGIN example

```
LOGINID   CUSTGRP   PSWD        OPTIONS
1234      BNRRCH    N      N    $
```

6 The ACD login ID must match the MICB physical port connection to the Meridian SL-100. The ACD agents login must be in descending order, otherwise the MICB card cannot login the agents. After adding the ACD login IDs, enter the first agent's ID in the MICB BUI (see "Step 1 – Basic Card Settings" on page 67).

Note: If using Enhanced ACD Login to login specific ACD agent IDs, datafill tables CUSTACD and ACDENLOG to make sure MICB ACD agents can log in.

Figure 16
DNROUTE example

```
AREACODE OFCCODE STNCODE DNRESULT
-----------------------------------------------------------------
214 997 1601 FEAT ACD MICB PRIM 0 0
214 997 1602 FEAT ACD MICB SUPP 0
214 997 1603 FEAT ACD MICB SUPP 0 (Also used for TUI and Assistant DN)
        .......cont until # of ports needed are configured
214 997 1701 FEAT ACD MICB SUPP 0 0
214 997 1702 FEAT ACD MICB SUPP 0
214 997 1703 FEAT ACD MICB SUPP 0
          .......cont until # of ports needed are configured
```

Note: The DNs in bold are only required when using single access DNs.

Figure 17
OFRT example

```
RTE RTELIST
---------------------
600 (RT 214 NP LCL 9971400 Y N $) $
```

Note: Use this table to forward, through night service, the ACD main conference and chairperson conference to the MICB ACD prime DN. This example uses 997 1400 as the ACD Prime DN.

7 Define each MICB port as an M2616 digital telephone set. Define MICB ports as ACD agents in SERVORD. Define the digital set keys as follows:

- Key 1: ACD
- Key 1: M0200
- Key 1: COMMUNICTR
- Key 2: Secondary DN
- Key 3: Not Ready (NRD)
- Key 4: ACD Not Ready (ACDNR)
- Key 5: Fast Transfer (FXR)

The following example shows how to datafill the ACD agents using SERVORD. The configuration requires up to 32 LENs and 64 DNs. ACD Incalls and Key 2 use a secondary DN.

Figure 18
QLEN example

```
LEN:     IPE1  00 0 00 00
TYPE: SINGLE PARTY LINE
SNPA: 214
DIRECTORY NUMBER:     9971401            (NON-UNIQUE)
LINE CLASS CODE:  M2616 WITH DISPLAY AND HANDSFREE
CUSTGRP:         BNRRCH  SUBGRP: 0  NCOS: 0  RING: Y
ACDKEY: INCALLS     MICB1     1     N
CARDCODE:  5D51AB    GND: N  PADGRP: NPDGP  BNV: NL MNO:Y
PM NODE NUMBER     :    50
PM TERMINAL NUMBER :    1
DNGRPS OPTIONS:
OPTIONS:
COMMUNICTR
MSB
ACDNR
KEY       DN
---       --
1       ACD          9971401    INCALLS    MICBPRIM1    1    N
2      DN            9971501
KEY     FEATURE
---     -------
3 ACDNR
4 MSB $
5 FXR
16 HANDSFREE
```

Note: When adding the display feature to the M2616 set, use OPTKEY1, Option M0200.

Define Agent IDs as consecutive numbers within the lower and upper limit (see "Step 1 – Basic Card Settings" on page 67).

8 In table OFCENG, set configure ALL_ACD_LOGIN_IDS_VALID **Y**.

Figure 19
OFCENG example

PARMNAME	PARMVAL
ALLOW_RINGING_ON_TIP_SIDE	N
ALL_ACD_LOGIN_IDS_VALID	Y

This procedure is now complete

Dual-card configuration

The dual-card configuration enables a single conference to occur on two cards and have up to 62 participants depending on access type. In the dual-card configuration, one card is the primary card, and the other is the secondary card. Each card can host single-card conferences of three to 32 participants, or a dual-card conference, which occupies ports on both cards.

> ***Note:*** There is no need for MICB cards in a dual-card configuration to reside next to each other in an IPE shelf. Software establishes the audio connections between the two cards. There is no hardware connection between the two cards.

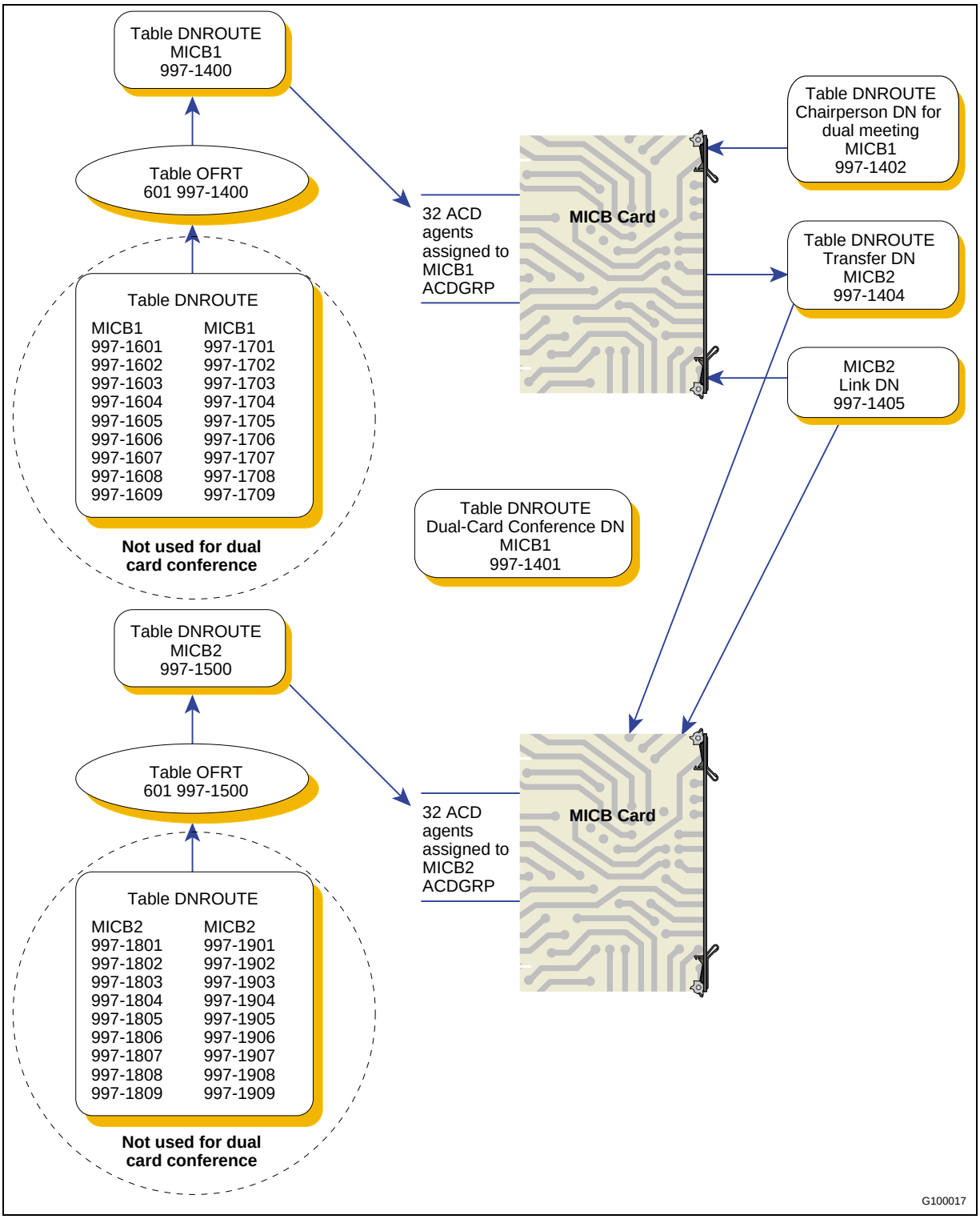
Datafill the following tables and command interfaces for dual-card configuration:

- table LNINV
- table ACDGRP
- table ACDSGRP
- table ACDRTE (requires a new entry)
- table ACDLOGIN
- table DNROUTE
- table OFRT

Figure 20 on page 56 provides an example of the datafill for dual-card setup.

> ***Note:*** If single-number access is being used, DN pairs are not required. Instead configure two single-number access DNs: one for callers to use to access simple conferences on the primary card and one for callers to use to access simple conferences on the secondary card.

Figure 20
Dual-card conference, 1 conference, 62 ports



Service Orders
Add an additional ACD group for the second card.

Figure 21
ACDGRP example

```
ACDNAME CUSTGRP ACDRNGTH THROUTE NSROUTE PRIOPRO DBG
MAXCQSIZ MAXWAIT ACDMIS MSQS DISTRING OBSWTONE FRCNGTSV
OPTIONS
-----------------------------------------------------------------------
MICB2 BNRRCH 12 OFRT 601 OFRT 601 0 Y 2 0 N N NONE N N (ACDDISP 4)
(NONIMCUT ) $
```

Add additional ACD subgroup information for the second card.

Figure 22
ACDSGRP example

```
ACDGROUP SUBGROUP RECORDER
-------------------------------------------------------
MICB2 1 NONE
```

Add additional login IDs for the second card agent logins. These login IDs must be in sequential order.

Figure 23
ACDLOGIN example

LOGINID	CUSTGRP	PSWD		OPTIONS
1234	BNRRCH	N	N	$

Add table DNROUTE to provide DNs for the following:

- second MICB card (for single-card conference and chairperson)
- transfer DN (to transfer conference calls from MICB card 1 to MICB card 2)
- link DN (provides speech path between the two cards)
- 62-port Main conference DN
- chairperson DN for MICB card 1

> ***Note:*** From all of these DNs, part are for the primary card and the rest are for the secondary card. However, when configuring these DNs in the MICB BUI, all dual-card DNs are configured on the primary card.

Figure 24
DNROUTE example

```
AREACODE OFCCODE STNCODE DNRESULT
-----------------------------------------------------------------
214 997 1600 FEAT ACD MICB2 PRIM 0 0
214 997 1401 FEAT ACD MICB1 SUPP 0 (Used for Dual Card MAIN Conference)
214 997 1402 FEAT ACD MICB1 SUPP 0 (Used for Dual Card Card 1 chairperson)
214 997 1403 FEAT ACD MICB2 SUPP 0 (Used for Dual Card Card 2 chairperson)
214 997 1404 FEAT ACD MICB2 SUPP 0 (Used for Dual Card Transfer DN)
214 997 1405 FEAT ACD MICB2 SUPP 0 (Used for Dual Card Link DN)
214 997 1802 FEAT ACD MICB2 SUPP 0 (Used for single card conferences)
214 997 1803 FEAT ACD MICB2 SUPP 0 (Used for single card conferences)
        .......cont until # of ports needed are configured
```

Note: The DNs in bold are only required when using single access DNs.

Use table ACDRTE to allow a dual-card conference to overflow from MICB card 1 to MICB card 2 when there are no more available ports on card 1.

Figure 25
ACDRTE example

```
ACDGRP      OPTNAME              OPTION
MICB1       OVFL    OVFL         (MICB 2)
```

Use table OFRT to add the DN routing for the second MICB card.

Figure 26
OFRT example

```
RTE RTELIST
---------------------
601 (RT 214 NP LCL 9971600 Y N $) $
```

Configuration procedure

To set up a dual-card configuration using direct meeting access, follow the steps in Procedure 3 on page 59.

Procedure 3
Configure a dual-card conference

1. Install the two cards and their Ethernet adapters identical to single-card installation. See Procedure 4 on page 61.

   Note: There is no need for the two cards to be next to each other in the shelf or cabinet.

2. Busy and Return to Service (RTS) the two cards in the IPE PM level of the MAP terminal.

3. For each card, connect a VT100 terminal to the card and enter the keycode information, including the appropriate number of ports. Wait for each card to verify the keycode information.

4. For each card, log into the card through the CLI (default login: admin). Enter the System Attributes Editor, enter **sa** then **sy**, and modify the following information:

   The subnet mask, the gateway address, and the IP address

   Note: After entering the Ethernet information, the CLI asks if you want to restart the cards. Select **YES** at this point.

5. From a PC, ping each MICB card to make sure that they have a correct connection to the LAN. To ping an IP card, perform the following:

   a Click on the **Start** button and select **Run** from the Start Menu.

   b In the Open: field, enter **ping <IP address>** where <IP address> is the IP address of one of the MICB cards.

   c Click the **OK** button, and observe the DOS window that opens. If you receive the message: “Reply from <IP address>...”, you have set up the LAN connection correctly and you can continue. If you receive the message: “Request timed out”, there is a problem with the LAN connection.

6. Configure the DNs for the dual-card configuration.

7. Configure each port on the two new cards as an M2616 set. See Procedure 2 on page 51. Refer to SERVORD information in Figure 18 on page 54.

8. Open up the web browser on your PC. In the URL field of the browser, enter the following: **<IP address>** where < IP address> is the MICB IP address.

9. Log into the BUI (defaults: admin and 000000) and select the MICB Installation Wizard (see “MICB Installation Wizard” on page 67).

This procedure is now complete

MICB installation and configuration procedures

Once the site is prepared for installation and the Meridian system software is configured, use the steps in Table 10 to complete the MICB installation.

Table 10
MICB installation summary

Step	Description
1	Install a serial Maintenance terminal for preliminary card setup using the following procedures: • Procedure 4, "Install the Ethernet Adapter card," on page 61 Use one of the following three procedures to connect the serial Maintenance terminal to the MICB as follows: • Procedure 5, "Access the MICB directly," on page 62 • Procedure 6, "Access the MICB remotely using a modem," on page 63 • Procedure 7, "Access the MICB remotely using a LAN hub," on page 63 If your system is an CSE 1000 or Option 11C, use one of the following three procedures to connect the serial Maintenance terminal to the MICB as follows: • Procedure 8, "Access the MICB directly – Option 11C or CSE 1000," on page 64 • Procedure 9, "Access the MICB remotely using a modem– Option 11C or CSE 1000," on page 64 • Procedure 10, "Access the MICB remotely using a LAN hub – Option 11C or CSE 1000," on page 65
2	Install the MICB card(s) using the following: • Procedure 11, "Install MICB cards," on page 65
3	Configure the Maintenance terminal for command line interface (CLI) access as follows: • Procedure 12, "Set up CLI access from the Maintenance," on page 65 Define the MICB Ethernet parameters using the CLI System Attributes Editor as follows: • Procedure 13, "Configure initial card parameters using the CLI," on page 66
5	Complete the installation using the MICB BUI Install Wizard as follows: • Procedure 14, "Access the administration BUI," on page 66 • See "MICB Installation Wizard" on page 67 for a description of how to configure the MICB card(s) using the Install Wizard.

Procedure 4
Install the Ethernet Adapter card

1. Remove the cover plate from the I/O panel at the rear of the IPE module.
2. Remove the I/O panel retaining screws and lift the I/O panel from the module.
3. Set up the I/O panel filter connector for the card slot you have assigned for the MICB card installation.
4. Your next step depends on the configuration of that filter connector.
   - **a** If this connector has a permanent connection to the backplane cable, remove the filter connector from the I/O panel.
   - **b** If a 50-pin connector joins the filter connector and the backplane cable, disconnect the 50-pin connector from the I/O panel filter connector. Then, being careful to save the retaining screws, remove the filter connector from the I/O panel.
5. Install the NT5D52AC Ethernet Adapter card into the selected I/O panel connector cutout using the saved retaining screws.
6. Fasten the I/O panel to the module using the retaining screws.
7. Replace the module cover plate.

This procedure is now complete

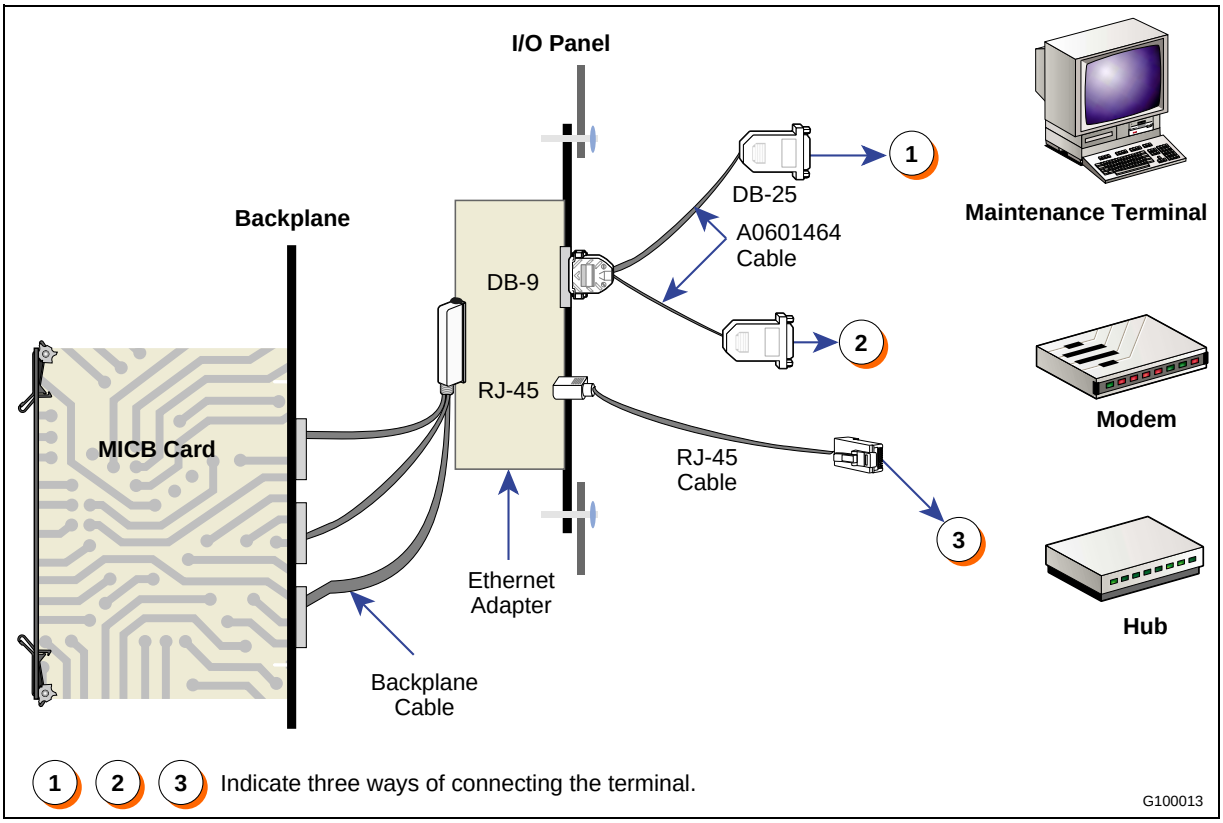
Table 11 lists the pin number assignments for the Maintenance terminal cable that connects the IPE module I/O panel that the following procedures use. The cable connects to the nullmodem for direct terminal connection or to a modem for a remote maintenance terminal.

Table 11
Maintenance cable

J2 DB-25 pin	J1 50-pin	Description	J2 DB-25 pin	J1 50-pin	Description
1	25	Reserved	14	48	LAN_Rx-
2	22	RS-232 Tx	15	13	Reserved
3	20	RS-232 Rx	16	14	Reserved
4	18	Reserved	17	15	Reserved
5	10	Reserved	18	36	Reserved
6	16	Reserved	19	37	Reserved
7	21	GND	20	19	Reserved
8	17	Reserved	21	38	Reserved
9	11	Reserved	22	39	Reserved
10	24	LAN_Tx+	23	40	Reserved
11	49	LAN_Tx-	24	41	Reserved
12	12	Reserved	25	N.C.	Not Connected
13	23	LAN_Rx+			

Refer to Figure 27 when connecting the Maintenance terminal (that is, VT100) in the following procedures.

Figure 27
Terminal connection through the Ethernet Adapter



Procedure 5
Access the MICB directly

1 Position the Maintenance terminal on a desk near the system.

2 Verify that the Ethernet Adapter card is on the I/O panel as described in Procedure 4 on page 61.

3 Plug the terminal cable DB-9 female connector into the DB-9 male connector on the Ethernet Adapter card on the I/O panel.

4 Plug the DB-25 male connector at the other end of the terminal cable into the RS-232 connector on the terminal. A nullmodem is not required. If a gender changer is required, purchase one from a local electronics store.

This procedure is now complete

Procedure 6
Access the MICB remotely using a modem

1. Verify that the Ethernet Adapter card is on the I/O panel as described in Procedure 4 on page 61.
2. Plug the terminal cable DB-9 female connector into the DB-9 male connector on the Ethernet Adapter card on the I/O panel.
3. Plug the DB-25 male connector at the other end of the terminal cable into the DB-25 female connector of a DB-25F/DB-25M nullmodem adapter. If a female-to-female nullmodem is required, use a customer-supplied nullmodem.
4. Plug the DB-25 male connector of the nullmodem adapter DB-25F/DB-25M into the DB-25 female connector on the modem. If a female-to-female nullmodem is required, use a customer-supplied nullmodem.
5. Plug the modular modem cable RJ11 plug into the RJ11 jack on the modem.
6. Plug the other end of the modular modem cable RJ11 plug into the RJ11 jack on the wall.

This procedure is now complete

Procedure 7
Access the MICB remotely using a LAN hub

1. Verify that the Ethernet Adapter card is on the I/O panel as described in Procedure 4 on page 61.
2. Plug the modular cable RJ-45 plug into the RJ-45 jack on the NT5D52AC Ethernet Adapter card.
3. Plug the RJ-45 plug at the other end of the modular cable into the Ethernet LAN hub.
4. Make the remaining Ethernet connections as required using standard Ethernet connection rules.

Note: For local testing purposes, or direct connection from the Ethernet port to a PC, use an Ethernet cross-over cable purchased at a local computer store.

This procedure is now complete

If installing the MICB card in an Option 11C or CSE 1000, use the following procedures to connect the Maintenance terminal.

Note: These procedures do not apply to the Meridian 1 Options 51C, 61C or 81C or the Meridian SL-100.

In the procedures that follow, the connections are the same for the Option 11C and the CSE 1000, the only difference is that the connectors are on the back of the Call Server and Media Gateway for the CSE 1000, whereas they are on the bottom of the Option 11C cabinet.

Table 12 describes the DB-9 pin assignment that the next two procedures use.

Table 12
DB-9 RS-232 port pin out

9-pin (male) serial connector pin #	Signal Description
2	RS-232 TX (transmit)
3	RS-232 RX (receive)
5	GND

Procedure 8
Access the MICB directly – Option 11C or CSE 1000

1. Position the Maintenance terminal on a desk near the system.
2. If the system is an Option 11C perform the following:
   - **a** Verify that the Ethernet Adapter is installed in the Option 11C.
   - **b** Plug the terminal cable DB-9 female connector into the DB-9 male connector on the Ethernet Adapter on the I/O panel.
   - **c** Plug the DB-25 male connector at the other end of the terminal cable into the RS-232 connector on the terminal. If the connection requires a gender changer, obtain one at a local electronics store.
3. If your system is a CSE 1000, connect the NTBK48 three-port SDI cable to the 9-pin SDI connection (COM RS-232) at the back of the Call Server and Media Gateway.

This procedure is now complete

Procedure 9
Access the MICB remotely using a modem– Option 11C or CSE 1000

1. Verify that the Ethernet Adapter/Medium Access Unit (MAU) is installed in the Option 11C or CSE 1000. Insert the industry-standard MAU into the Ethernet Connection on the back of the Call Server and Media Gateway.

   Note: The Ethernet MAU comes with the cable kits for the Call Server and Media Gateway.
2. Plug the terminal cable DB-9 female connector into the DB-9 male connector on the Ethernet Adapter/MAU on the I/O panel.
3. Plug the DB-25 male connector at the other end of the terminal cable into the DB-25 female connector of the customer-supplied DB-25F/DB-25M nullmodem adapter.
4. Plug the DB-25 male connector of the DB-25F/DB-25M nullmodem adapter into the DB-25 female connector on the modem.
5. Insert the modular RJ11 plug into the RJ11 jack on the modem.
6. Insert the other end of the RJ11 plug into the RJ11 jack on the wall.

This procedure is now complete

Procedure 10
Access the MICB remotely using a LAN hub – Option 11C or CSE 1000

1 Verify that the Ethernet Adapter/MAU is installed in the Option 11C or CSE 1000. Insert the industry-standard MAU into the Ethernet Connection on the back of the Call Server and Media Gateway.

Note: The MAU comes with the cable kits for the Call Server and Media Gateway.

2 Insert the modular cable RJ-45 plug into the RJ-45 jack on the Ethernet Adapter/MAU.

3 Insert the RJ-45 plug at the other end of the modular cable into the LAN hub.

4 Make the rest of the Ethernet connections as required using standard Ethernet connection rules.

This procedure is now complete

Procedure 11
Install MICB cards

1 Identify the card slots selected for MICB card(s). Refer to Table 4 on page 42.

2 Make sure to properly place the PCMCIA hard drive card in the lower faceplate PCMCIA slot.

3 Pull the top and bottom extractors away from the MICB faceplate.

4 Insert the MICB card into the card guides and carefully push it until it makes contact with the backplane connector.

5 Push the top and the bottom extractors towards the faceplate to insert the MICB card into the faceplate connector and to lock it in place.

6 Observe the red LED at the top of the faceplate (the card LED).

This LED blinks three times after the self-test successfully completes. When the MICB software loads, the LED blinks three more times and then remains lit. This takes approximately 45 seconds.

7 Repeat Steps 1 through 6 for each additional MICB card.

This procedure is now complete

Procedure 12
Set up CLI access from the Maintenance

1 Specify the VT-100 type terminal interface characteristics to make sure they are compatible with the MICB RS-232 interface.

2 Set the interface parameters as follows:

- Transmission speed: 9600 bps
- Data bits: 8
- Stop bit: 1
- Parity: No
- Flow control: none

Note: Do not use XON/XFF flow control.

This procedure is now complete

The next step is to define IP parameters using the CLI.

Procedure 13
Configure initial card parameters using the CLI

1 From the VT-100 type terminal press the **Enter** key.

The logon window appears.

2 At the login prompt, enter the following:

admin

Where “admin’ is the default administrator password.

3 Access the System Administration menu. Enter:

SA

The System Administration menu opens.

4 Access the System Attributes Editor. Enter:

SY

The System Attributes Editor opens.

5 Enter the following IP attributes for the MICB card:

- Subnet mask – The part of the IP address which represents a subnetwork within a network. The subnet mask has a format of XXX.XXX.XXX. XXX, where XXX is in the range 0-255. Subnet mask in binary presentation of 32 bits has at least the first eight digits “1” and the last digit is “0”.
- Gateway address – Is in the XXX.XXX.XXX.XXX format, where every token is in the range 0-255.
- IP address – The internet protocol address which has the same format as the gateway address.

6 Enter **S** to save the parameters.

7 Exit the CLI and proceed to Procedure 14. All other card configuration is performed from the BUI.

This procedure is now complete

Procedure 14
Access the administration BUI

1 Check the installation by doing the following:

a Run a browser, either Netscape or Microsoft Internet Explorer.

b In the location field, enter:

http://<MICB IP address>

c Login as an administrator. The default ID and password are admin and 000000 (six zeros).

d Proceed with the installation using the Installation Wizard (see below).

This procedure is now complete

MICB Installation Wizard

Overview

The MICB Installation Wizard provides an easy method for configuring new systems. Only a user who logs in as an administrator can use the Installation Wizard. An administrator accesses the Installation Wizard by clicking on the Install Wizard link on the BUI's MICB Dashboard. For more information about accessing this tool, see, "Administration BUI" on page 96.

After completing a Wizard session, the administrator can try operating the card (that is, schedule a conference and place a call), so long as the Meridian system setup is complete. An administrator can return to the Wizard at any time to change system definitions.

The Installation Wizard consists of four steps, each of which appears on a separate window. For a new installation, follow the Wizard step-by-step. For already installed systems, go directly to a specific window to modify one or more fields. The windows are as follows:

1. **Basic Card Settings** – use this window when getting started.
2. **Access Numbers** – select the dialing method (that is, direct meeting or single-number) and enter the DNs according to Meridian system configuration.
3. **Define First User** – define at least one user in order to perform sanity tests, such as scheduling conferences and placing calls. This step eliminates the need to go to a separate window to define a user after finishing using the Wizard, just to perform some testing.

   Because this step is required only during initial installation, the BUI excludes it (that is, grays it out) after a successful installation. Normal user administration is performed from a separate window in the Administration BUI.
4. **Dual Card Meetings** – define the parameters for dual-card meetings. This step appears only in the primary card of a dual-card MICB configuration.

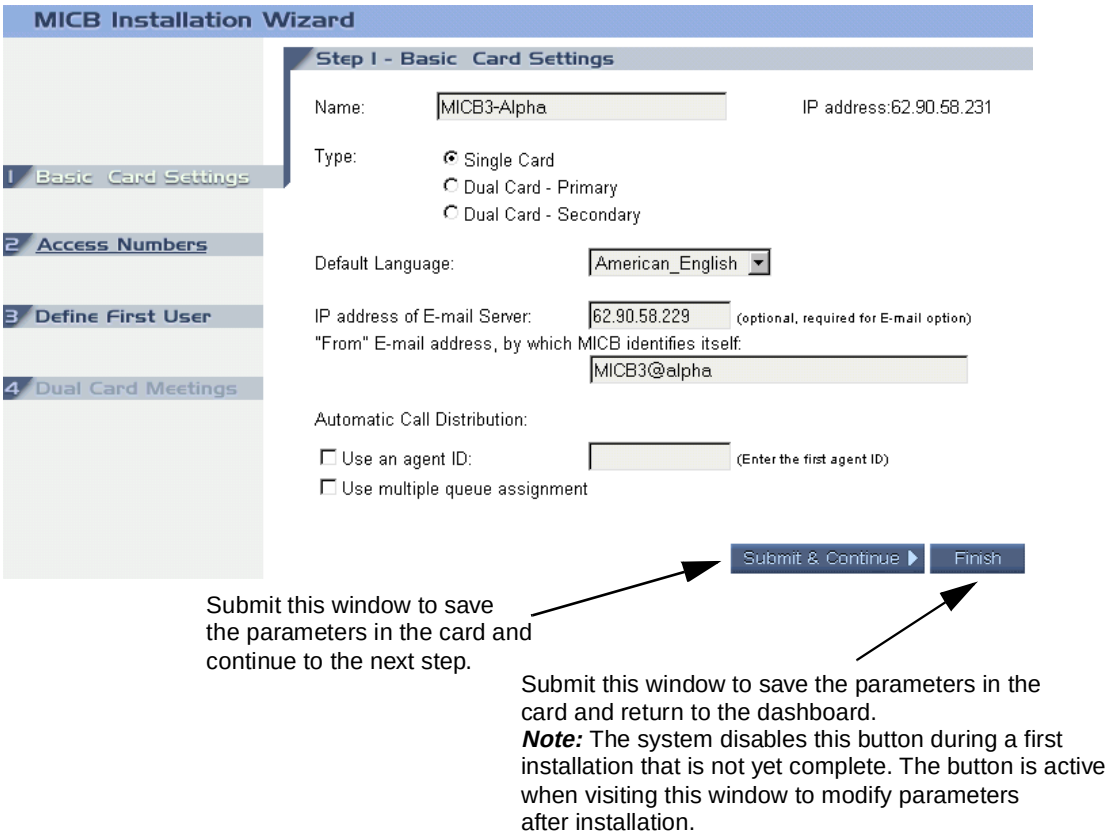
Conventions

All Installation Wizard windows list the steps on the left of the window. During installation advance step-by-step by clicking on the **Submit & Continue** button. After installation is complete, access a specific step directly by clicking on its name in the list.

Step 1 – Basic Card Settings

Figure 28 on page 68 shows the Basic Card Settings window. Click on the **Install Wizard** link on the MICB Dashboard to access this window.

Figure 28
Installation Wizard: Step 1 – Basic Card Settings window



Submit this window to save the parameters in the card and continue to the next step.

Submit this window to save the parameters in the card and return to the dashboard.
Note: The system disables this button during a first installation that is not yet complete. The button is active when visiting this window to modify parameters after installation.

Table 13 describes the parameters, from top to bottom, of the Basic Card Settings window.

Table 13
Basic Card Settings parameters

Item	Description
Name	Enter the card's name. *Range:* Free text up to 20 characters.
IP Address	Shows the IP address of the card, which appears as view only. ***Note:*** Define the card address using the CLI.

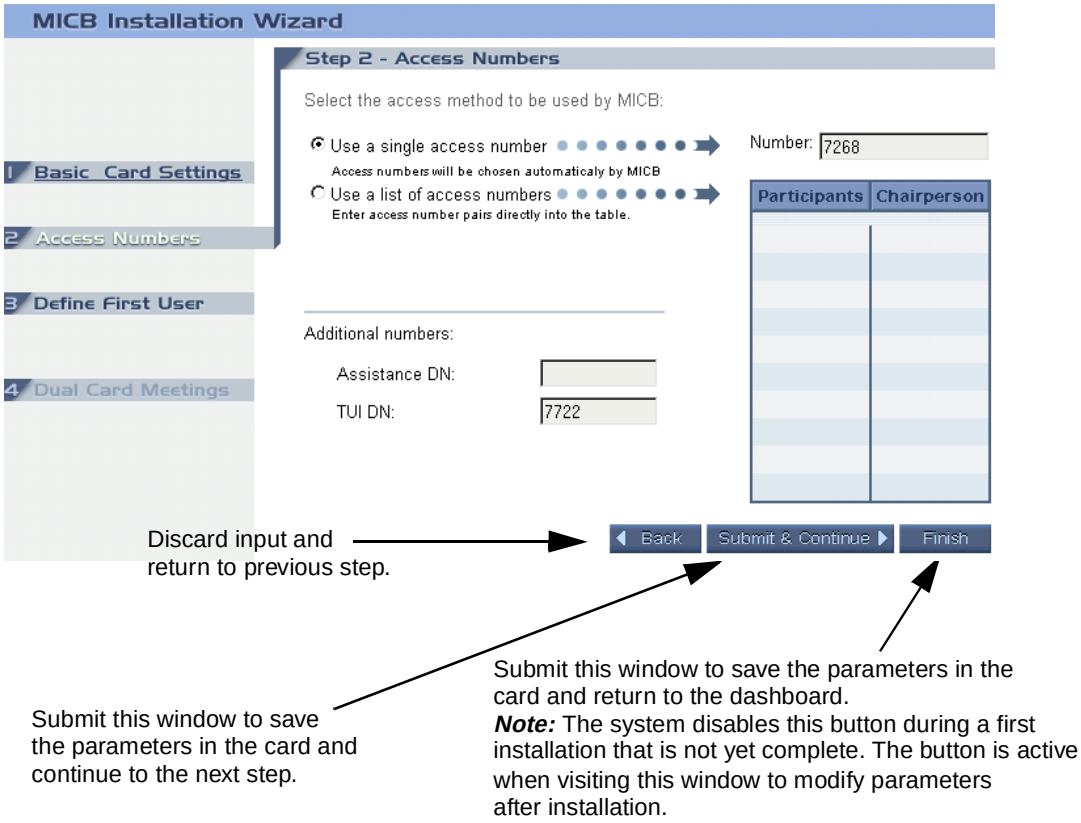
Table 13
Basic Card Settings parameters (Continued)

Item	Description
Type	Define the card's configuration type as follows: • Single card (stand-alone). • Primary card in a dual-card pair. • Secondary card in a dual-card pair. ***Note 1:*** Dual-card meeting configuration in Step 4 uses this information. If information is changed here, a window opens reminding you to change the settings of a dual-card meeting. ***Note 2:*** When an MICB card of type "single" already configured with 10 DNs pairs is changed to "primary" or "secondary", one of the DN pairs must be deleted. This is because in a dual-card set one DN pair is reserved for the dual meeting configured in Step 4. The MICB attempts to find a free DN pair (that is, with no conferences scheduled on it) and deletes it. If no such DN is found, the MICB deletes the DN pair with the fewest conferences. In this case, a confirmation box appears that allows the administrator to confirm or cancel the whole operation. ***Note 3:*** When a "primary" or "secondary" card is changed to be "single", all dual meetings are changed to simple meetings and their port size is reduced to the capacity of this card.
Default Conference Language	Determine the default voice-prompt language for conferences and the TUI. When scheduling a conference, users can select a language from the available set, but if the user does not specify a language this parameter applies. *Default:* American English.
IP address of E-mail Server	Enter the IP address of the server that the MICB uses to send scheduling confirmation and administration E-mail messages. If this field is left empty, or an incorrect address is specified, the MICB will not send E-mail messages. However, the rest of the system will operate properly. ***Note:*** The E-mail server must support the Simple Mail Transfer Protocol (SMTP).
"From" E-mail address	Enter the E-mail address which the MICB uses to identify itself when sending E-mails. This item appears in the "From:" field of sent E-mails. ***Note 1:*** Some E-mail servers require this information as a mandatory field. It cannot be empty, but it can be a non-existent address. Some servers will not deliver the E-mail if it is not correct. ***Note 2:*** MICB never receives E-mails, so it does not require an address. However, the "from" address is used when returned mail occurs (for example, someone replies to the MICB's E-mail or the network returns an undeliverable E-mail). If the address is unreal, the returned mail is not delivered. If the "from" address is someone's real address, they will receive the MICB's returned mail.
Automatic Call Distribution	Define the ACD setup according to the Meridian system ACD configuration. **Use an agent ID** – Indicate whether ACD is configured with the agent ID option. If yes, enter the four-digit agent ID of the first MICB port in the adjacent text box. The other ports use the succeeding agent IDs. **Use multiple queue assignment** – Indicate if ACD is configured with the multiple-queue option. An entry is required, because this option affects the agent login process which the system applies to the ports.

Step 2 – Access Numbers

Use this step to define the access method, direct meeting or single-number, and the DNs according to Meridian system configuration. Figure 29 shows the Access Numbers window.

Figure 29
Installation Wizard: Step 2 – Access Numbers window



Discard input and return to previous step.

Submit this window to save the parameters in the card and continue to the next step.

Submit this window to save the parameters in the card and return to the dashboard.
Note: The system disables this button during a first installation that is not yet complete. The button is active when visiting this window to modify parameters after installation.

Table 14 describes the parameters, from top to bottom, of the Access Numbers window. Configure all the DNs in this window according to Meridian system configuration.

Table 14
Access Numbers parameters

Item	Description
Use a single access number	Enter the single DN to use for accessing all conferences.
Use a list of access numbers	This field requires a list of DN pairs, because with direct meeting access users dial the conference DN and then the chairperson DN to enter the meeting. The number of DNs defined equals the maximum number of simultaneous conferences allowed. Configure up to 10 DN pairs. Define only nine DN pairs for primary or secondary cards in a dual-card set. One DN must be reserved pair for dual-card meetings (see "Step 4 – Dual Card Meetings" on page 71).
Use a list of access numbers (Continued)	Delete DNs by clicking on a table cell and pressing the **Delete** key, which leaves the cell empty. DNs that are in use by a future or current conference cannot be deleted; an error message appears when submitting the form. When upgrading from MICB 2, the system uses the same table. The old DN pairs appear in the table.
Assistance DN	Enter the DN of an operator or attendant. The system dials this DN when the chairperson in an active conference selects "call assistant" from the TUI or BUI.
TUI DN	Enter the DN to access TUI services.

Step 3 – Define First User

This step appears only during a new installation. Use this window to define a new user for testing the MICB after completing installation. The user defined here can be deleted, or modified, from the regular User Administration window.

This window is identical to the "new user" window (see Figure 54 on page 110), except it includes the Wizard step titles at the top of the window. The action buttons are the same as in Step 2, except that the Finish button only appears in the case of a single-card MICB.

Step 4 – Dual Card Meetings

Configure the parameters for a dual-card meeting in this window (see Figure 30 on page 72). This step appears only when the card is a member of a dual-card set (that is, the configuration type selected in Step 1 is either "Dual Card – Primary" or "Dual Card – Secondary").

Input the data in this window is allowed only on the primary card; on the secondary card this window appears as view only.

Note: The secondary MICB card must be installed and configured first. Dual-card meeting parameters and DNs are defined in the primary MICB only. The primary MICB sends the relevant information to the secondary MICB. Therefore, the secondary MICB must be connected to the LAN and operational when the primary is being configured.

All DNs must be configured in the Meridian system.

Figure 30
Installation Wizard: Step 4 – Dual Card Meetings

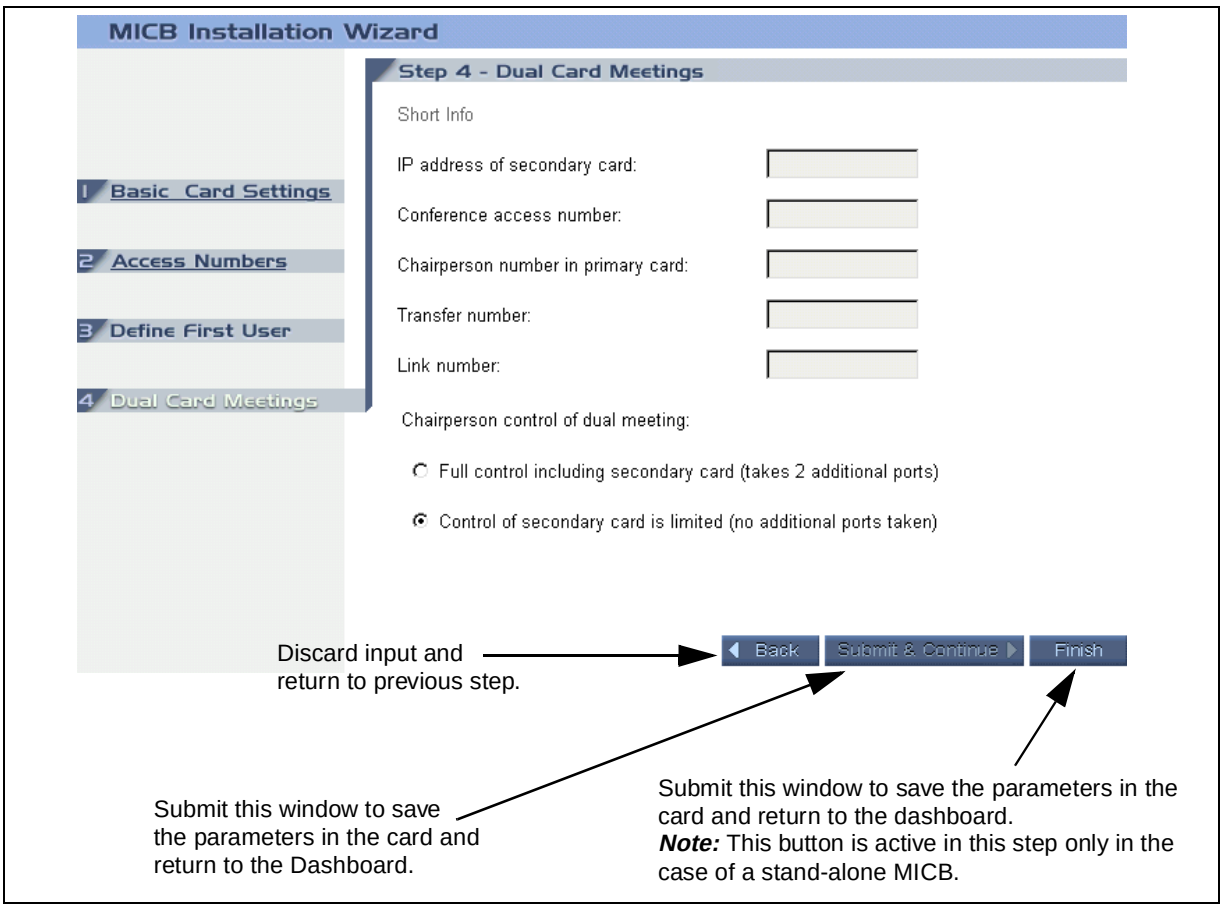


Table 15 describes the parameters, from top to bottom, of the Dual Card Meetings window.

Table 15
Dual Card Meetings parameters

Item	Description
IP address of secondary card	Enter the IP address of the secondary card.
Conference access number	Enter the DN of the dual-card meeting. Callers will dial this number to access the dual-card meeting.
Chairperson number in primary card	Enter the chairperson DN for the dual-card meeting. The chairperson uses this number to access the dual-card meeting.
Transfer number	Enter the DN that the MICB uses to transfer calls from the primary card to the secondary card. The system hides this number from end users.
Link number	Enter the DN that the MICB uses to create a voice path between both cards. The system hides this number from end users.
Chairperson control of dual meeting	For more information see, "Dual-card meeting" on page 96. **Full control including secondary card** – If this is clicked, the chairperson commands apply to both cards. In this case, the maximum conference size in a 64-port card pair is 60 ports. **Control of secondary card is limited** – If this is clicked, some chairperson commands are limited to the primary card (for example, TUI roll call command and dial out). The maximum conference size in a 64-port card pair is 62 ports.

Browser user interface

Purpose

This chapter describes how to use the browser user interface (BUI), a web-based application, for conference scheduling, chairperson operations, and system administration.

The chapter contains the following sections:

- **"Overview" on page 75** – introduces the browser user interface and its system requirements.
- **"Scheduling BUI" on page 81** – describes the interface that users and super-users can use to schedule conferences.
- **"Chairperson operations" on page 91** – describes the interface that a chairperson can use to control an active conference.
- **"Administration BUI" on page 96** – describes the interface that an administrator uses for MICB configuration and administration.

Overview

The HTML/HTTP based BUI provides a fast response time and supports 20 active BUI users in a direct LAN connection. The BUI supports open access from anywhere in the Internet, even behind gateways and firewalls. Access the MICB web server over an Ethernet connection. To access the MICB server, use the following internet browsers:

- Microsoft Internet Explorer, version 4.01 or higher.
- Netscape Communicator, version 4.5 or higher.

Note: The system does not support browsers running on MacIntosh computers.

The MICB web server runs on the MICB card. The MICB card acts as a stand-alone system. Users navigate their browser directly to the card's IP address.

User types

When logging in to the MICB BUI, your login ID connects you to the server as a distinct user type. The administrator determines the user type for each user. Table 16 shows the three user types and their functionality.

Table 16
BUI user types

User type	Description
User	A user can reserve meetings under their account, and modify and delete these meetings. Users can see only the meetings that they schedule.
Super-user	In addition to normal user functions, a super-user can reserve meetings under other users' accounts. A super-user can modify and delete the meetings of other users. Super-users can see all meetings.
Administrator	The administrator manages MICB system parameters and resources such as user IDs and group-call tables.

Log into the BUI

Figure 31 shows the first window that appears when reaching the BUI.

Figure 31
MICB home page layout

The only possible action from this window is to click on the **LOGIN** button.

Follow the steps in Procedure 15 to login.

Procedure 15
Login to the BUI

1 Click on the **LOGIN** button.

The window in Figure 32 appears.

Figure 32
Login dialog box (Internet Explorer)

2 Enter your login ID in the “User name” field. To log into the administrator BUI, enter an administrator ID.

3 Enter your password in the “Password” field. When logging in the first time, enter six zeroes (000000). To log into the administrator BUI, enter an administrator password.

4 Click on the **OK** button.

If your login is unsuccessful, the system re-displays the dialog box. After a pre-defined number of unsuccessful logins, the system blocks the user.

Note: To find a missing password, see “Appendix A: Password security” on page 187.

This procedure is now complete

Depending on the login ID type, Table 17 shows the windows that open when entering the BUI.

Table 17
Login entry point

Login entry	BUI Application
Regular or super-user ID	Scheduling BUI. Schedule meetings from this window.
Administrator user ID	MICB Dashboard. This window opens the administration dashboard, from which the administration of system resources and options, such as users, permanent conferences, conference access numbers etc., can be performed.
Meeting chairperson number and password	Meeting Control window. This window allows a chairperson to control an active meeting.

Login password change

Follow the steps in Procedure 16 to change passwords after logging in.

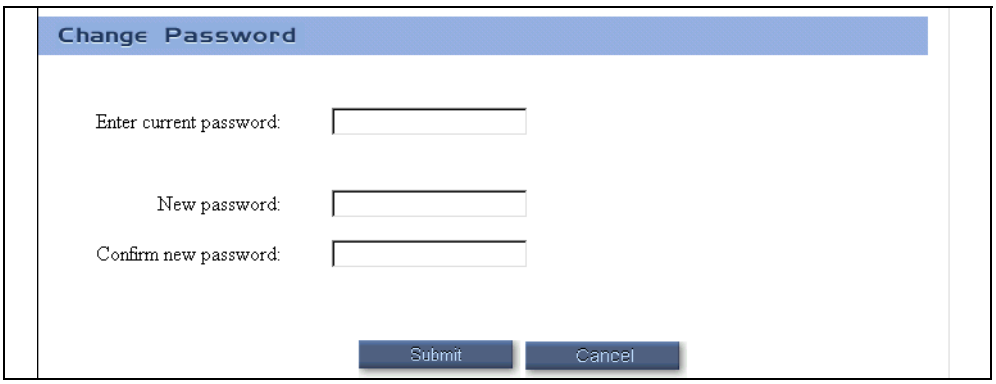
Procedure 16
Change your login password

1 Click on the change **Change Password** button on the first window that opens after logging in (see Figure 36 on page 82).

Note: Change Password is a link on the Dashboard.

The window in Figure 33 opens.

Figure 33
Change password window



2 Enter the current password for authentication, then the new password. Enter the new password a second time for confirmation.

The passwords do not appear when entered (asterisks appear).

3 Click on the **Submit** button to apply the changes. Click on the **Cancel** button to abort the changes.

In both cases, the system returns to the previous window.

This procedure is now complete

Customize the BUI home page and title bar

Initially, the MICB home page comes with a set format. The Customized BUI Home Page and Title Bar feature enables administrators to add a customer-designed image to the home page and a company logo to the title bar. The title bar is fixed through the entire BUI session.

The following are the prerequisites for using this feature:

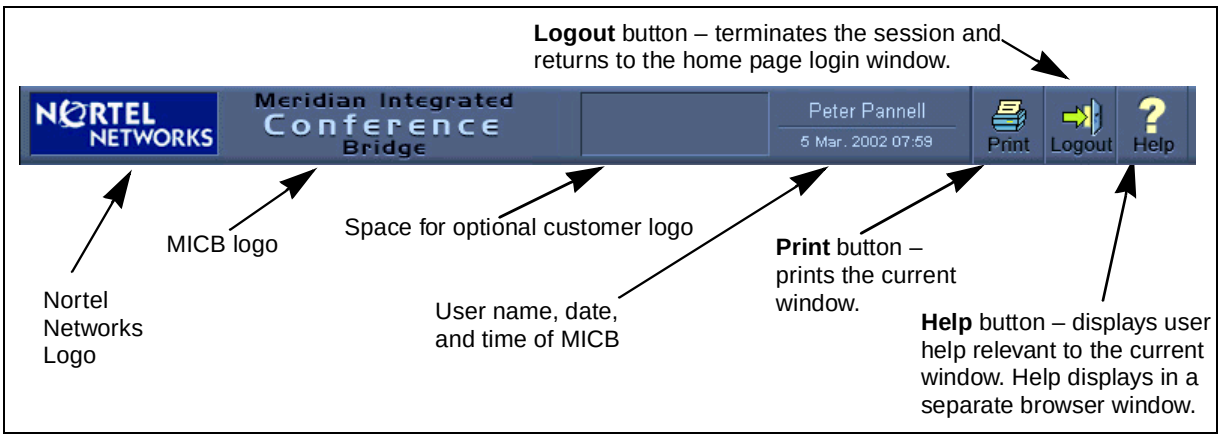
- The image must fit reasonably in the browser window. Nortel Networks recommends that the image be no larger than 690 pixels wide and 420 pixels high.
- The logo must be no larger than 124 pixels wide and 40 pixels high.
- The image must be in GIF format.

The MICB Dashboard provides a tool for uploading and installing the customer's images (see "Company images upload" on page 105).

Fixed title frame

Figure 34 shows the fixed title frame that appears on top of all conferences. Subsequent screen captures do not show this frame.

Figure 34
BUI fixed title frame



Help window

Clicking on the **Help** button on the title frame opens a separate browser window in which it displays the Help window. This enables users to continue with BUI operations while the on-line help is open. The following four different help files exist, according to user type and role:

- User Help (scheduling windows)
- Super-user help (scheduling windows for super-user)
- Chairperson control help (chairperson control window)
- Administrator help

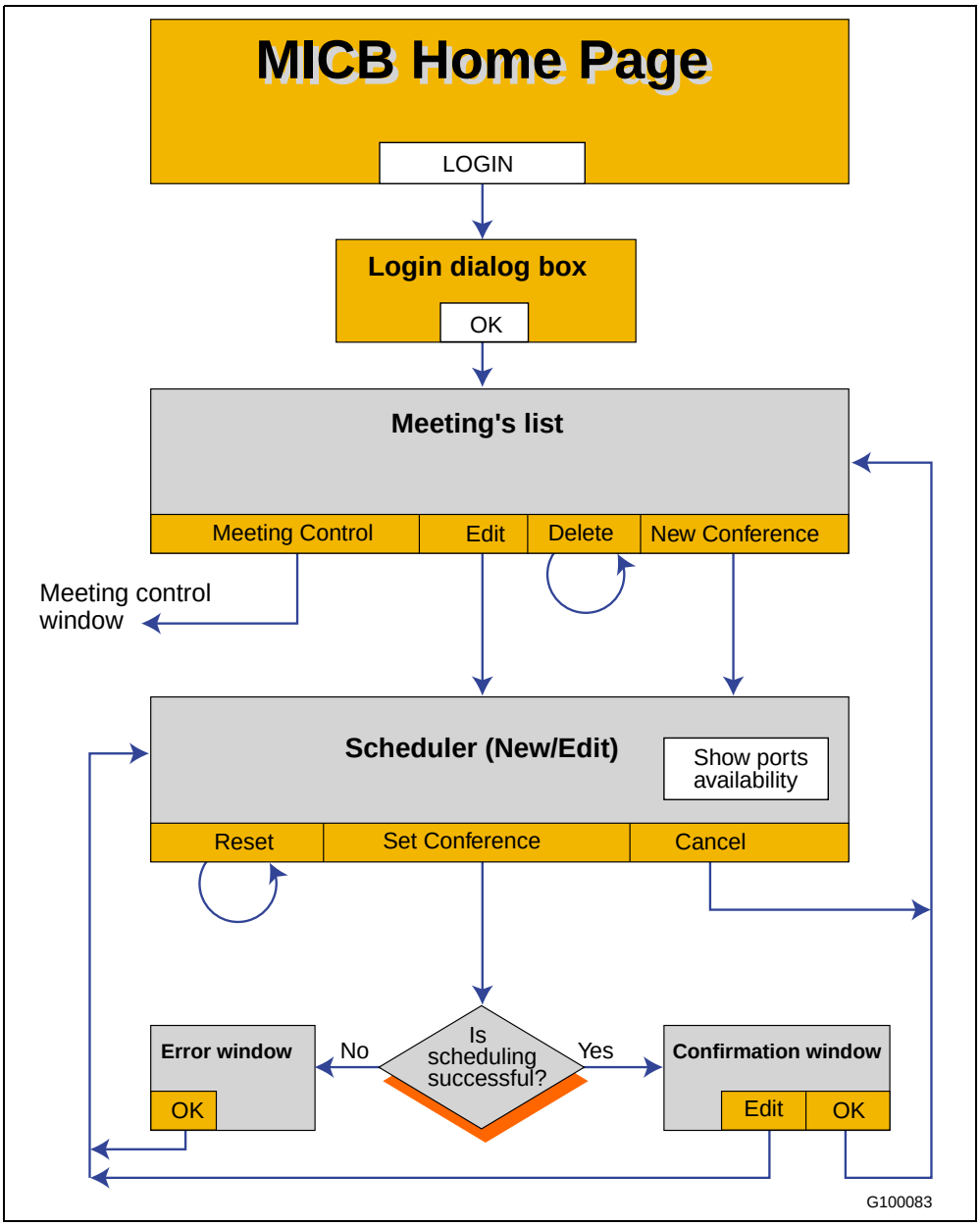
The Help window has two frames; topic links appear on the left and help text appears on the right. Click on an item in the left frame help topics to access information about the required topic.

Click on the **Close window** link to close the Help window.

Scheduling BUI

Figure 35 shows the navigation between the Scheduling BUI windows.

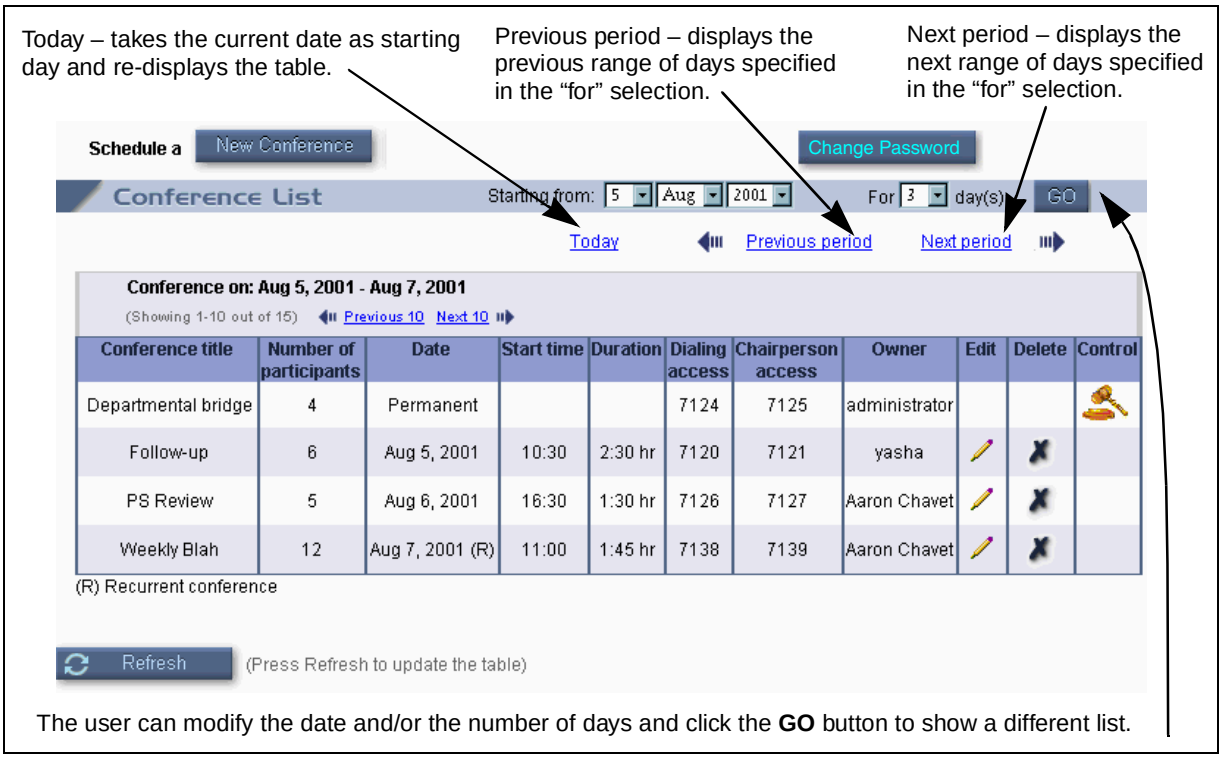
Figure 35
Scheduling BUI navigation flowchart



Meetings List window

Figure 36 on page 82 shows the Meeting List window that appears directly after user login. This window displays a table of the user's meetings and provides access to scheduling operations.

Figure 36
Meetings List window (super-user's display)



If this window is accessed by a user, the window displays the conferences scheduled by that user only. If this window is accessed by a super-user, the window displays all scheduled conferences. The system sorts the list by time. The list includes conferences that begin on the previous day, but finish on the specified date. In this case, the system displays the conference on the top of the list.

The maximum number of conferences per page is 10. When the list of conferences is longer than one page, click on the "Next 10" or "Previous 10" links to view additional conferences.

For each conference, click on the corresponding icon next to the conference to perform the following:

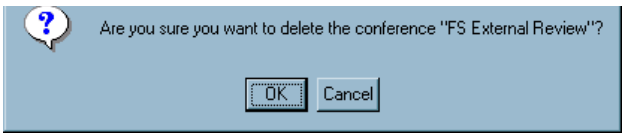
- **Pencil icon** – edit the conference (or just view all details).
- **X icon** – delete the conference (the BUI automatically updates the display).
- **Gavel icon** – jump to the "Meeting Control" window for an active conference (the icon appears only for active conferences).

The BUI can display past conferences, up to the “aging” factor that an administrator defines (see Figure 48 on page 99). When a conference reaches the aging factor, the conference is deleted from the list.

A super-user can view permanent conferences, but cannot edit or delete them. Therefore, the system does not display the Edit and Delete icons next to permanent conferences that are not accessed by an administrator.

Table 18 describes the columns in the Meeting List window.

Table 18
Meeting List window fields

Field	Description
Conference title	Shows the subject text that appears when scheduling a meeting. It can be empty.
Number of participants	Shows the number of ports reserved for this meeting.
Date	Shows the conference date. For permanent conferences, the date shows “Permanent”. For recurrent conferences, the letter “R” follows the date.
Start time	Shows the conference start time. For permanent conferences, this fields is empty.
Duration	Shows the conference duration. For permanent conferences, this fields is empty.
Dialing access	Shows the conference access number (DN).
Chairperson access	Shows the chairperson access number.
Owner	Shows the name of the person who scheduled the conference. This column appears only for super-users, because they can view all meetings. When a super-user schedules a conference and assigns another user in the “owner” field, that user becomes owner of the conference and their name appears here.
Edit	Click on the Edit icon to open a window for editing this conference. The window opens with the selected item’s parameters.
Delete	Click on the Delete icon to delete this conference. When the Delete icon is clicked, the following confirmation dialog box appears:  If the conference is active, the following additional line appears before this question: “Warning! this conference is active.”
Control	The Control icon applies to active conferences only. Click on the gavel icon to open the Meeting Control window for this conference.

To schedule a new conference, click on the **New Conference** button on the top left-hand corner of the window. A new window appears (see Figure 37).

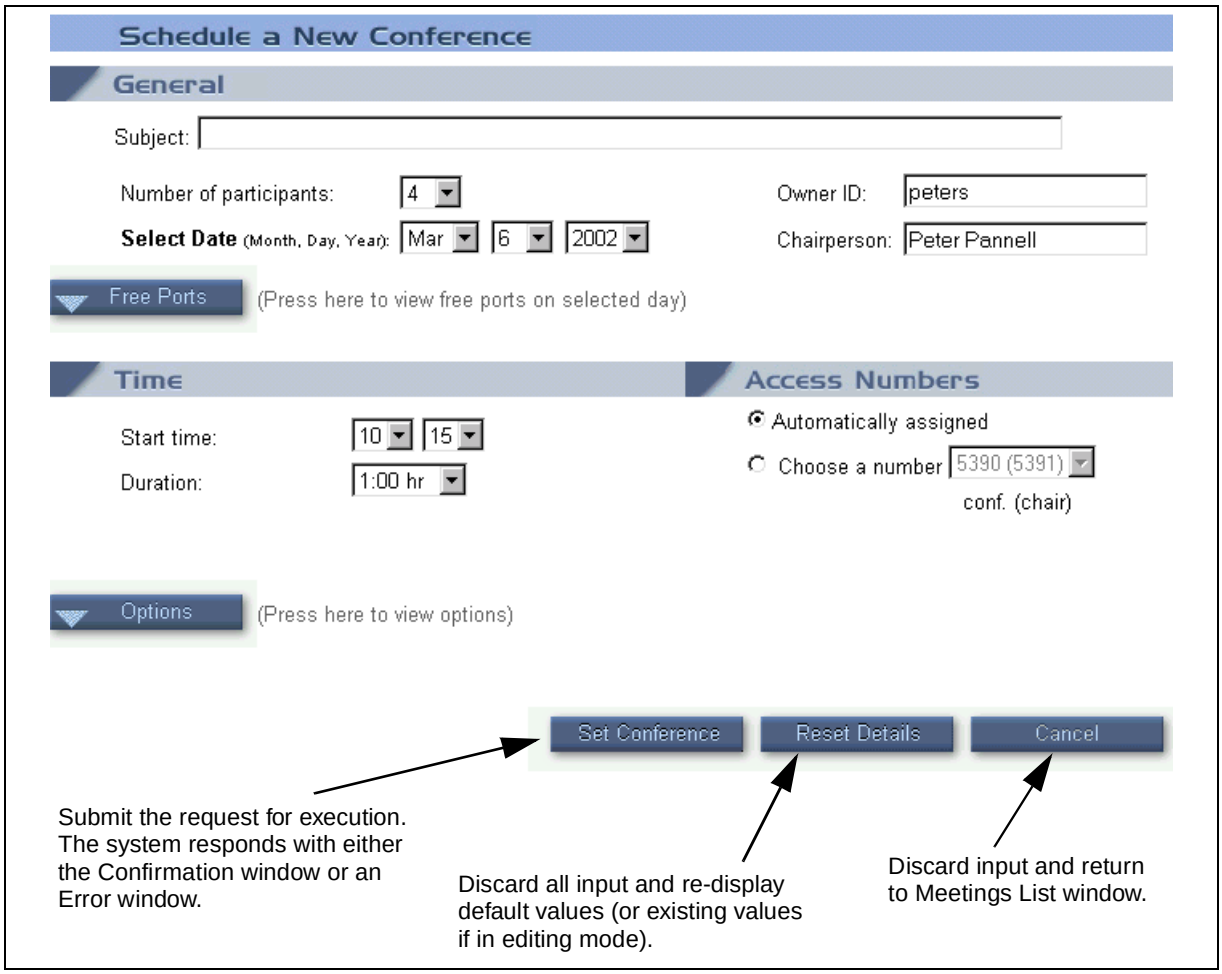
Scheduling window

Click on the **New Conference** button, or click on the edit icon (a pencil), in the row of an already scheduled conference to open the Scheduling window.

General section

Figure 37 shows the scheduling window when it first opens.

Figure 37
Scheduling window – Schedule a New Conference



All fields have defaults, but users typically select the date and time, and number of participants. The system provides defaults for the other parameters or generates the values automatically.

After scheduling a conference, view the Scheduling Confirmation window to verify the entries. See Figure 40 on page 90 for an example.

Table 19 describes the fields in the Scheduling window, by section.

Table 19
Scheduling window fields

Field	Description
General section	
Subject	Enter text that describes the purpose of the conference. *Range:* Enter up to 20 characters or leave this field empty. *Default:* Empty.
Number of participants	Enter the number of ports to reserve for this conference, including the chairperson ports. The application makes sure that the total number of reserved ports for this time period does not exceed system capacity. The system performs validation after submission. Preview port availability by opening the “Free Ports” expanded window. *Range:* 3 to 32. *Default:* 4
Dual MICB meeting link (not shown in Figure 37 on page 84)	Click here if a dual-card meeting is required. A similar window with the following dual-card meeting attributes opens: • Up to 60 or 62 ports are available, depending on the configuration parameter “full chairperson control”. • The “Access Numbers” section displays a fixed dual-card meeting DN, which cannot be changed. ***Note:*** This link appears only on the primary MICB card in a dual-card set.
Select date	Select the date the conference starts from the pull-down menus. *Range:* Current day to one year ahead of current day. *Default:* Current day. ***Note:*** This field cannot be modified when editing an existing conference.
Owner ID	Enter the user ID of the user who scheduled the conference and has permission to delete or edit it. When the BUI displays this field to a regular user, it shows that user’s ID is not editable. When the BUI displays this field to a super-user, the super-user can edit it.
Chairperson	Enter the name of the chairperson for the user’s reference. *Range:* Text up to 20 characters. *Default:* Empty.
Free Ports section – see “Free Ports section” on page 87.	

Table 19
Scheduling window fields (Continued)

Field	Description
Time section	
Start time	Enter the time that the conference starts. The minutes box shows 15-minute increments (that is, 0, 15, 30, and 45). *Range:* Hours/15-minute increments. *Default:* Current time. The default value of the time field is rounded to the nearest 15 minutes according to the following rule: • In the first 10 minutes of the interval, the system rounds the time off to the past. For example, if the time is 8:23, the box shows the time as 8:15. The system interprets this as an immediate conference. • In the last five minutes of the interval, the system rounds it to the future 15-minute value. For example, 8:26 appears as 8:30.
Duration	Enter the duration of the conference. *Range:* Up to 12 hours in 15-minute increments (the selection box shows all possible values). *Default:* 1 hour.
Access Numbers section	
DN pair usage option	Select the access DN pair to use as follows: • Automatically assigned (the default) – the MICB selects the DN pair; no user action is required. • Choose a number – select a number from the list. The list shows pairs of numbers in the format: [conference (chairperson)]. The system checks the availability of the number when the form is submitted for execution. If the numbers are not available, the scheduling fails.
Options section – see "Options section" on page 87.	

When in edit mode, the title of this window is: "Edit a Conference". The following fields cannot be modified when editing a conference:

- date
- dual-card meeting option (that is, users cannot make a single-card conference dual and vice versa)
- recurrent option

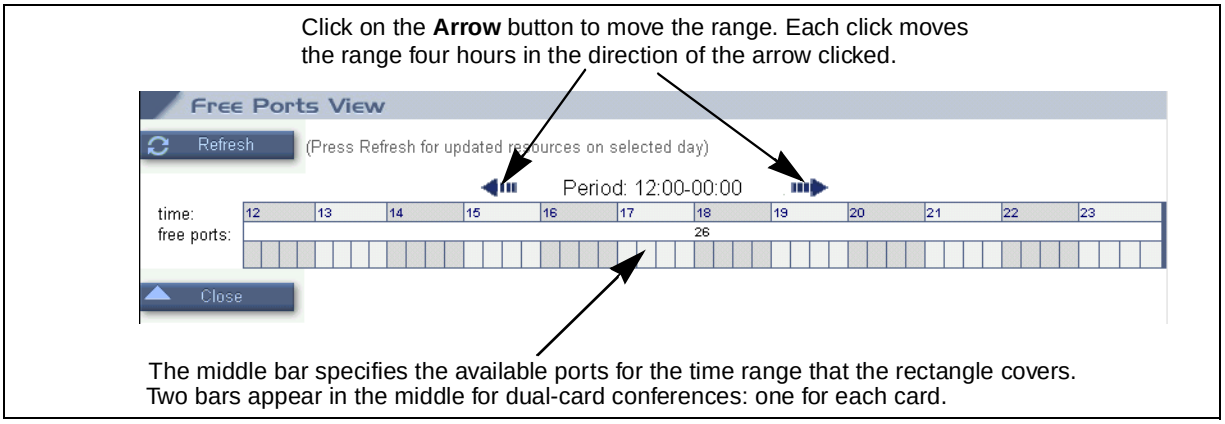
Only the following fields can be edited during an active conference:

- number of participants
- duration
- add ports as needed (under the Options section)

Free Ports section

Figure 38 shows the how the scheduling window is expanded after clicking on the **Free Ports** button. The information in this window refers to the date set above it in the Scheduling window. The time scale covers 12 hours in 15-minute increments.

Figure 38
Scheduling window – Free Ports section



Options section

Figure 39 shows how the scheduling window is expanded after clicking on the **Options** button.

Figure 39
Scheduling window – Options section

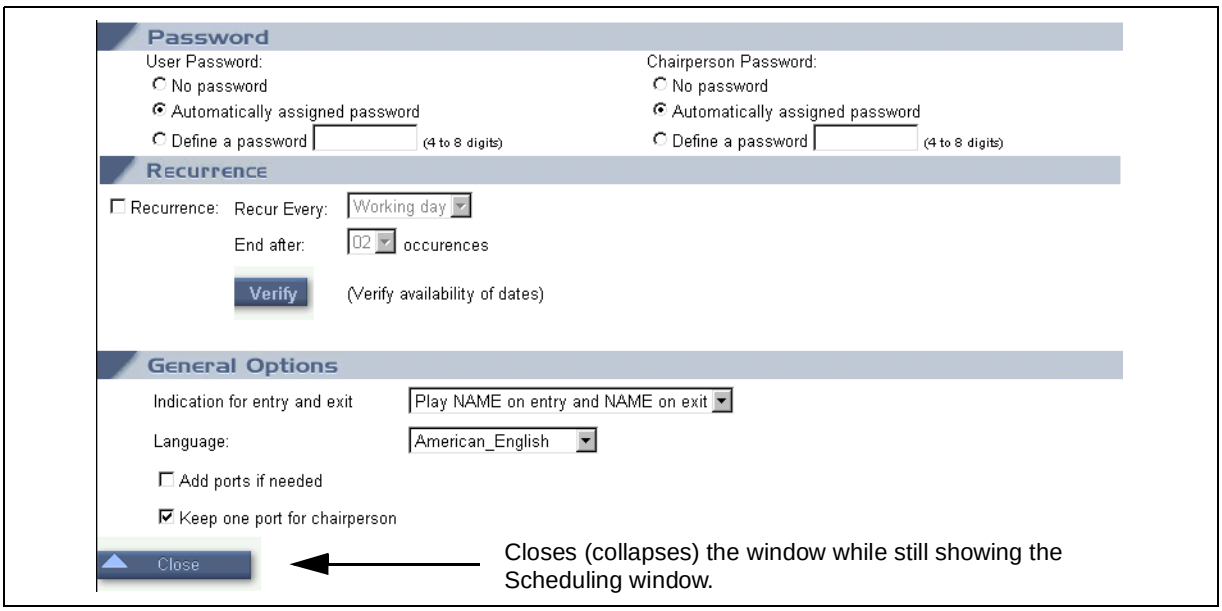


Table 20 describes the fields in the Options section.

Table 20
Scheduling window – Options section fields

Field	Description
Password section	
User Password	Enter an optional password for the conference. If configured, callers must enter this password to join the conference. Available options are as follows: • No password – no optional password. • Automatically assigned (the default) – The system automatically generates the password. The administrator sets the password length from 4 to 8 digits. • Choose a password – The user defines the password. The range is 4 to 8 digits. The window shows the password as it is entered. The system does not check the password for uniqueness. Different conferences can use the same password.
Chairperson Password	Enter a password for chairperson authentication. This field has the same options as the user password.
Recurrence section (Does not appear for dual-card conferences, because they do not support the recurrence option).	
Recurrence	Use this checkbox to activate or de-activate the recurrence feature. The adjacent criteria applies when this box is checked. ***Note:*** The recurrence option is only available when a specific DN pair in the Basic window is selected. If a DN pair is not selected, a pop-up message instructs you to select the DN pair first.
Recur Every	Enter the recurrence interval. *Available values*: Day, workday, week, two-weeks, and month. ***Note:*** If the first conference is not a workday, the workday option is not available.
End After	Define the number of conference occurrences. Up to 30 occurrences can be defined, but they cannot be more than a year in advance.
Verify button	When this button is clicked, the system verifies port availability without actually setting them up. The system displays a result page that shows if there are resources available for each occurrence (see "Recurrent Meeting Verify Result window" on page 91).
General Options section	
Indication for entry and exit	Define how the system announces when people enter or exit a conference. The following options are available from the pull-down menu: • Play name on entry and name on exit (the default). • Play name on entry and tone on exit. • Play tone on entry and tone on exit. • Silence (no indication for entry or exit).

Table 20
Scheduling window – Options section fields (Continued)

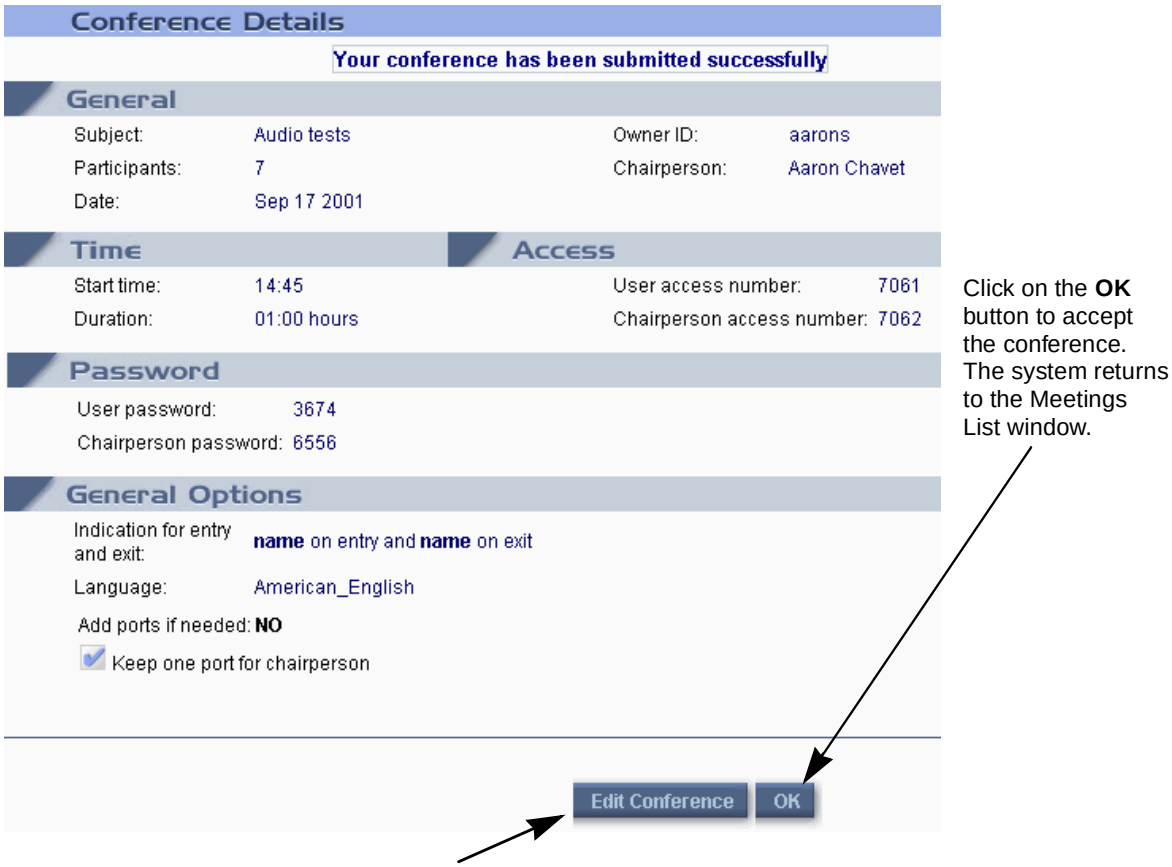
Field	Description
Language	Select the language the system uses for voice prompts during the conference. The pull-down menu offers the set of languages available in the system. The default is the MICB card's default language that an administrator selects using the Installation Wizard (see "Step 1 – Basic Card Settings" on page 67). When using single-number access, the preferred language takes affect after the caller enters the conference ID and password. Before that the system uses the default language.
Add ports if needed	When this box is checked, the system allows the meeting to expand beyond the number of reserved ports if more than the anticipated number of participants show up. The system adds ports only if there are enough ports available (that is, they are not reserved for another meeting).
Keep one port for chairperson	Click on this box to reserve a port for the chairperson. When all but one of the ports are occupied, and the chairperson has not yet dialed in, the remaining port is not available for a participant. If this box is not checked, the system uses the ports on a first-come, first-serve basis. In this case, if all the ports are taken up by participants, the system does not allow the chairperson to enter the conference. *Default:* the option is checked (on).

Scheduling Confirmation

Figure 40 on page 90 shows the window that appears after successfully scheduling a new, or modifying an existing, meeting. The system displays the window after it stores the conference in the database.

The BUI displays the conference details and selected options in the same layout as the Scheduling window.

Figure 40
Scheduling Confirmation window

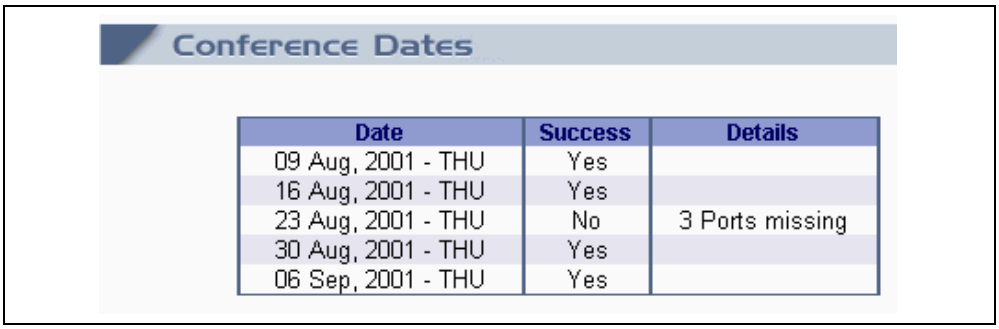


Click on the **OK** button to accept the conference. The system returns to the Meetings List window.

Click on the **Edit Conference** button to modify the conference. The system returns to the Scheduling window with the conference's details displayed.

In the case of a recurrent meeting, a Conference Dates section appears at the bottom of this window. The Conference Dates section lists the dates in which the conference is scheduled, including the first date specified in the meeting details (see Figure 41).

Figure 41
Recurrent Dates Confirmation window



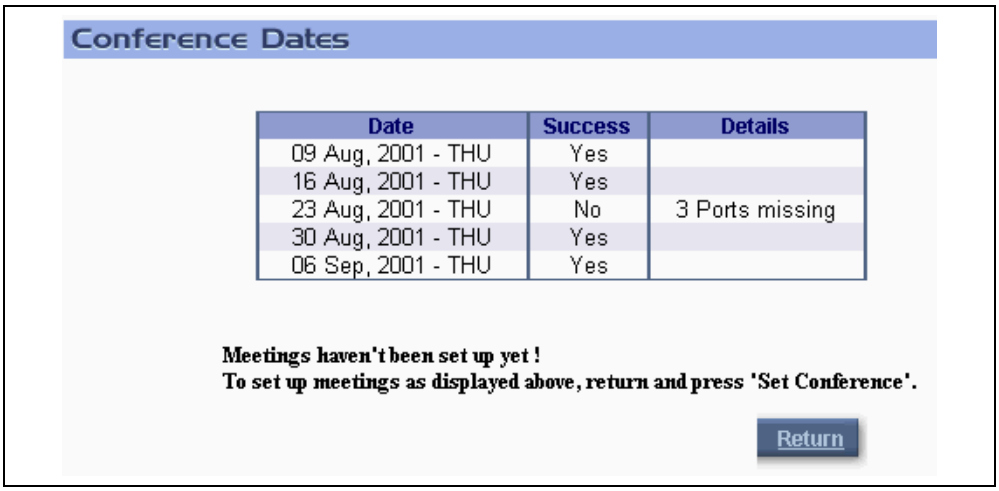
Date	Success	Details
09 Aug, 2001 - THU	Yes	
16 Aug, 2001 - THU	Yes	
23 Aug, 2001 - THU	No	3 Ports missing
30 Aug, 2001 - THU	Yes	
06 Sep, 2001 - THU	Yes	

In the previous example, the system denied one date, because the ports were not available.

Recurrent Meeting Verify Result window

Figure 42 shows the window that the system displays when the **Verify** button is clicked when setting up a recurrent conference.

Figure 42
Recurrent Conference Verify Result window



The window displays the success result for each date specified in the recurrence criteria. In the case of a failure, the system indicates the reason (for example, not enough ports or DN is already in use).

> ***Note:*** Editing the details of a recurrent conference only changes the conference for the selected day. All other occurrences of the recurrent conference are not changed.

Chairperson operations

Meeting Control window

The Meeting Control window is available to the chairperson only. The chairperson can access it in the following ways:

- From the LOGIN window, enter the chairperson access number and chairperson password of the active meeting.
- From the Meetings List window, in the Control column click on the gavel icon next to an active meeting in the list.

A window opens showing details of the specific meeting. Users cannot select another conference to control when this window is open.

The BUI allows only one active window per meeting. The associated voice port is the one identified as chairperson by access number. Figure 43 shows the window when a chairperson is on the call. There is a different window when there is no chairperson present (see Figure 45 on page 95).

Figure 43
Meeting Control window – Active chairperson

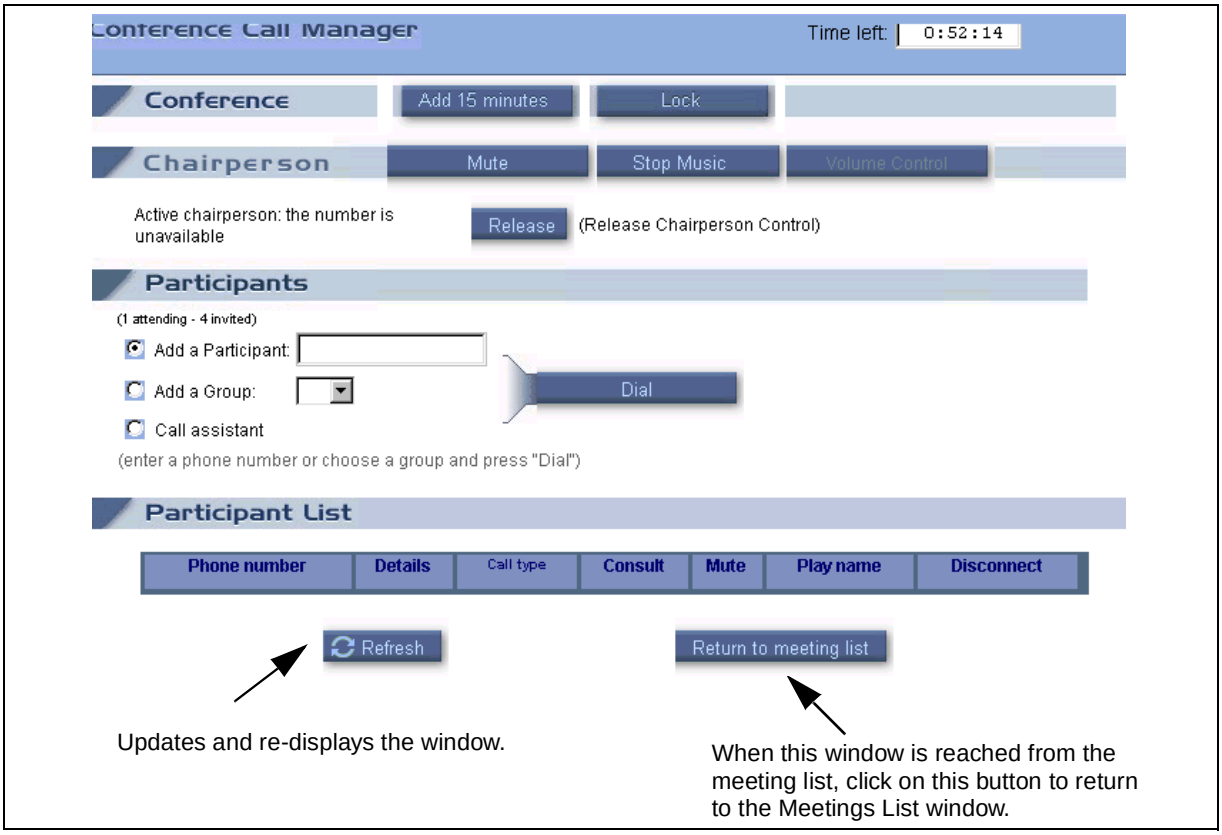


Table 21 describes the options available in the Meeting Control window.

Table 21
Meeting Control window fields

Field	Description
Conference section	
Add 15 minutes button	Click on this button to add 15 minutes to the conference duration. The chairperson can invoke this command any time during the meeting. If successful, the system updates the “Time Left” indication.
Lock/Unlock button	Click on this button to toggle from being locked to unlocked (or vice versa).

Table 21
Meeting Control window fields (Continued)

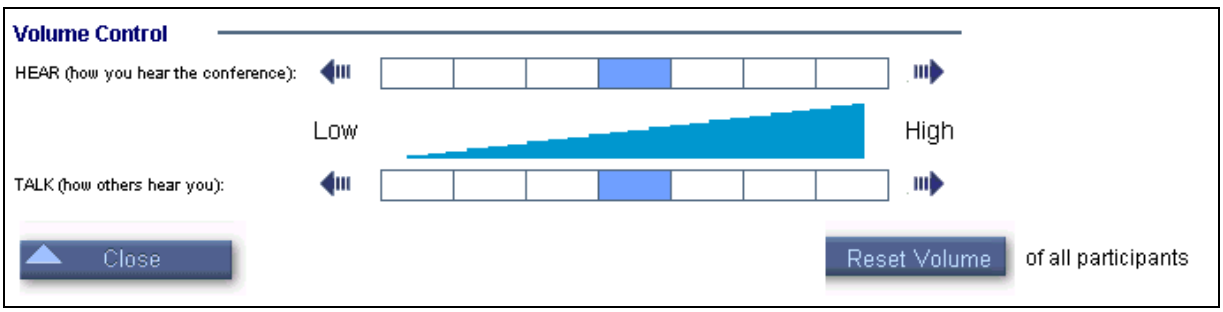
Field	Description
Chairperson section	
Active chairperson	If the chairperson joins the conference by dialing in, this field shows the CLID of the call, if available. If not available, the window displays “number not available”. If the chairperson joins the call by outdialing, this field shows the called number. This is part of the Acquire Chairperson Control feature.
Mute/Unmute button	Click on this button to toggle between muting and unmuting the chairperson’s voice port only. When muted, this button appears as “Unmute”.
Stop Music button	Click on this button to toggle between stopping and resuming music when alone in the meeting. When stopped, this button appears as “Resume Music”.
Volume Control button	Click on this button to open a volume control panel (see Figure 44 on page 94). Use this panel to increase or decrease the volume in hear and talk directions.
Participants section	
Count & announce button	Click on this button to announce to the conference the total number of participants, followed by participants’ names as recorded in the name entry.
Mute all button	Click on this button to mute all participants, except the chairperson. When muted, the button becomes “Unmute all”.
Disconnect all button	Click on this button to disconnect all participants, except the chairperson. When clicked, the BUI opens a dialog box (OK/CANCEL) to confirm this operation.
Dial-out control	**1** Provides a radio button list to select the following type of dial-out: Add participant; Add a group (that is, Group Call); Assistant call. **2** The Dial button starts call origination. After call origination, the system connects the chairperson to a private call with the called party. The window changes to two buttons relevant to this state: “Return with called party”; “Return without called party.” In addition, the following chairperson call-related buttons are disabled: Self Mute; Stop Music; Volume Control; Count & Announce, and Mute All.
Participant’s List section (Shows a table of details and chairperson controls for each participant, excluding the chairperson.)	
Phone number	CLID or called number.
Details	The chairperson can enter text in this field for personal reference (for example, the participant’s name).

Table 21
Meeting Control window fields (Continued)

Field	Description
Status	Shows regular, dial-out, or expand.
Consult/End consultation button	Click on this button to invoke a private call with the participant. When in a private call, an icon appears indicating this status. During a consultation, an icon appears beside “End consultation”.
Mute/Unmute button	Mute or unmute an individual participant. When muted, an icon appears beside Unmute.
Play name	Click on the icon to play the participant’s name as recorded by the name entry feature. The system plays the name on the chairperson’s desktop, not their telephone.
Disconnect	Click this icon to disconnect the participant. Before disconnecting, the system displays a dialog box. The window shows: “Disconnect this participant?” with **OK** and **Cancel** buttons to click on.

The system updates the window automatically every two minutes.

Figure 44
Volume Control Panel

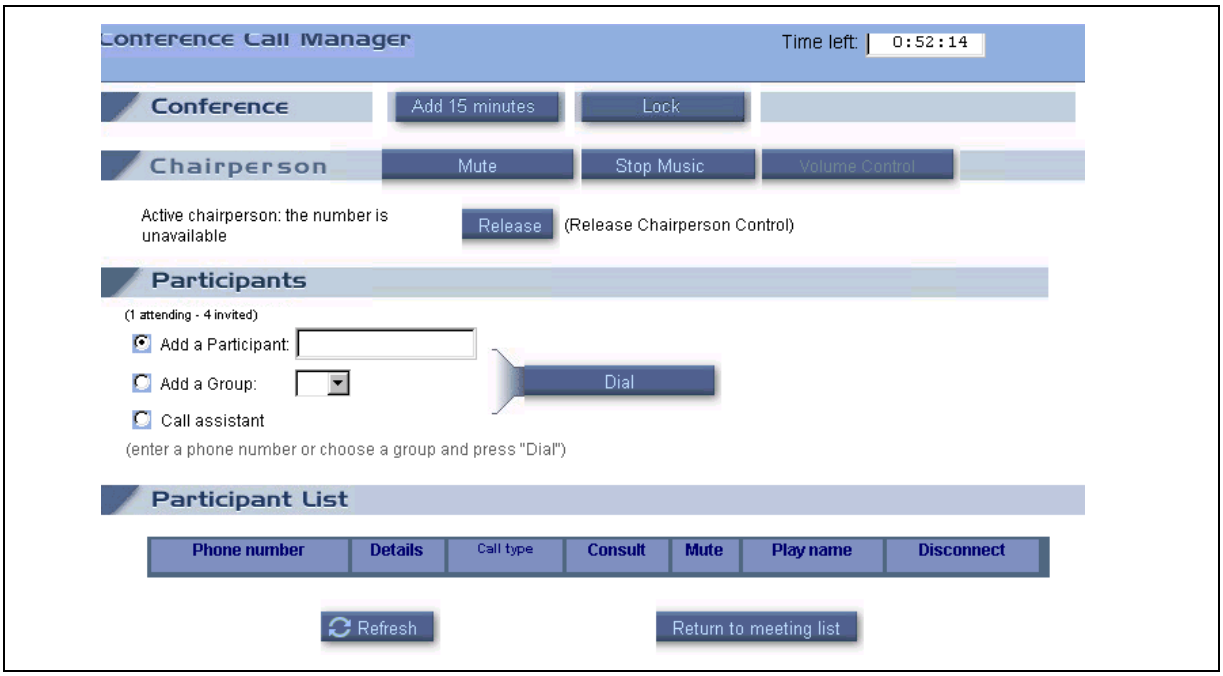


The two scales in the middle of this window show the current increase/decrease level for hear and talk directions. The middle of the scale is zero, which signifies no volume change. Click on one of the arrows to increase or decrease the volume. The colored rectangle in the scale advances one step for each arrow click.

Click on the **Reset Volume of all participants** button to restore the initial volume level of all participants.

When no chairperson is present in the conference, the system disables call-related buttons (see Figure 45 on page 95).

Figure 45
Meeting Control window – Chairperson not present



The following features are unavailable in this mode:

- Self mute/unmute
- Stop/play music
- Volume control
- Dial out
- Consult with participant

After the chairperson joins the conference the window changes to the one that Figure 43 on page 92 shows.

Dual-card meeting

Commands that a chairperson operates from the BUI in a dual-card meeting apply to participants in both cards. The feature operates as follows in a dual-card conference:

- **Dial-out to a specified number** – dial-out works only with the “full chairperson control” configuration option. If limited control is selected, these commands work on the primary card only.
- **Consult with participant** – consultation works only with the “full chairperson control” configuration option. If limited control is selected, these commands work on the primary card only.
- **Play name** – this feature works with participants on both cards. The system plays the name on the chairperson’s desktop, not the telephone.

Release chairperson control

The Meeting Control window contains a button to release chairperson control. This button releases both TUI and BUI control. Clicking the button allows someone else to acquire chairperson control and enter the BUI control window of the meeting.

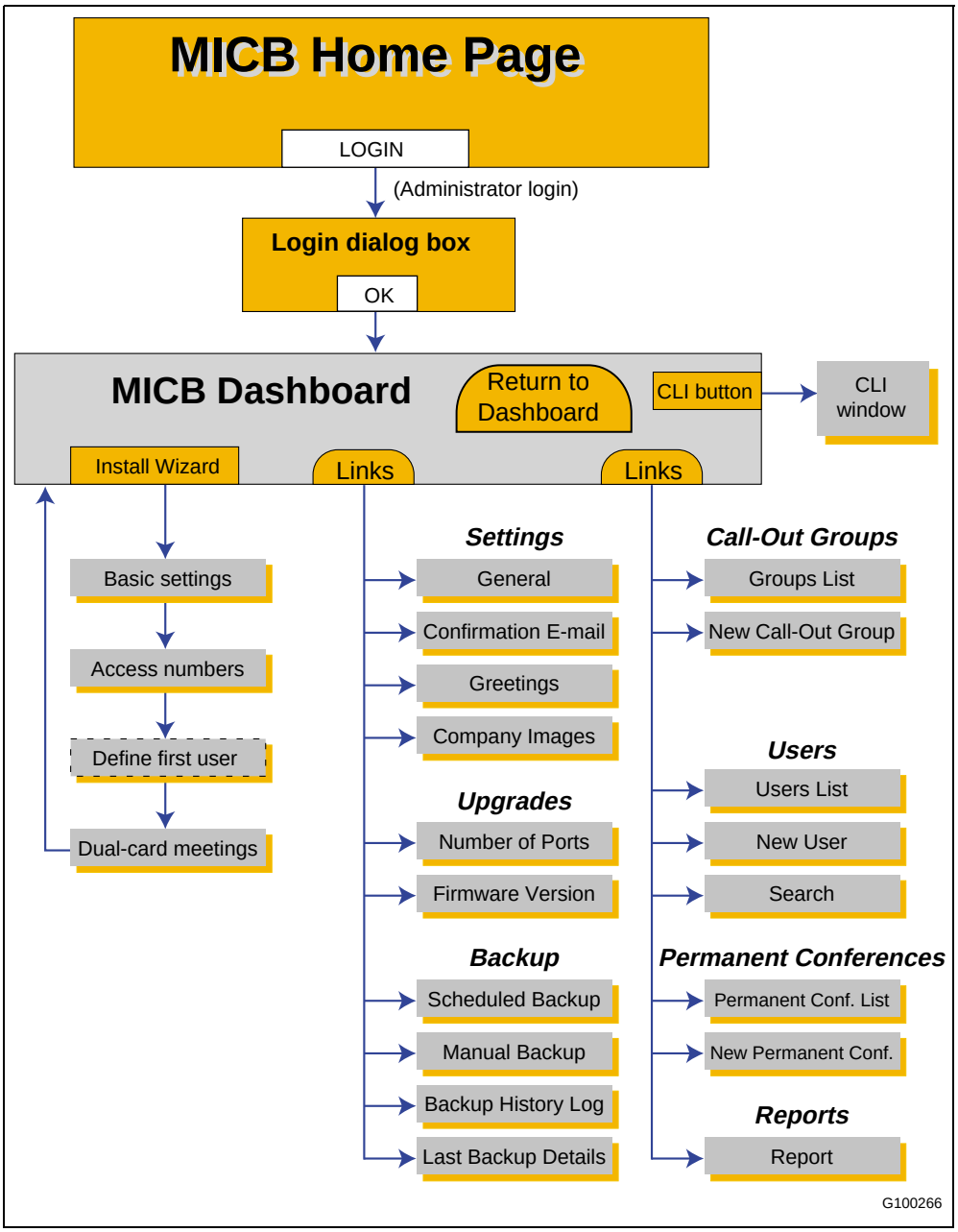
Administration BUI

Introduction

This section applies to administrators only. The main administration window is the MICB Dashboard, which appears directly after an administrator logs in. The dashboard provides access to the relevant window to perform the required task (see Figure 46 on page 97).

A special function is the Installation Wizard, which guides an administrator through a quick and easy process for configuring a new card. For more information about the Install Wizard, see “MICB Installation Wizard” on page 67.

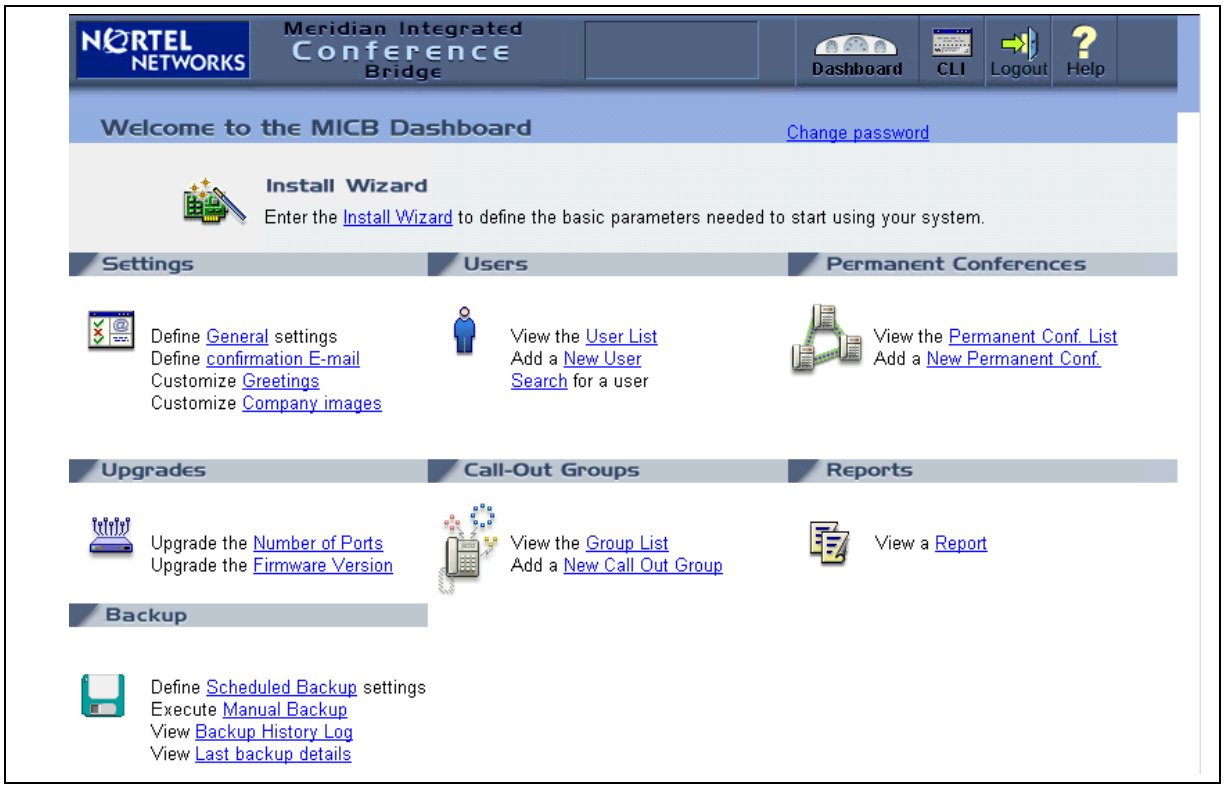
Figure 46
Administration BUI navigation flowchart



MICB Dashboard

The MICB organizes the Dashboard as an internet portal. The Dashboard groups links by subject (see Figure 47)

Figure 47
Administration BUI MICB Dashboard window



The title frame on top, which is present for all administration windows, contains the following buttons:

- **Dashboard** – click here to return to the dashboard, while discarding the input in the current window.
- **CLI** – opens an additional window for input and output of CLI commands (from more information, see "CLI command summary" on page 147).

From the Dashboard, the "Change Password" link opens the Change Password window shown in "Login password change" on page 78. Access the Change Password window from the Dashboard to change the current administrator password.

The MICB Dashboard has the following sections:

- MICB Installation Wizard
- Settings
- Users
- Permanent Conferences
- Upgrades
- Call-out Groups
- Reports
- Backup

Settings

This subject groups several parameters and definitions. Links to sub-subjects appear on the Dashboard.

General Settings window

Figure 48 shows the General Settings window

Figure 48
MICB Dashboard – General Settings window

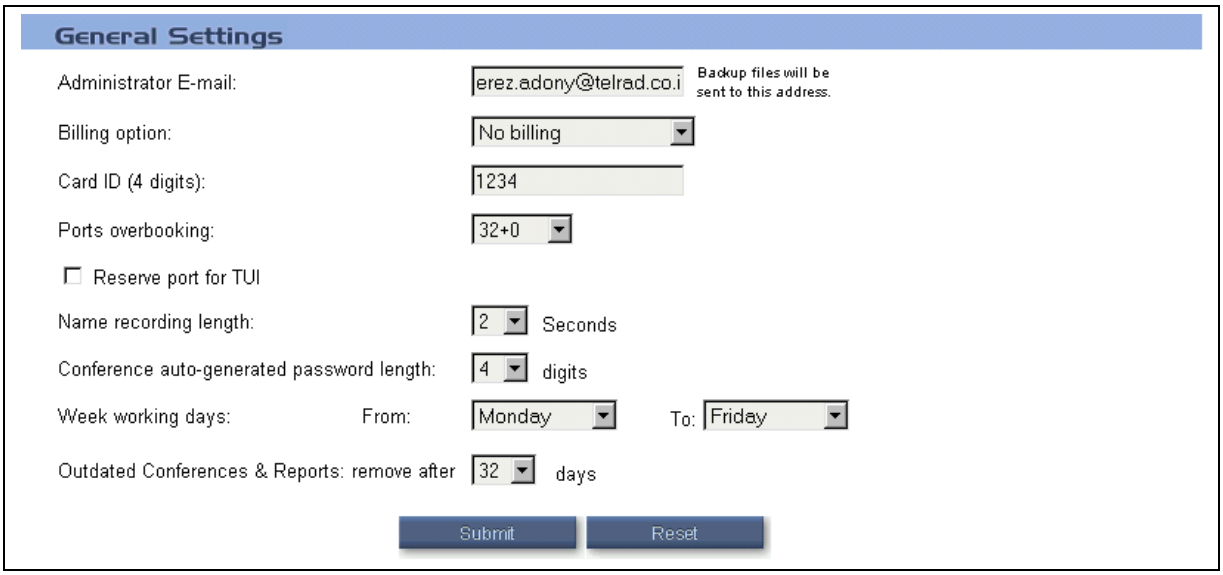


Table 22 on page 100 describes the options available in the General Settings window.

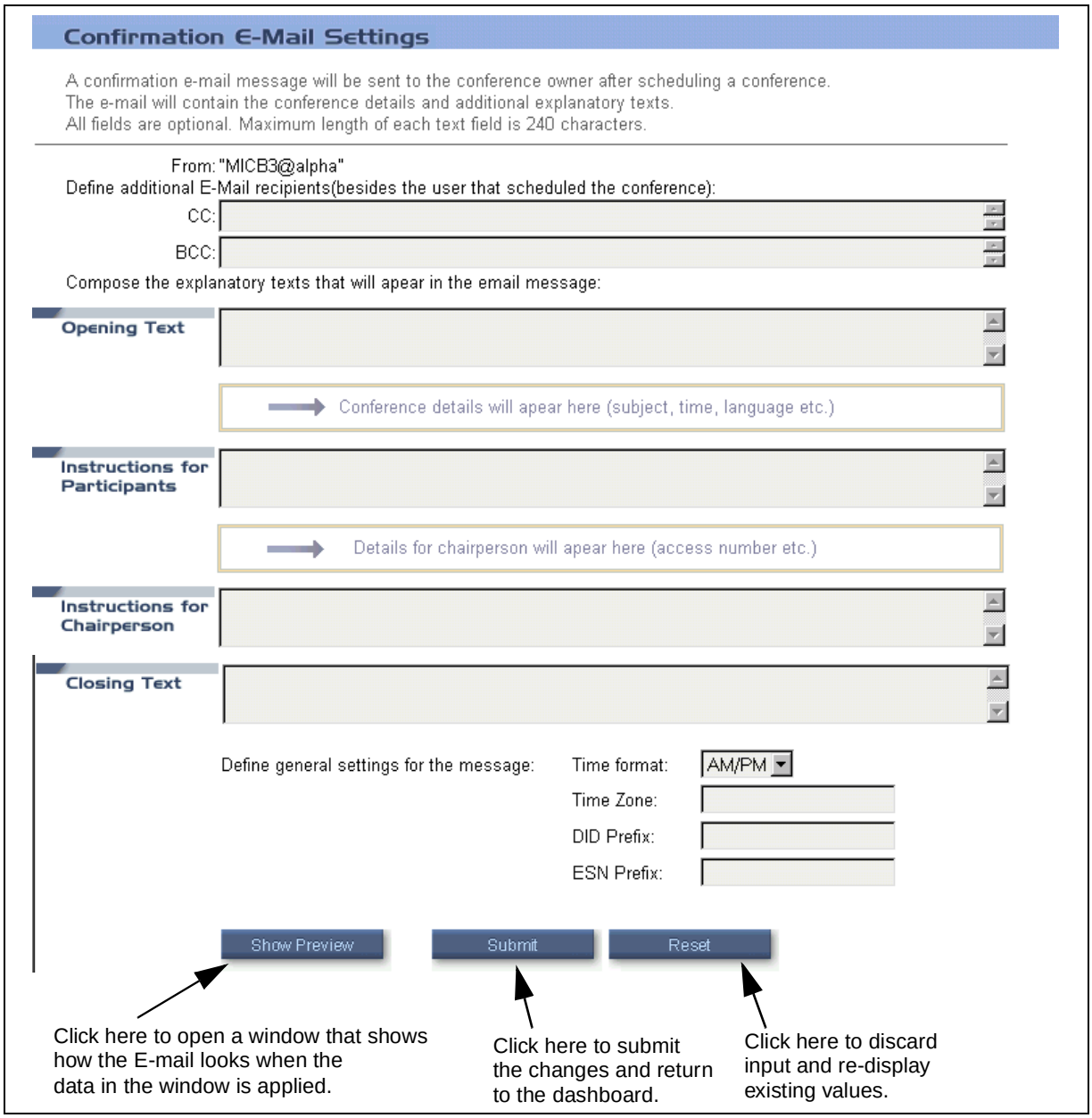
Table 22
General Settings window fields

Field	Description
Administration E-mail	Enter the E-mail address to which the MICB sends administration material, including backup files.
Billing option	Select a billing option for this card from the pull-down menu. The options are as follows: • **No billing** – The MICB does not issue a billing report. • **Billing reports** – The MICB issues a billing report (see "Billing Report" on page 168). • **Billing reports & CDR** – The MICB issues a billing report and a CDR record (see "Meridian 1 Call Detail Recording" on page 173). ***Note:*** The Billing reports & CDR record option is not available on the Meridian SL-100.
Card ID (4 digits)	Enter the card ID that the system uses for billing purposes. *Range:* A four-digit decimal.
Ports overbooking	Enter the number of ports the Overbooking feature adds. The available values are shown in the form of 32 + N, where 32 is the physical capacity and N is the addition for overbooking. *Range:* From 32 + 0 (no overbooking) to 32 + 8 for cards with 32 ports. In cards with less than 32 ports, the maximum N is the proportional fraction of 8 (for example, 16 + 4 for a card with 16 ports). *Default:* N = 0 (no overbooking).
Reserve port for TUI	Click in the box to dedicate one of the card's port for TUI access, which is not available for meetings. When this box is not checked, the system does not reserve a port for the TUI; when all ports on the MICB are busy the TUI is inaccessible.
Name recording length	Enter the duration, in seconds, of the spoken name in the name-entry option. When the system prompts the callers for their name, recording after the beep takes place for the specified duration. *Range:* 2-10 seconds. *Default:* 2 seconds.
Conference auto-generated password length	Enter the number of digits for the conference or chairperson password, when a user selects the password to be automatically generated by the MICB.
Week working days	Select the range of working days from the pull-down menu. The MICB uses this information when creating recurrent conferences with the option "Workday". *Range:* Any day of the week. *Default:* Monday to Friday.
Outdated Conferences & Reports: remove after	From the pull-down menu, select the number of days these files are kept before the system deletes them (also referred to as the "aging factor"). For scheduling data, this field applies to conferences that have already taken place. The system keeps future conferences as long as required.

E-mail template

Figure 49 shows the window in which an administrator can customize the scheduling confirmation E-mail.

Figure 49
MICB Dashboard – Confirmation E-mail Settings



The window shows the layout of the E-mail. The customizable text fields are editable. Additional parameters to define appear at the bottom of the window.

Table 23 describes the options available in the Confirmation E-mail Settings window.

Table 23
Confirmation E-mail Settings fields

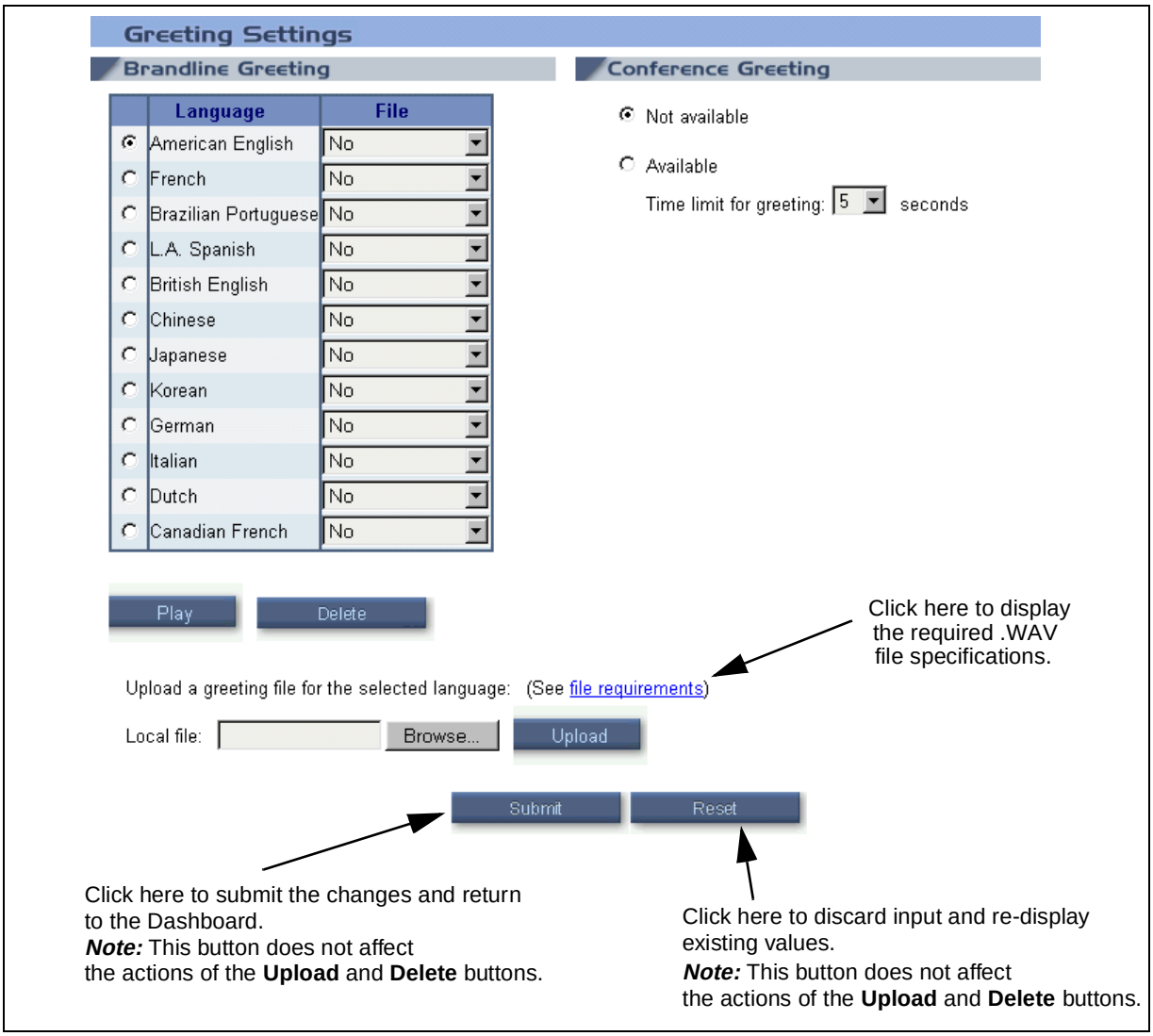
Field	Description
From	The sender's address defined in the first step of the Install Wizard. This field is view only.
CC:	Enter the E-mail address, or list of addresses, which will receive a carbon copy (CC) of all confirmation E-mails that the MICB sends. Separate the addresses by a space.
BCC:	Enter the E-mail address, or list of addresses, which will receive a blank carbon copy (BCC) of all confirmation E-mails that the MICB sends. The system hides these addresses; they do not appear on the E-mails.
Opening text	Enter the header that appears before the fixed part of the E-mail (that is, the meeting details). *Example:* company name or slogan.
Instructions for Participants	Enter the information that appears after the meeting details. *Example:* dialing instructions and list of TUI commands.
Instructions for Chairperson	Enter information for the chairperson in this field. *Example:* chairperson TUI commands and other tips for the chairperson.
Closing text	Enter the information that appears as a footer at the bottom of the E-mail body.
Time format	From the pull-down menu, select the time format that the E-mail uses (that is, 24-hour or AM/PM).
Time Zone	Enter the time zone of the MICB in free text. The MICB does not check the syntax. *Example:* GMT-5 (EST), Eastern Standard Time, or New York (GMT-5).
DID Prefix	Enter the DID prefix that callers use to access the card from the public network. Enter this value as free text. *Example:* (613) 961.
ESN Prefix	Enter the prefix that callers use when accessing the card by Electronic Switched Network (ESN). Example: 846.

Customize greetings

Figure 50 on page 103 shows the window used to customize the following greetings:

- Brandline greeting
- Per-conference user's greeting

Figure 50
MICB Dashboard – Greeting Settings window



The table in this window lists the available languages. For each language, the factory-made greetings can be replaced with a customized greeting in the form of a .WAV file.

Brandline greeting

Follow the steps in Procedure 17 on page 104 to replace the brandline greeting for a given language.

Procedure 17
Replace the brandline greeting

1. Upload the .WAV file from your computer to the MICB using your computer's operating system.
   a. Click on the **Browse** button.

      A Choose dialog box opens on your computer.

   b. Scroll through the dialog box to select the location of the .WAV file and click on the **Open** button.

      The system closes this dialog box and the selected file's name appears in the read-only Local file: text box.

   c. Click on the **Upload** button.

      The MICB loads the file into the card and adds the file name to the combo-box next to the selected language.

      Note: The upload action is immediate. There is no need to submit and save it. It cannot be cancelled by clicking on the **Reset** button.
2. Click on the radio button next to the language in the table to select the language.
3. Select the desired .WAV file you uploaded in the File column for that language.
4. Click on the **Submit** button to save the change.

This procedure is now complete

There are two additional action buttons as follows:

- **Play** – Click on this button to play the selected greeting. The system plays the file of the selected language on your computer.
- **Delete** – Click on this button to delete the selected greeting from the card. The system removes the file's name from the combo-box. Before deleting the file, the BUI opens a dialog box that asks: "Are you sure you want to delete greeting file xxxx.WAV?"

  After the system deletes the file, it removes the file from the combo-box that contained it. The selection returns to the "factory default" greeting.

  Note: The delete action is immediate. There is no need to submit and save it. It cannot be cancelled by clicking on the **Reset** button.

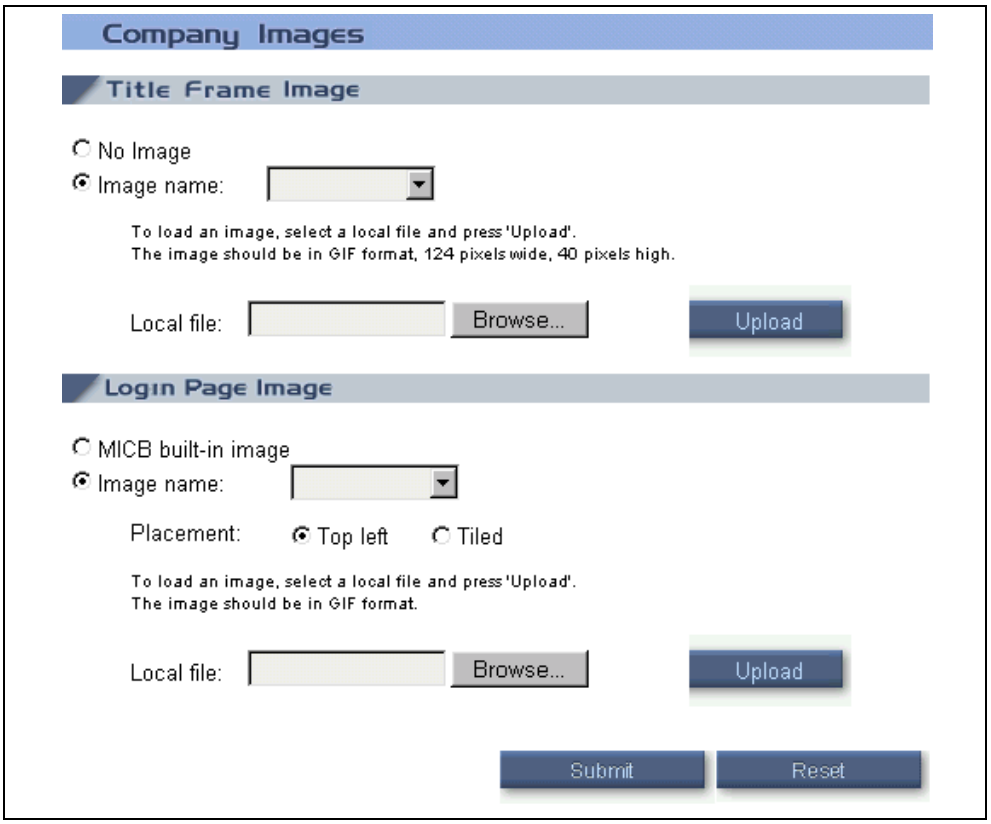
Conference-specific greeting

Use these fields in the Greeting Settings window to enable or disable the Conference-specific Greeting feature. Click on the **Available** radio button to enable the conference-specific greeting. When selected, the administrator can define the maximum length of the greeting. The range is from two to 10 seconds; the default is five seconds.

Company images upload

Figure 51 shows the window that an administrator can use to customize the MICB home page image and the customer's logo on the title frame. Images must be in GIF format.

Figure 51
MICB Dashboard – Company Images window



Title Frame Image

"No image" is the default. Follow the steps in Procedure 18 on page 106 to use a customized image.

Procedure 18
Use a customized image

1 Click on the **Browse** button.

A choose local file dialog box provided by your computer's operating system opens. This window allows an administrator to select a file in their computer.

2 Navigate to the folder that contains the file to upload, select the file and click on the **Open** button.

The system closes the dialog box and the selected file's name appears in the read-only Local file: text box.

3 Click on the **Upload** button.

*The system uploads the file into the MICB card and the file name appears in the box adjacent to the **Image name:** radio button.*

4 To activate the image, click on the **Submit** button.

The new image becomes the customer logo and the system discards the previous image.

Note: If the **Reset** button is clicked, instead of the **Submit** button, the system discards the image.

This procedure is now complete

The maximum image size is 124 pixels wide by 40 pixels high. The system does not allows a larger image, as this distorts the frame. If a customer image is not supplied, the customer's logo on the home page remains an empty rectangle.

Note: The MICB does not check the image size; the administrator is responsible for verifying the correct size.

Login Page Image

Upload this image in the same way as in Procedure 18. The image should fit reasonably in a browser window. For example, the MICB default image is 690 pixels wide by 420 pixels high. The system accepts a smaller image.

The additional placement parameter allows the image to be placed on the login window as follows:

- **Top left**– the system places the image on the top-left corner of the window and leaves the background empty (that is, the browser's background color). This is the default.
- **Tiled** – the system duplicates the image as many times as needed to cover the window's space.

Upgrades

See "Upgrade procedures" on page 180 for more information about how to use the Dashboard to perform card and firmware upgrades.

Users

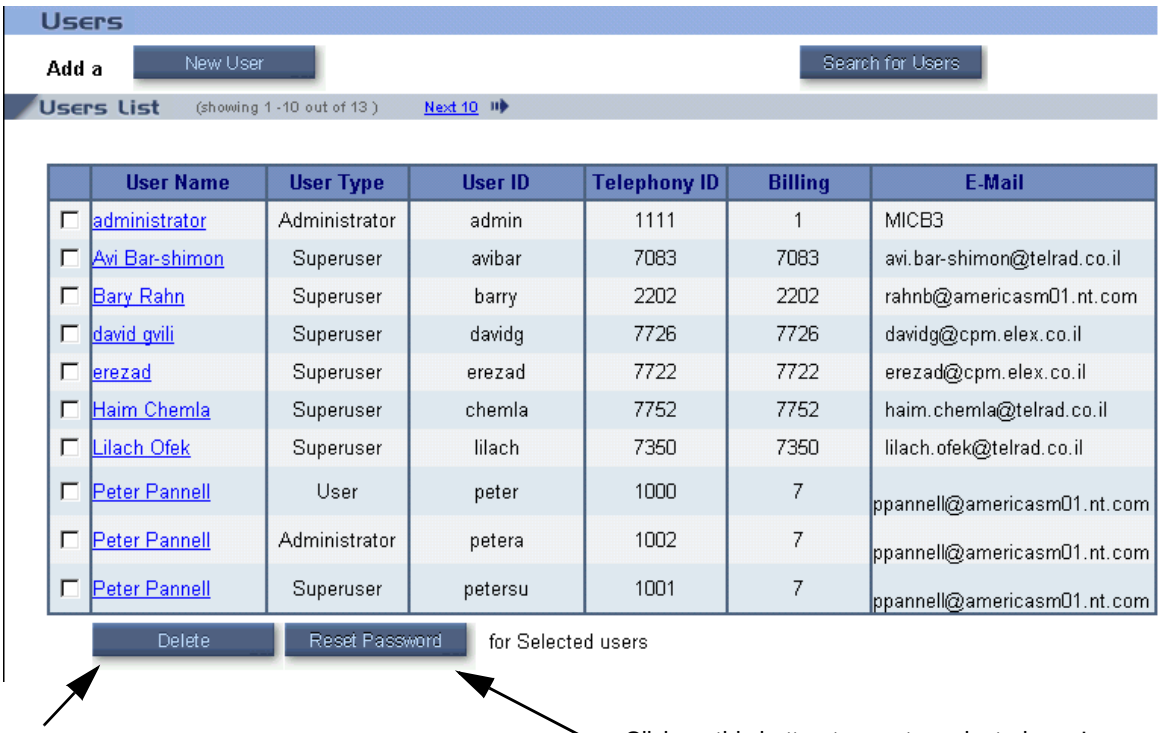
This section enables an administrator to go directly to the following windows:

- Users List
- New User
- Search

Users List

Figure 52 shows the User List window which is the main window for users administration.

Figure 52
MICB Dashboard – User List window



Click on this button to delete selected users. Before deleting, the system displays the following dialog box, for example: "Are you sure you want to delete these four users?"

Click on this button to reset a selected user's password back to the initial password (that is, six zeros - 000000). Use this button if users forget their password.

The buttons on top of the window are for additional administrator actions; the sections that follow describe these actions.

The window displays a list of users in the form of a table that the systems sorts alphabetically by name. The table shows 10 users, with each user in a separate row. Click on the “Next 10” or “Previous 10” links to view additional users. Find a specific user by clicking on the **Search for Users** button (see “Search for a user” on page 110).

Table 24 describes the columns in the Users List table.

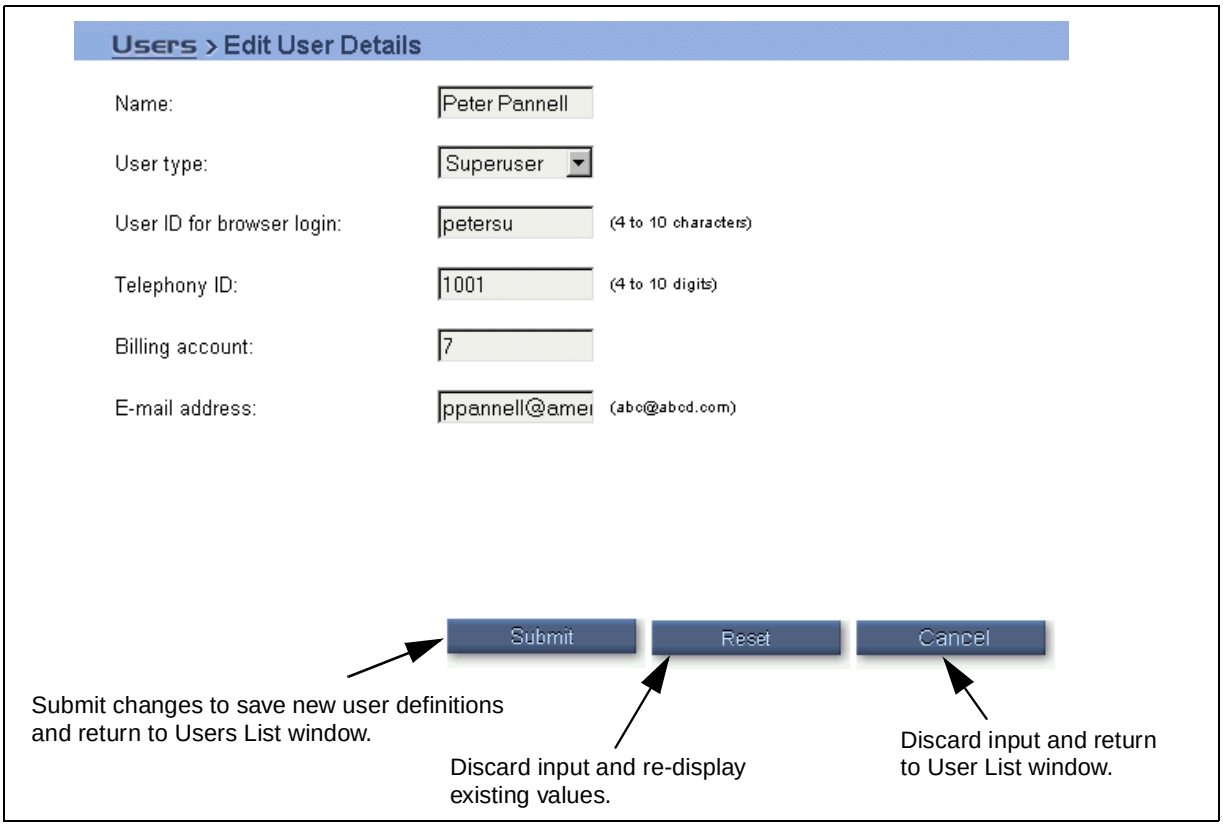
Table 24
User List table columns

Column	Description
User name	Free text up to 20 characters. The BUI treats the whole name as one string; there is no distinction of first and last name. The name is a link. Click on the name to open the Edit User window for this user.
User type	The user type: user; super-user, or administrator.
User ID	The login ID for the BUI, up to 10 characters.
Telephony ID	The TUI Login ID, up to 10 digits.
Billing	An account number for the user, which the system uses for billing purposes. This number appears in billing reports. The field can be empty, if the billing feature is not being used.
E-mail	The user’s E-mail address for receiving scheduling confirmation by E-mail. It can be empty, in which case the user does not receive scheduling confirmation E-mails.
Checkboxes	Click on a checkbox to select the corresponding user. The buttons below the table perform actions on selected users.

Edit a user

When an administrator clicks on a name in the Users List window, the Edit User Details window opens (see Figure 53 on page 109). Use the Edit User Details window to modify the properties of an existing user. The window shows all the properties of the selected user. The properties in this window can be modified. The fields are the same as those in Table 24.

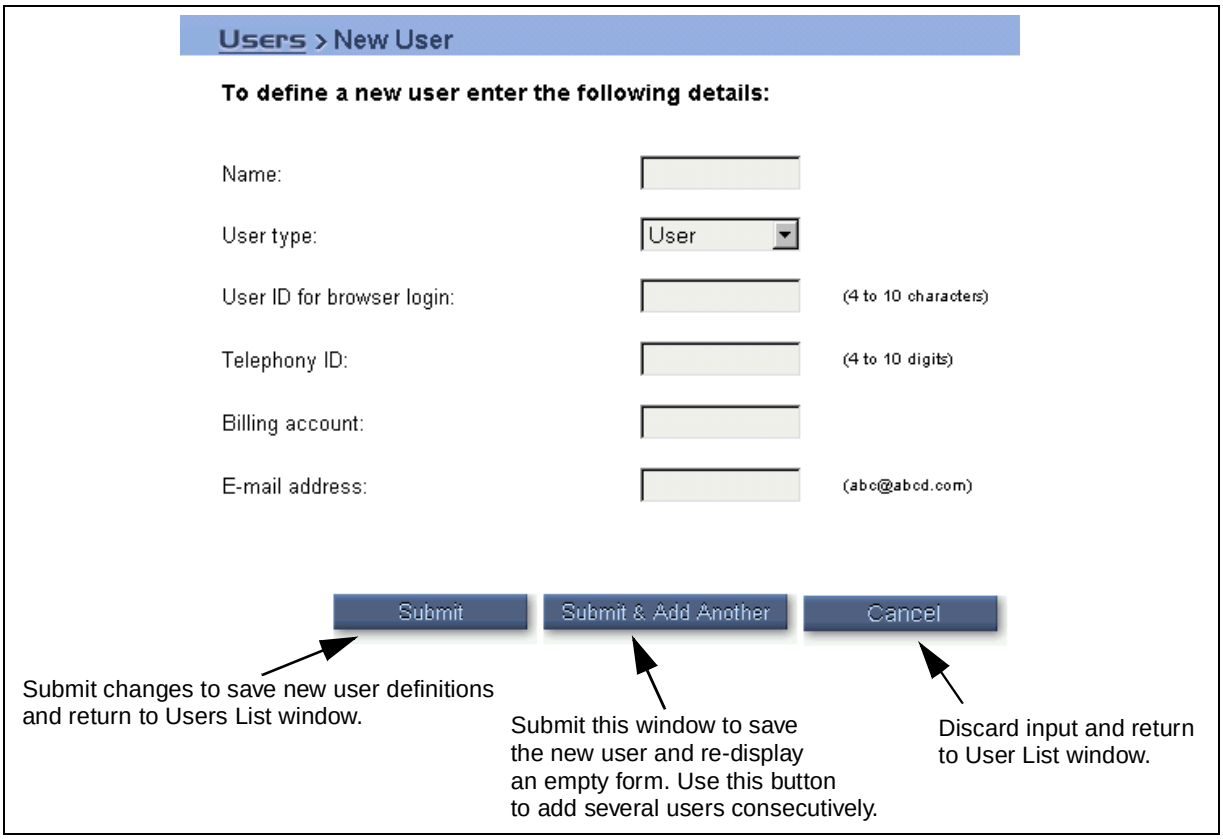
Figure 53
MICB Dashboard – Users > Edit User Details window



Add new user

Click on the **New User** button in the User List window to access the New User window. Use the New User window to add new users (see Figure 54 on page 110).

Figure 54
MICB Dashboard – Users > New User window

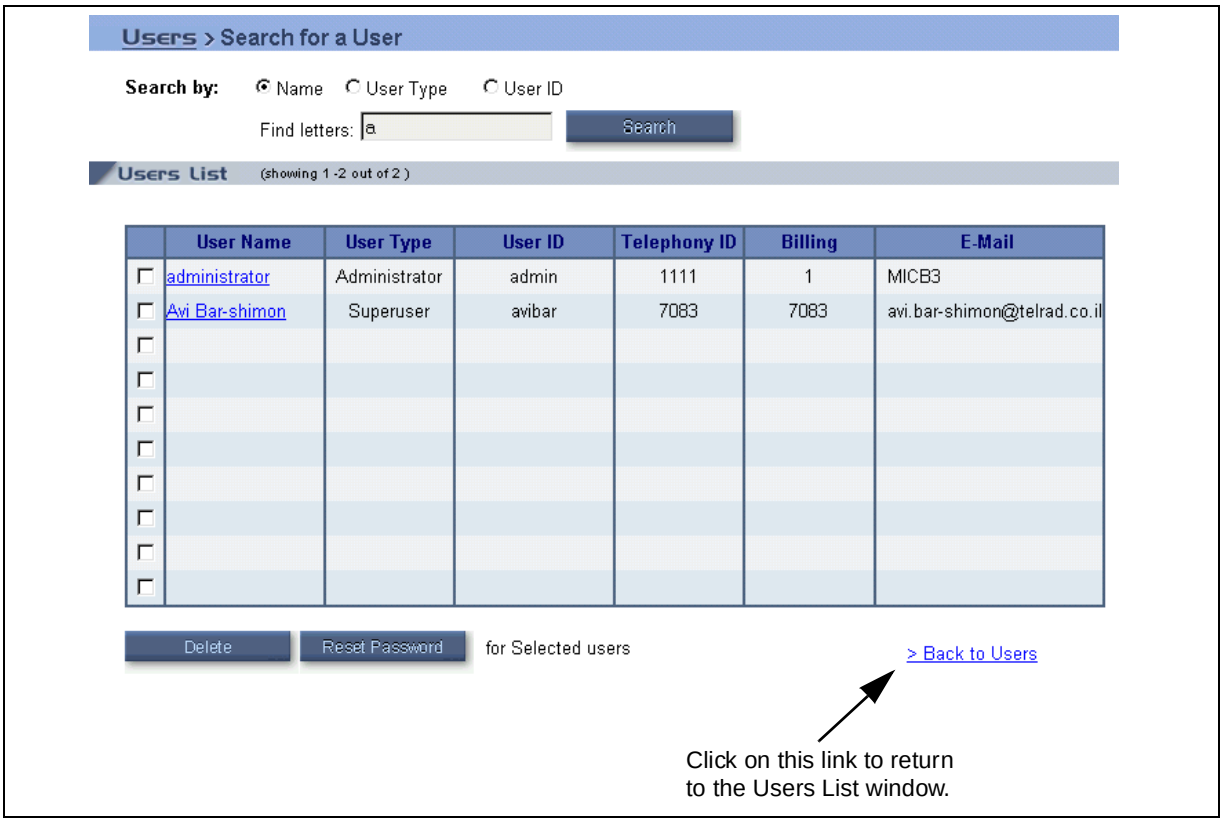


Note: The password for a new user is initially 000000 (that is, six zeros). Nortel Networks recommends that the user change it during the first login session.

Search for a user

When the Search for User **button** in the Users List window is clicked, the Search for a User window opens. Use the Search for a User window to view a subset of users depending on the criteria entered (see Figure 55 on page 111).

Figure 55
MICB Dashboard – Users > Search for a User window



Click on one of the **Search by:** radio buttons to specify the field to search.The following options are available:

- Name (the system treats the whole name as one string and makes no distinction between first and last name)
- User Type
- User ID

The system searches the string depending on the entry in the Find letters: field. All values that begin with this string match the criterion. The search is not case-sensitive. In the above example, the field to search is by name and the letters to find are “a”. The system displays all names that begin with “a” in a table similar to that in the User List table (see Table 24 on page 108).

Import users

Use the **Import User** button in the User List window to import the user list from the mate MICB card in a dual-card pair. This button only appears in a primary or secondary MICB card; it does not appear in stand-alone MICB configurations. Use this window to define the same users on both cards, instead of re-entering all user data a second time. The user list can be imported after entering it on the first card.

Before importing, the Dual Meeting parameters must be defined (see "Step 4 – Dual Card Meetings" on page 71). If the second card's IP address is not configured, an error message appears.

After clicking on the **Import User** button, the confirmation dialog box in Figure 56 appears.

Figure 56
MICB Dashboard – Import Users Confirmation box

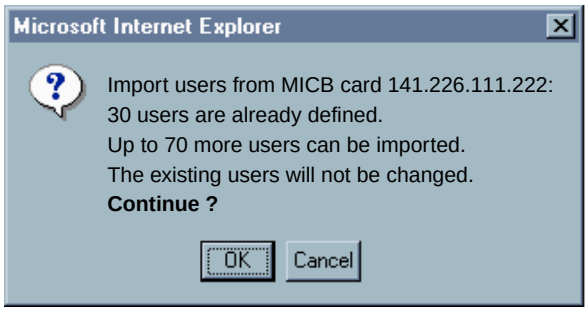


Table 25 describes the information that this message displays.

Table 25
Import Users Confirmation box text

Text line	Description
First	Indicates from which card the users will be imported. If the card is the primary card it shows the IP address of the secondary card and vice versa.
Second	Shows how many users are already defined in this card.
Third	Shows how many users can be imported. An MICB card can have up to 100 users. When the number of users reaches 100, the system terminates the import process.
Fourth	Informs the administrator that existing users will not be changed (that is, the system does not import a user ID if an identical user ID already exists on the card).
Fifth	Asks for confirmation, or cancellation, of the import.

Click on the **OK** button to start the import process.When the system completes the import, it updates the User List window to include imported users. At this point, the user can be deleted or modified as per normal operation.

Call-out Groups

This section enables an administrator to go directly the following windows:

- Call-Out Group List
- Add New Call-out Group

Call-Out Group List

Figure 57 shows the Call-Out Group List window which is the main window for group list administration.

Figure 57
MICB Dashboard – Call-Out Group List window

The window displays a list of groups in the form of a table, sorted by group number. The table is read-only. Table 26 describes the information that appears in the table's columns.

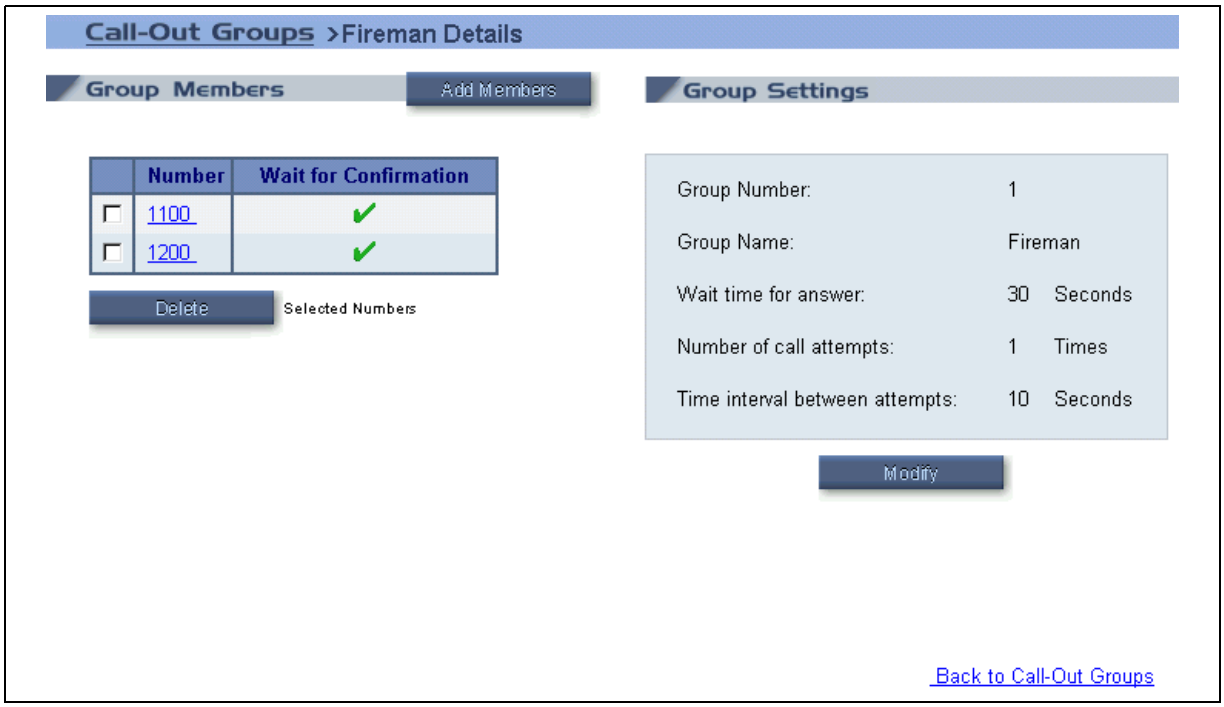
Table 26
Call-Out Group List table columns

Column	Description
Group #	The number that identifies the group. The chairperson uses this number when calling a group from the TUI. *Range:* 1 to 64
Group Name	Free text, up to 20 characters, that describes this group. The name displayed is a link. Click on the name to open the Group Details window for this group.
Members	Shows the number of members in the group.
Checkboxes	Click in a checkbox to select the group. The **Delete** button at the bottom of the window can then be used to delete the group. Before deleting the group, the system displays the following dialog box, for example: "Are you sure you want to delete these three groups?"

Click on the **New Call-Out Group** button to open a window for adding new groups (see page Figure 62 on page 120).

Group details
Click on the group's name in the table in the Call-Out Group List window to open the Call-Out Groups Details window (see Figure 58 on page 115). Use the Call-Out Groups Details window to view and modify an existing group.

Figure 58
MICB Dashboard – Call-Out Groups > Details window



The window shows the members and properties of the selected group. The members appear in a table, with one member per row. Click on the “Next 10” or “Previous 10” link to view additional group members. Table 27 describes the columns in the Group Members table.

Table 27
Group Members table columns

Column	Description
Number	The telephone number of this member. The system dials this number when a chairperson calls this group. Maximum number length is 31 digits. The number displayed is also a link. Click on the number to open the Edit Member window in which the group member can be edited.
Wait for Confirmation	Activate, or de-activate, the answer confirmation for this member as follows: • **Activated** (checkmark) – The default value for new members. When the system calls this number due to group call-out activation, the MICB waits for a “human” answer confirmation. The system prompts the called party to enter an asterisk (*) from their DTMF keypad. If the system does not receive this confirmation, the MICB retries the call as defined in the group’s properties. The system does not connect the called party to the conference, until it receives the answer confirmation. • **Not activated** (X) – The MICB does not wait for confirmation. Upon call origination, the system connects the call to the conference.

Table 27
Group Members table columns (Continued)

Column	Description
Checkboxes	Click on a check box to select a member of the group. The **Delete** button at the bottom of the window can then be used to delete the group member. Before deleting the group, the system displays the following dialog box, for example: "Are you sure you want to delete these five members?"

Use the **Add Members** button at the top of the Group Members table to add a member to the group (see Figure 59 on page 117).

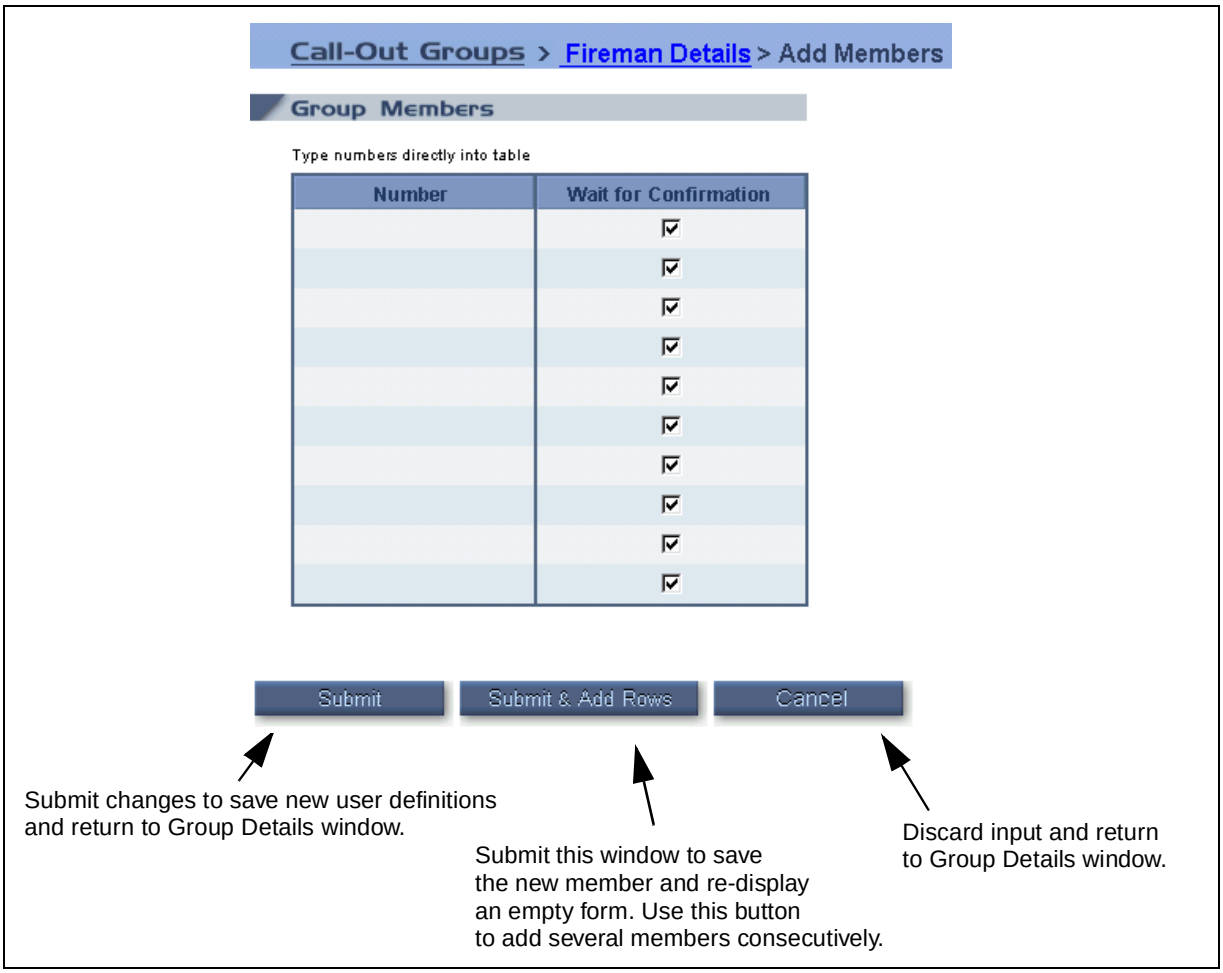
The right side of the window displays the group's properties for outcalling retries. These settings apply only to members with the option "Wait for Confirmation" activated. Table 28 describes these parameters which are view only. Click on the **Modify** button to open a window in which these settings can be changed (see Figure 61 on page 119).

Table 28
Group Settings Retry parameters

Field	Description
Wait time for answer	The number of seconds to wait for the called party to answer when calling numbers in this group.Time is measured from call origination, so it includes the dialing and ringing stages. An answer here, refers to the DTMF * keypad press. *Range:* 15-90 seconds. *Default:* 30 seconds.
Number of call attempts	The number of times to try each number in case of failure. Value 1 means only 1 attempt, no retries. *Range:* 1-3. *Default:* 1.
Time interval between attempts	The number of seconds the system waits, before retrying the same number. *Range:* 5-30 seconds. *Default:* 10.

Add Members – Click on the **Add Members** button in the Call-Out Groups Details window to open the Add Members window. Use the Add Members window to add one or more members to an existing group (see Figure 59 on page 117).

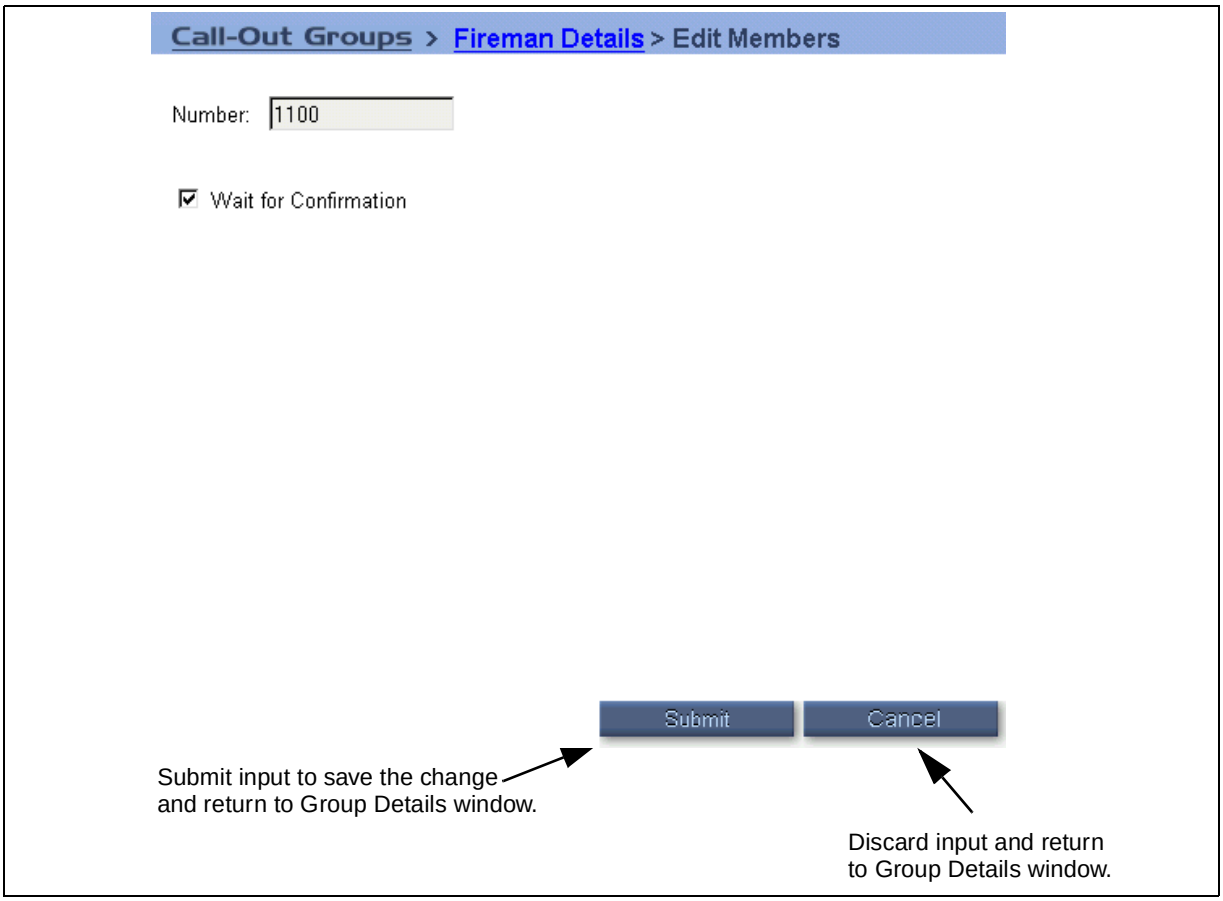
Figure 59
MICB Dashboard – Call-Out Groups > Details > Add Members window



Add members by entering the phone number directly in the table. The default “Wait for Confirmation” option setting is active (that is, checked in the corresponding checkbox). Uncheck the checkbox if you need to change the default setting. The table contains 10 rows.

Edit Member – Click on a specific number in the Call-Out Groups Details window to open the Edit Members window. Use the Edit Members window to modify a member’s number or confirmation option (see Figure 60 on page 118).

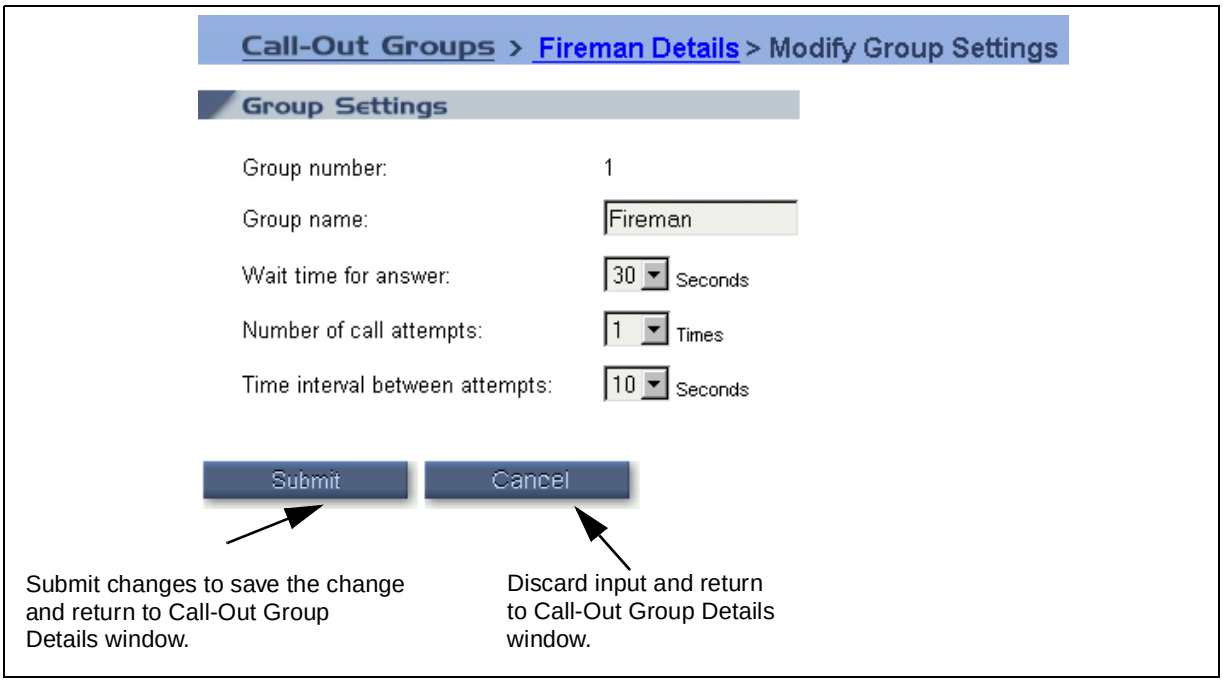
Figure 60
MICB Dashboard – Call-Out Groups > Details > Edit Members window



Edit the number directly in the text box. Change the “Wait for Confirmation” option by clicking in the in Wait for Confirmation box.

Edit Group Properties – Click on the **Modify** button in the Call-Out Groups Details window (below the Group Settings table) to open the Modify Group Settings window. Use the Modify Group Settings window to modify the call-out retry parameters of the group (see Figure 61 on page 119).

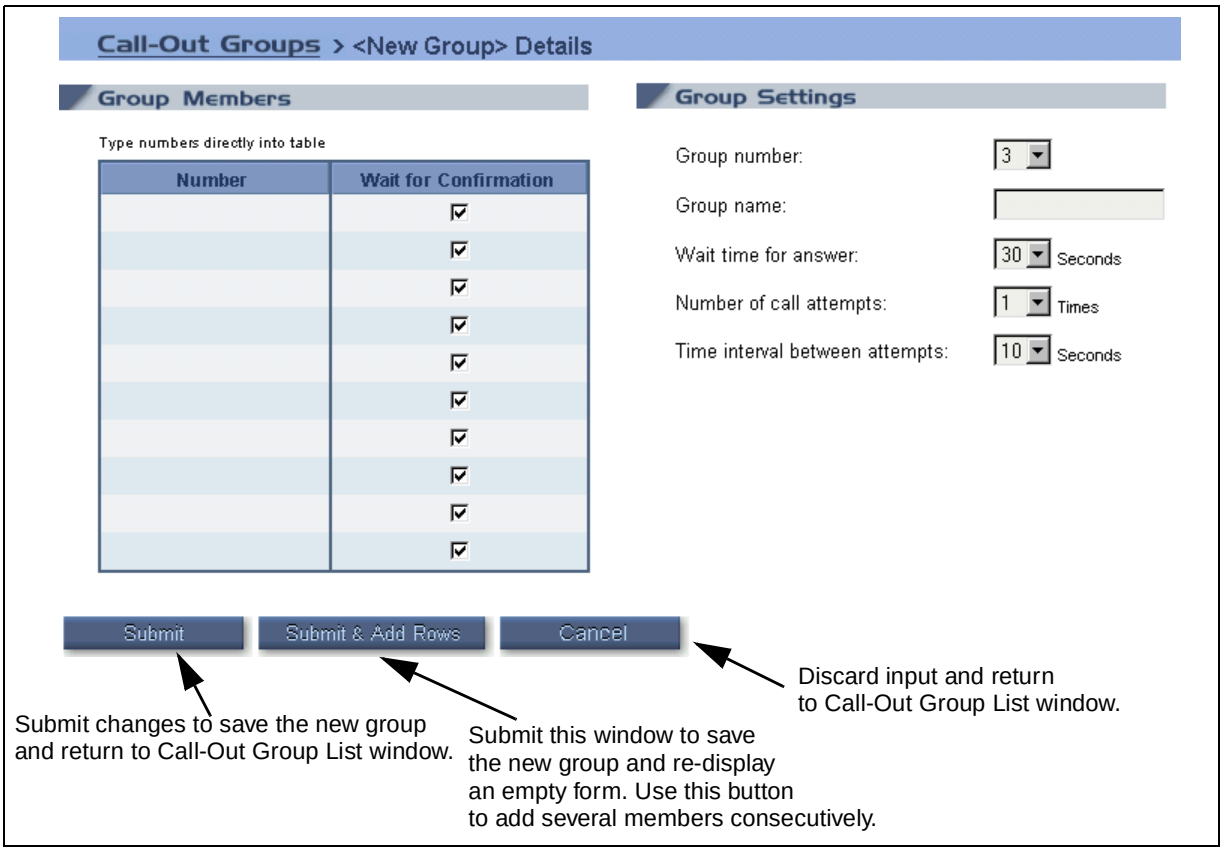
Figure 61
MICB Dashboard – Call-Out Groups > Details > Modify Group Settings window



The Group number is view only. The name and parameters can be modified as described in Table 28 on page 116.

Add a New Group
Click on the **New Call-Out Group** button in the Call-Out Group List window to open the <New Group> Details window. Use the <New Group> Details window to add a new call-out group. Use this window to fill in the new group's members and set the retry parameters (see Figure 62 on page 120).

Figure 62
MICB Dashboard – Call-Out Groups > <New Group> Details window



This window has the same layout as the Call-Out Group Details window (see Figure 58 on page 115), except here all fields are editable. The Group number pull-down menu shows only available numbers (that is, numbers not used by other groups).

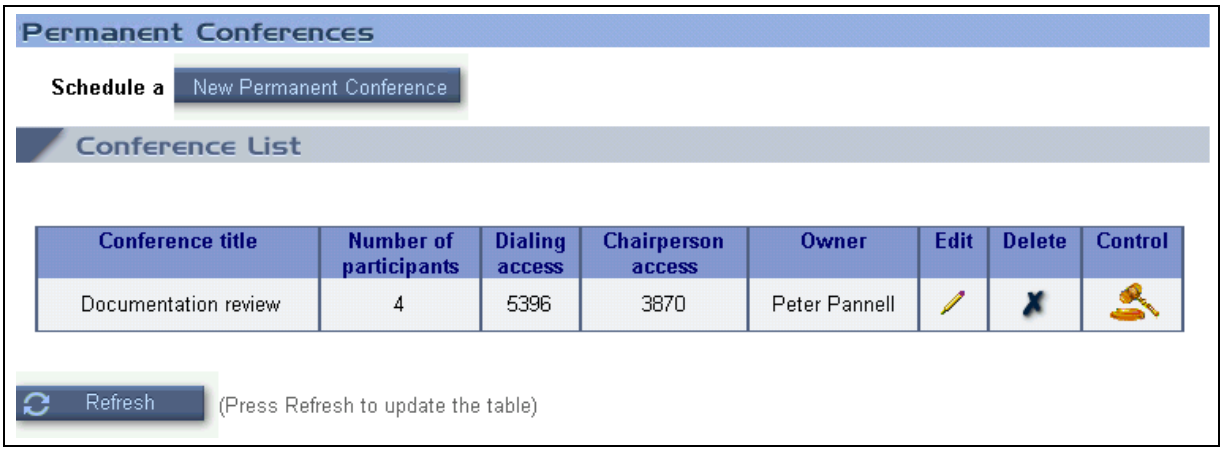
Permanent Conferences

Under this subject an administrator can access the Permanent Conferences List window or go directly to the New Permanent Conference window.

Permanent Conferences List

Figure 63 on page 121 shows the Permanent Conferences List window.

Figure 63
MICB Dashboard – Permanent Conferences List window



The Conference List table shows a list of permanent conferences in the card. This table is similar to the regular conference table (see Figure 36 on page 82), except that the time-related fields (that is, start and duration) do not exist. Start and duration are irrelevant in permanent conferences. All other fields are the same.

Note: Because a permanent conference is always active, the control icon exists for all conferences in the table.

New/Edit Permanent Conference

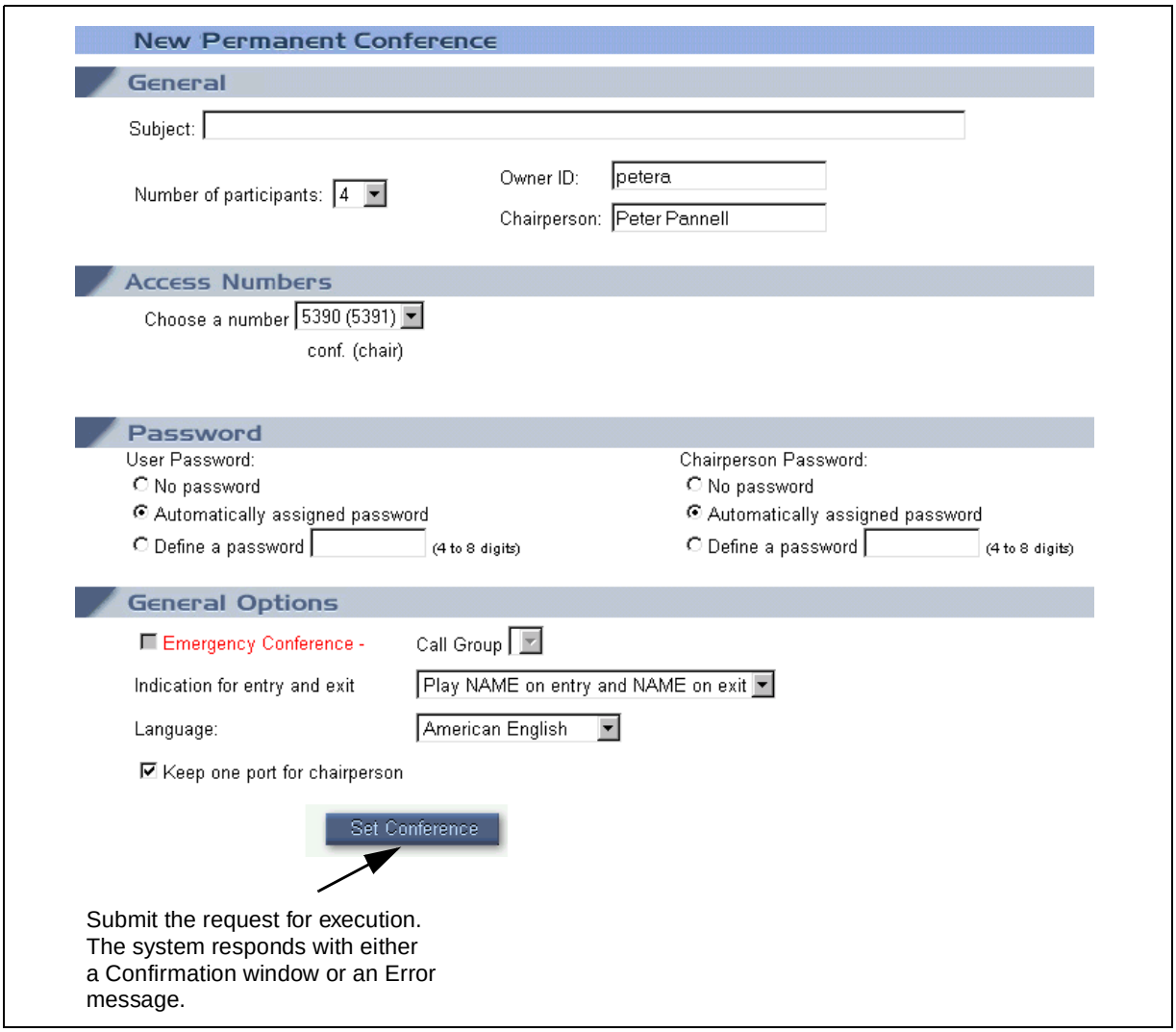
Use the Permanent Conferences List window to perform the following:

- Define a new permanent conference. Click on the **New Permanent Conference** button to open the New Permanent Conference window.
- Edit an existing conference. Click on the edit icon in the conference row of the Conference List table to open the Edit Permanent Conference window.

Note: These two windows are identical, except during the edit operation the window's title shows "Edit Permanent Conference".

Figure 64 on page 122 shows the New/Edit Permanent Conference window.

Figure 64
MICB Dashboard – New/Edit Permanent Conference window



This window is similar to the regular conference scheduling window (see "Scheduling window" on page 84), except that all time-related fields are not applicable. The start time and duration do not appear in this window. In addition, there is no dual-card meeting link, because a permanent conference cannot be a dual-card meeting.

The option "add port if needed" is always no for permanent conferences, so it does not appear in this window.

Unlike the regular scheduling window that has pop-up sections, all fields and options appear on the basic window.

Table 29
Permanent Conference New/Edit parameters

Field	Description
General section	
Subject	Enter text that describes the purpose of the conference. *Range:* Enter up to 20 characters, or leave this field empty. *Default:* Empty.
Number of participants	Enter the number of ports to reserve for this conference, including the chairperson ports. The application makes sure that the total number of reserved ports for this time period does not exceed system capacity. The system performs validation after submission. *Range:* 3 to 32. *Default:* 4
Owner	Enter the user ID that will appear for this conference in billing reports and logs. Any user in the card can be assigned as the owner. However, since this is a permanent conference, the owner cannot modify or delete the conference, unless they are an administrator. Thus, this field is only for billing and logging reference. *Default:* The administrator that defines the conference.
Chairperson	Enter the name of the chairperson for user's reference. *Range:* Text up to 20 characters. *Default:* Empty.
Access Numbers section	
DN pair usage option	The administrator must select a DN pair from the list. The list shows pairs of numbers in the format: [conference (chairperson)]. The system checks the availability of the number when the form is submitted for execution. If the number is not available, the operation fails.
Password section	
User Password	Enter an optional password for the conference. If configured, callers must enter this password to join the conference. Available options are as follows: • None – no password. • Automatically assigned (the default) – The system automatically generates the password. The administrator sets the password length from 4 to 8 digits. • Define a password – The user defines the password. The range is 4 to 8 digits. The window shows the password as it is entered. The system does not check the password for uniqueness. Different conferences can use the same password.
Chairperson Password	Enter a password for chairperson authentication. This field has the same options as the user password.

Table 29
Permanent Conference New/Edit parameters (Continued)

Field	Description
General Options section	
Emergency conference	Click in this box to define an emergency conference with an associated call group. The system automatically calls the specified group's members from the conference when the chairperson dials the conference. The selection box lists existing groups in the card. This type of conference is for invoking emergency personnel (for example, firemen).
Indication for entry and exit	Define how the system announces when people enter or exit a conference. The following options are available from the pull-down menu: • Play name on entry and name on exit (the default). • Play name on entry and tone on exit. • Play tone on entry and tone on exit. • Silence (no indication for entry or exit).
Language	Select the language the system uses for voice prompts during the conference. The pull-down menu offers the set of languages available in the system. The default is the MICB card's default language. When using single-number access, the preferred language takes affect after the caller enters the conference ID and password. Before that the system uses the default language.
Keep one port for chairperson	Click on this box to reserve a port for the chairperson. When all the ports are occupied but one, and the chairperson has not yet dialed in, the remaining port is not available for a participant. If this box is not checked, the system uses the ports on a first-come first-serve basis. In this case, if all the ports are taken up by participants, the system will not allow the chairperson to enter the conference. *Default:* the option is checked (on).

Backup

For more information on how to use the MICB Dashboard to backup files, see "Backup and restore procedures" on page 155.

Reports

For more information on how to use the MICB Dashboard to generate and view reports, see "Reports" on page 161.

Telephone user interface

Purpose

This chapter describes how to use the telephone user interface (TUI) to:

- invoke commands during an active conference
- schedule conferences and record greetings

The chapter contains the following sections:

- **"Overview" on page 125** – introduces the telephone user interface.
- **"TUI operation during an active conference" on page 126** – provides procedures for using TUI features from a dual tone multi-frequency (DTMF) telephone while in an active conference.
- **"TUI services" on page 136** – describes TUI services available when there is no active conference, such as scheduling.

Overview

Active conference

The MICB provides a DTMF, menu-driven telephone user interface. The TUI enables the chairperson, and conferees, to invoke commands from their telephone during an active conference, such as mute or unmute. This functionality is provided during a meeting with no additional provisioning required.

Scheduling and recording features

To access the TUI for scheduling and recording, dial the TUI DN. The system prompts the user to enter their TUI ID and password.The system responds depending on the user ID as identified by the TUI ID as follows:

- Regular user – the TUI responds with a voice menu with the following two items:
  - — schedule a conference
  - — record a conference-specific greeting

Note: If the second feature is disable by the administrator (see Figure 50 on page 103), the system skips this item and the user directly enters the scheduling menu.

- Administrator – An administrator does not schedule a conference. The TUI responds with a voice menu with the following two items:
  - — record a conference-specific greeting
  - — record a system brandline greeting

Note: If the first feature is disable by the administrator (see Figure 50 on page 103), the system skips this item and the administrator directly enters the brandline greeting menu.

Scheduling and recording greetings requires a system TUI DN and TUI ID for each user. For more information about defining a new DN, see "Installation and configuration" on page 41. For more information about defining a DN for the TUI, see "Step 2 – Access Numbers" on page 70.The BUI must be used to define a TUI user ID for each user (see "Users List" on page 107).

If a second user dials the TUI DN when the TUI is in use, the MICB plays a voice message announcing that the port is in use.

TUI operation during an active conference

This section describes how the TUI can be used while in an active conference.

Chairperson features

Dial-out

The chairperson can dial out and call a new party outside of the conference. They can talk with the party or bring the party into the conference. As a chairperson, dial **0<DN>#* (# is a digit entered by the chairperson after the DN) to dial a party outside the conference or **0* to access the operator.

Bring the party into the conference by dialing **2* or disconnect the call by dialing **3*. If the chairperson dials the wrong number, dial **3* and re-dial. To redial the last number dialed, dial **#*.

The MICB card selects the port for dialing out. The port is available if the number of ports reserved for the conference is greater than the number of conferees that have joined the conference. When all reserved ports are taken, the port can be available, if there are un-reserved ports on the MICB card and the port expansion feature is enabled for that conference. If all reserved ports are taken and there are no unscheduled ports available, the system cannot complete the call.

Note: When the chairperson dials out to another MICB conference, two ports are seized, the dial-out port of the local MICB and the dial-in port of the remote MICB. This connection can be terminated only if the chairperson drops the dial-out port of the local MICB. However, normally the dial-out call is a telephone, so the system only seizes one port.

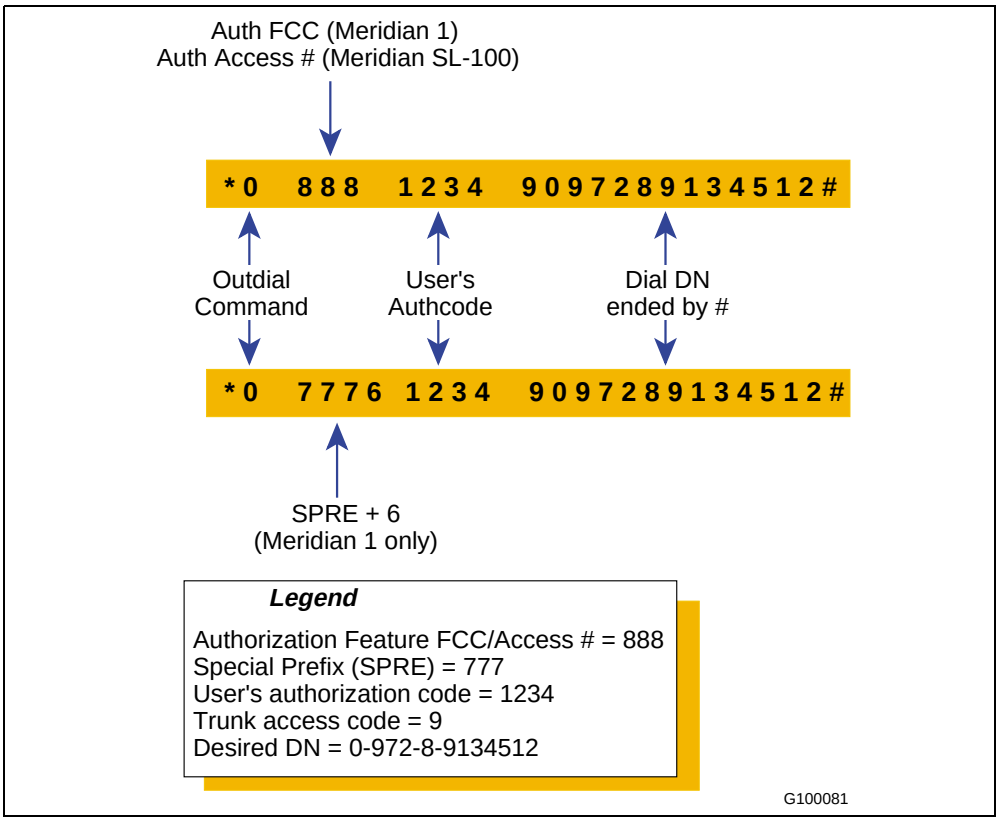
Dial-out Authorization

The Dial-out Authorization feature enables the chairperson to connect external parties to the conference when the desired destination number is restricted.

This feature uses the Meridian Authorization feature. As such, the chairperson must be aware of outdialing restrictions and know the authorization access code (Flexible Feature Code – FFC or Special Prefix – SPRE on the Meridian 1; Auth Access # on the Meridian SL-100).

The chairperson must enter the whole string of authorization numbers as the example in Figure 65 on page 128 shows. There are no confirmation tones or dial tone in the middle of dialing.

Figure 65
Dial-out Authorization dialing example



Note: In BUI, define the same sequence as above, except do not enter the command code ** 0*.

If using this feature and Group Call, make sure that the authorization access code precedes the restricted DNs in the group call list.

All ports mute/unmute toggle

A chairperson can place all conference participants, except the chairperson, on mute by dialing **10*. While on mute, the participants can listen to the conference. To unmute the participants, the chairperson dials **10* again. Because there is one command for mute and unmute, the system announces to the chairperson one of two possible voice messages: “All participants have been muted” or “All participants have been unmuted.” Only the chairperson hears the mute/unmute announcement.

Group call-out

Each MICB card supports up to 64 group call-out lists, each with up to 61 telephone numbers. Each telephone number can be up to 31 digits in length.

The administrator defines group call-out lists through the BUI (see "Call-out Groups" on page 113). The system saves the information on the MICB PCMCIA disk.

The administrator must define the following options for each group list:

- number of dial-out retries allowed (range: 1-3, default: 1)
- time between each dial-out retry (range: 15-90 seconds, default: 30)

The chairperson on an active conference can call all members of a group call-out list by dialing the following: **2 <group list number> #*. The MICB dials out to all the telephone numbers in the requested group call-out list simultaneously. If there are more than 31 numbers on the group call-out list, the system requires two MICB cards.

When the system uses two MICB cards in a group call-out, the primary card divides the group call-out list into two groups. The primary card dials one group of numbers and sends the second group to the secondary card over the TCP/IP LAN. The secondary card then dials the second group of numbers. The system dials out both groups of numbers simultaneously.

The MICB card dials out by allocating a free port and originating the call on it. The system does not connect the port to the meeting, until the call successfully completes. After the MICB card originates the call, it plays a specific prompt and keeps repeating the prompt for a number of seconds (determined by the administrator). The default configuration forces the called party to respond by dialing a star * during this interval. When the MICB card detects the correct response, it connects the call to the meeting. If the MICB card does not detect the correct response within the defined time and the defined number of retries, the MICB card disconnects the call.

> ***Note:*** The administrator can configure the call to complete without requiring the called party to enter a star *. This option enables the connection to paging systems and auto-attendants.

The system limits group call-outs to the number of available ports on a conference. When a chairperson uses a list containing 61 numbers, and the meeting has 20 free ports, the system dials only the first 20 telephone numbers.

Group Call-out Smart Retry – When the chairperson makes a group call-out to the same group for the second time, the system repeats the call-out only to numbers that are not connected in the conference. The second call-out includes calls to the following:

- numbers not successfully connected in the previous group call-out
- numbers that were connected, but then disconnected

The Group Call-out Smart Retry feature minimizes port usage during group calls.

Lock or unlock the conference

The chairperson can lock the conference to prevent any new conferees from joining by dialing **4*. The chairperson can unlock the conference allowing new conferees to join by dialing **4* again. A caller trying to join a locked conference hears an announcement indicating that the conference is locked. The system then disconnects the call. The chairperson can dial-out and include a conferee when the conference is locked.

Because there is one command for lock and unlock, the system announces to the chairperson one of two possible voice messages: “Meeting is locked” or “Meeting is unlocked.” Only the chairperson that activates the command hears the lock/unlock announcement.

Count conferees

The chairperson can count the number of conferees that have joined a conference by dialing **69* (for announcing to the chairperson only), or **60* (for announcing to the whole conference). The MICB card issues a string of voice prompts, one for each conferee in the conference, that only the chairperson hears. If a new conferee joins the conference after the chairperson activates the command, the MICB card does not count that new conferee. If the system drops a conferee after the “count the conferees” or “play list” command, they are counted, but not named.

When the chairperson dials **69/*60*, the conferees hear a quiet click.

Table 32 on page 133 lists the TUI subcommands available to the chairperson when counting conferees.

Drop all conferees

The chairperson can drop all conferees from the conference, except the chairperson, by dialing **90*. The MICB does not issue an announcement to the conferees before disconnecting. After the system disconnects the conferees, the MICB card issues an announcement to the chairperson indicating that there are no conferees on the conference. The announcement is followed by 60 seconds of music. The conference remains active, so conferees can dial in again.

Drop last dialed conferee

The chairperson can drop the last conferee to join the conference through dial-out by dialing **91*. The chairperson can drop the last conferee to dial in by dialing **92*. These commands are not repeatable (that is, the chairperson can drop the last conferee to dial in, but not the second-to-last to dial in). If the chairperson is the last to dial into the conference, the MICB card cannot execute the **92* command.

Conference duration expansion

The chairperson can expand the duration of a conference by 15 minutes by dialing **98*. If the expansion is successful, the chairperson receives the voice message, “Your meeting duration has been expanded.” If the duration expansion is not successful, because there are not enough resources, such as ports or DNs, the chairperson receives the message, “Your meeting duration has not been expanded.”

The maximum conference duration, including all chairperson expansions, is 12 hours. The MICB card does not permit conference duration expansion to a conference scheduled to end within three minutes of the expansion request.

Chairperson command summary

Table 30 lists conference commands that the chairperson can execute on the telephone set while a conference is in progress.

Table 30
Chairperson commands

Chairperson Command	Description
*0<DN>#	Dial out to a DN (called party directory number, which is not a conference participant).
*0#	Dial out to the assistant DN.
*2<GN>#	Group call-out, where GN is the group number to call.
*4	Lock or unlock the conference.
*7	Volume control.

Table 30
Chairperson commands (Continued)

Chairperson Command	Description
*10	All ports mute/unmute toggle.
*19	Self mute/unmute toggle.
*52	Release chairperson control.
*60	Count conferees and announces names to all participants.
*69	Count conferees and announces names to chairperson only. Activates a scrolling menu for the chairperson (see Table 32 on page 133).
*90	Drop all ports, except the chairperson's port.
*91	Drop the last dialed-out port.
*92	Drop the last dialed-in port.
*98	Extend the conference by 15 minutes.
*99	Stop or start the initial conference music by the chairperson, which is possible only when the chairperson is the first person joining the conference. The first entry stops it, the second entry starts it.
*	Abort current command.
*#	Redial last dialed DN.

Table 31 shows the commands available during a dial-out call (that is, after dialing *0<DN>#).

Table 31
Chairperson commands during dial-out call

Chairperson dials ...	In order to ...
*2	Return to the conference with dialed party.
*3	Return to the conference without dialed party.

While the system is announcing the list of conference participants after the chairperson enters *69, the chairperson can execute the commands in Table 32.

Table 32
Chairperson commands during count command

Chairperson dials ...	In order to ...
#	Stop and start the playlist.
0	Consult privately with the conferee.
1	Mute/unmute the conferee.
2	Play the current conferee name greeting.
*3	Return to the conference.
4	Select the previous conferee and play name.
6	Select the next conferee and play name.
9	Disconnect the current conferee.
**	Start and stop the help menu.

Features available to all participants

Self mute/unmute toggle

All conference participants, including the chairperson, can put themselves on mute by dialing **19*. While on mute, the participant can listen to the conference. To unmute, the participant dials **19* again. Because there is one command for mute and unmute, the system announces to the participant one of two possible voice messages: “Muted” or “Unmuted.” Only the participant that activates the command hears the mute/unmute announcement. The mute/unmute command is available to those participants who dial into the conference and who the chairperson brings into the conference using the dial-out command.

Stop or start music

This feature stops or starts the initial conference music, which is possible only when the conferee is the first person joining the conference. Dial **99*. The first entry stops it, the second entry starts it.

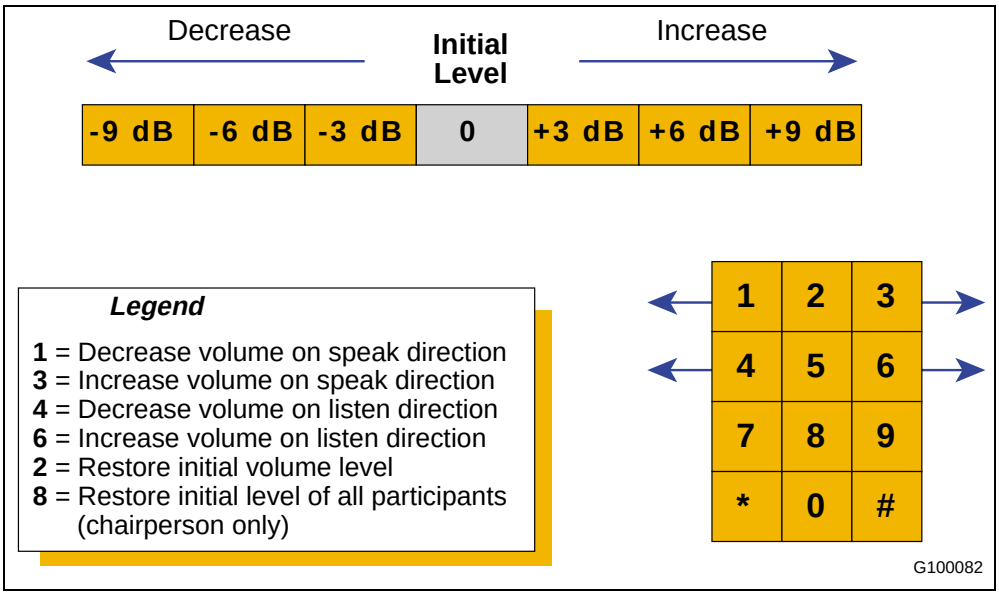
Adjust the audio volume of a conference

Follow the steps in Procedure 19 to adjust the volume of a conference.

Procedure 19
Adjust the conference audio volume

1 Dial **7* to adjust the volume. Figure 66 shows how the keypad operates this feature.

Figure 66
Volume control feature operation



When making a selection, the system applies the command, plays a confirmation tone, and returns the user to the conference.

2 Each invocation of the command advances one step in the required direction. To advance more than one step, the whole sequence must be repeated. For example, to reach the maximum volume in the listen direction, dial:

**76 *76 *76*

3 The menu can be interrupted, so the two-digit sequence can be entered without waiting for the menu.

This procedure is now complete

Help

The chairperson can access a help menu by dialing **. The help menu is a voice recording of all chairperson command options. The chairperson can stop the help menu before it finishes by dialing ** again.

The help command is sensitive to where the chairperson is in the command structure. For example, if the conference is in the normal active state, the chairperson hears the main list of commands after dialing ****. If the chairperson dials out to a person and then dials ****, the chairperson hears the list of commands relevant to dialing out. If the chairperson dials **69* or **60* to count conferees, and then dials ****, the chairperson hears the list of commands relevant to counting conferees.

Conferees can dial **** to hear a list of command options available to conferees. Only the participant who dials **** hears the relevant list of commands.

Conferee features

Acquire and release chairperson control

Follow the steps in Procedure 20 to acquire, or release, chairperson control.

Procedure 20
Acquire/release chairperson control

1 To acquire chairperson control, dial **51*. The system reacts as follows:

- *If another chairperson is present at the conference, the command fails. The system notifies the user and returns them to the meeting.*
- *If there is no active chairperson, the system prompts the user to enter the chairperson password for the meeting. If the password is correct, the user becomes the chairperson. If the password is incorrect, the system prompts the user to retry two more times. If the password is still incorrect, the command fails and the system returns the user to the meeting.*

2 To release chairperson control, dial **52*. Only the chairperson uses this command. When activated, the chairperson becomes a regular conference participant allowing someone else to acquire chairperson control.

This procedure is now complete

Conferee command summary

Table 33 lists conference commands that a conferee can execute on the telephone set while the conference is in progress.

Table 33
Conferee commands

Conferee command	Description
*7	Volume control.
*19	Self mute/unmute toggle.
*51	Acquire chairperson control.

Table 33
Conferee commands (Continued)

Conferee command	Description
*99	Stop or start the initial conference music, which is possible only when the conferee is the first person joining the conference. The first entry stops it, the second entry starts it.
*	Aborts current command.
**	Start or stop the help menu.

TUI services

This sections describes TUI services that are used when there is no active conference.

Schedule a conference

When using the TUI scheduler, first enter the TUI user ID and password. If a port is reserved for the TUI, only 31 ports are available for conference use. After scheduling a conference using the TUI, the BUI can be used to view, modify, or delete the conference.

The conference defined from the TUI has default attributes. Define the conference parameters, through the telephone keypad, at the prompts of a guided voice menu. The MICB plays messages when an error is made.

> ***Note:*** There are up to seven minutes to schedule a conference with the TUI. After seven minutes, the MICB sends a voice message indicating that the allotted time is over. The MICB then disconnects the call.

The MICB sets up the following default attributes:

- entry and exit by name
- no custom greeting
- no conference expansion
- no name for the name of the conference
- no name for the name of the chairperson

To schedule a conference through the TUI, follow the steps in Procedure 21 on page 137.

Procedure 21
Use the TUI to schedule a conference

1. Dial the TUI DN.
2. At the prompt, enter your TUI user ID.
3. At the prompt, enter your password (6 digits).
4. At the prompt, enter the date and time of the conference (optional). The default is the current day and time.
5. At the prompt, enter the duration of the conference.
6. At the prompt, enter the number of ports required for the conference.
7. At the prompt, enter the Conferee DN (optional).

   If a DN is not entered, the MICB card generates one. The MICB card determines the Chairperson DN automatically.
8. At the prompt, enter the password length (optional).
9. At the prompt, enter the language (optional).

   After entering all conference parameters, the MICB requests you to confirm the reservation.

Note: If configured, the web server sends a confirmation E-mail.

This procedure is now complete

Record a brandline greeting

The TUI can be used to record the customized brandline greeting when an administrator TUI password is used for the login. Procedure 22 shows how to use this feature.

Note: Although the greeting can be recorded in any language, the TUI instructions are in English only.

Procedure 22
Use a brandline greeting

1. Dial the TUI DN. Enter your TUI administrator ID and password.

   The system responds with a menu and steps through how to operate the feature.
2. The chairperson must activate the brandline greeting from the BUI.

This procedure is now complete

The maximum length of the greeting is 10 seconds. The system plays greetings to conference participants in the following order:

1 Initial greeting

   a MICB factory greeting – “Welcome to the conference call.”

   b Brandline greeting – “Welcome to Company XYZ’s conference call.” This greeting replaces the factory greeting.

2 Conference-specific greeting – “This is department 201’s weekly meeting.”

In this example, when participants call they hear: “Welcome to Company XYZ’s conference call. This is department 201’s weekly meeting.”

Note: Dual-card meetings use the brandline of the primary card, so that all participants hear the same greeting.

Record a conference-specific greeting

Conference-specific greeting operation is similar to brandline greetings, except that they can be recorded by users or administrators. The maximum length is configured by an administrator up to 10 seconds. The system deletes the voice file at the end of the conference and it cannot be used for other conferences. Follow the steps in Procedure 23 to configure a conference-specific greeting.

Procedure 23
Configure a conference-specific greeting

1 Dial the TUI DN. Enter your TUI user or administrator ID and password.

   The system provides a menu with various options.

2 Operational steps are as follows:

   a When scheduling a meeting, the system provides a reference number which uniquely identifies the meeting. The system displays this reference number in the BUI and in the confirmation E-mail.

   b After scheduling the meeting, dial the TUI Services DN, enter login data, and select “Record customer greeting” from the voice menu.

      The system prompts you to enter the reference number to identify the meeting.

   c Enter the number received in step **a**.

      The system repeats the number and prompts the user to confirm it or re-enter it.

   d Confirm or re-enter the number.

      The system provides a menu for recording the greeting similar to that used for the brandline greeting.

This procedure is now complete

After recording the greeting, it can be later verified, re-recorded, or deleted. Meeting details displayed in the BUI indicate whether or not a greeting exists.

This feature also applies to always-on conferences. However, for always-on conferences, only the administrator can record the conference-specific greeting.

A greeting recorded for a conference that is part of a recurrent chain applies to occurrences following that conference.

In dual-card meetings, the user or administrator records the custom greeting to the primary card. The system automatically copies it to the secondary card, so that all callers hear the same greeting.

Maintenance

Purpose

This chapter describes how to maintain and troubleshoot the MICB card and associated equipment.

The chapter contains the following sections:

- **“Maintenance overview” on page 141** – introduces the maintenance strategy.
- **“Diagnostic tools” on page 143** – lists the available maintenance tools.
- **“CLI command summary” on page 147** – shows the commands technicians can use from the CLI to perform maintenance activities.
- **“MICB fault isolation and correction” on page 150** – describes faults and shows recommended recovery actions.
- **“Error message handling” on page 151** – describes the on-line error message system.
- **“Backup and restore procedures” on page 155** – provides procedures for backing up and restoring data.

Maintenance overview

Perform operations, administration, and maintenance (OA&M) of the MICB system by using the command line interface (CLI). Access the CLI through a the following:

- A TTY terminal connected to the MICB card or through a PC emulating a terminal. The PC connects to the MICB card through the Ethernet Adapter.
- The administration BUI.

An operator can use the CLI to generate reports and perform port maintenance. An administrator can use the CLI to manage system administration, maintenance, and security.

To conduct conference OA&M for an MICB card, connect a terminal to the RS-232 port or the Ethernet connector associated with that MICB card. The maintenance terminal connects to each MICB card through an IPE module I/O panel connector or through the Ethernet adapter card.

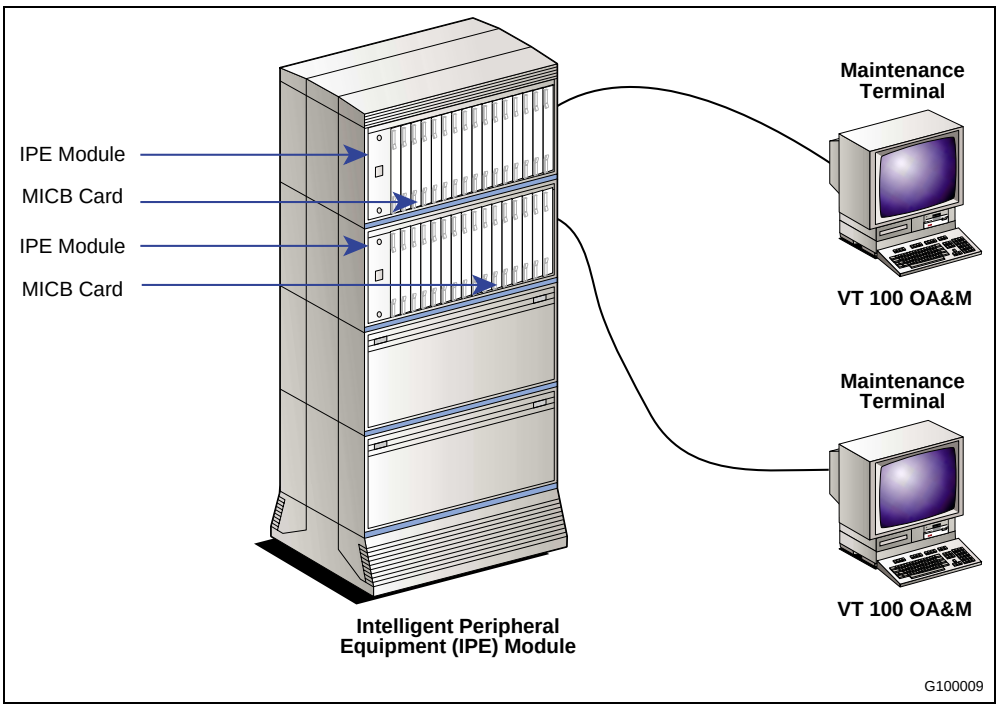
The Ethernet adapter provides two options:

- direct terminal connection or modem connection to DB-9 connector
- Ethernet connection, where multiple terminals connected to the Ethernet can access an MICB card

For the Ethernet connection option, an IP address assigned to the MICB card is required to enable access to the MICB through the LAN.

Figure 67 shows an Meridian system with two IPE modules. This example shows each IPE module with one MICB card. Each MICB card connects to its maintenance terminal through the associated IPE module I/O panel connector. Use one terminal for all MICB cards by moving the terminal cable to the I/O panel connector of the card to be accessed.

Figure 67
MICB card in the Intelligent Peripheral Equipment Module



Problem solving

A problem can have more than one cause. To isolate the cause, a knowledge of MICB operation is required. After identifying the cause, the problem can be corrected by replacing defective cards, connecting accidentally disconnected cables, or correcting software security problems. The Meridian system and the MICB provide built-in self-diagnostic indicators and software and hardware tools. These diagnostic facilities simplify system troubleshooting and reduce mean-time-to-repair (MTTR).

Make sure that the Meridian system is operating correctly, before diagnosing MICB problems.

FOR MORE INFORMATION

Refer to the following:

- **Meridian 1** – *Hardware Replacement* and *General Maintenance Information*
- **Meridian SL-100** – *IPE Reference Manual* and *Card Replacement Procedures*

Diagnostic tools

Use the following diagnostic tools to troubleshoot problems in the system, including problems with the MICB. When diagnosing MICB problems, use the following tools:

- LED indicators
- display codes
- card self-tests
- sanity monitoring
- diagnostic commands (that is, overlay commands for the Meridian 1 and MAP commands for the Meridian SL-100)
- history files
- TCP/IP connectivity test

MICB status LED indicator

The MICB has a red LED indicator at the top of the faceplate that indicates the status of the card. If the LED is lit, the card can be faulty or manual busy (Man). The card goes through a series of tests. When inserted into the slot or reset, the card:

- blinks three times during self-test
- runs software files from the PCMCIA to the MICB card

- blinks three more times
- stays on until a return to service (RTS) occurs

This procedure takes approximately 45 seconds. If the card turns on and remains on without blinking, the card is not functioning correctly. The LED turns off when the card returns to service.

Self-test

Each MICB card automatically performs a self-test when inserted into an operating system module, when it is powered up, or when the system is reset. A self-test can be performed on a card using software commands or menus.

The self-test checks general MICB functions and determines if they are operating correctly. The checks are useful when first installing the cards, because the card automatically starts the self-test when inserted. The self-test provides an immediate indication of the card's operating status by performing a detailed test and analysis of the installed hardware. The test determines the integrity of the hardware and establishes the connection of the MICB card.

Table 34 describes the items the system checks during the MICB self-test.

Table 34
MICB self-test sequence

Item tested	Description
Processor/Co-processor	Reads and stores processor ID. Runs processor self-test.
DRAM	Checks the amount of DRAM installed. Performs read/write test.
System I/O Controller	Performs read/write test on selected registers.
PCMCIA Controller	Performs read/write test on selected registers.
DS-30X Interface	Tests shared memory and performs loopback test over SD-30 LCA.
On-board DSP card	Checks the presence of DSP cards and initiates diagnostic tests on DSP cards, if present.
PCMCIA hard drive	Checks the presence of the hard drive and checks the configuration information.
PCMCIA Flash card	Checks the presence of Flash memory and checks configuration information.

Sanity monitoring

Sanity monitoring is a background routine that checks the operation of system resources, such as CPU activity and memory allocation. This background routine tries to restore normal operation if the system performance has degraded to an unacceptable level. If all attempts to restore normal operation fail, this routine restarts the system to restore operation. If the soft reset is not effective, the system initiates a full, board-level reset. If the full reset is not successful, the maintenance LED remains on.

Diagnostic commands

Meridian 1 overlay commands

Each card performs diagnostic tests as part of the daily routines. Diagnostic tests can also be activated from a maintenance TTY.

The boot time of the MICB from reset, or power up, to when the card is ready and from an ENLC to when the ports are idle is approximately two minutes.

All relevant system maintenance commands for an extended digital line card apply to the MICB and are handled transparently to the system. Use LD32 to enable and disable an ACD M2616 telephone.

Table 35 lists some of the commands used to control the MICB status and functions.

Table 35
Commands to enable/disable MICB channels

Command	Operation performed
LD 32	
DISC/ENLC	Disable/Enable specified card.
DISU/ENLU	Disable/Enable specified channel.
LOOP	Performs a network memory test, continuity test, and signaling test on the specified loop.
STAT	Get status of specified card/channel.
LD 30	
UNTT	Performs self-test on the MICB.

Meridian SL-100 diagnostic commands

Each card performs diagnostic tests as part of the daily routines. Diagnostic tests can be activated from the MAP terminal on the Meridian SL-100. The MICB card appears as an extended digital line card to the system. For the diagnostic routine to pass in the LTP level of the MAP terminal, the feature Communicator must be assigned assigned to key 1 of the LEN.

Table 36 lists commands used to control the MICB status and functions.

Table 36
Meridian SL-100 commands to enable/disable MICB channels

Command	Operation performed
IPE MAP Level	
Bsy Card x/ RTS card x	Disable/enable specified card.
Tst	Perform a network memory test, continuity test, and signaling test on the specified loop.
QueryPM Inven Card x	Get status of specified card.
LTP MAP Level	
Bsy	Make the LEN or DN busy.
Bsy INB	Take the port out of service. The system does not generate alarms.
RTS	Bring the MICB port in-service.

Note: During a one night Process (ONP), a no restart switch activity (SWACT) to the other central processing unit (CPU) drops active calls on the MICB card. A warm SWACT of the front end during maintenance activities does not affect active calls on the MICB card.

TCP/IP connectivity test

Maintenance technicians can use “ping” to test if the LAN connection is installed and configured properly. Perform a ping test in one of the following ways (they are equivalent so there is no need to try both):

- from a computer on the local LAN to the MICB card’s IP address
- from the CLI (under the **SMaint/** directory) to the IP address of a computer on the local LAN

CLI command summary

Using CLI commands

The CLI contains menus and submenus. To select a menu option, enter the appropriate short command or full command at the prompt. When a menu is selected, use the commands in Table 37 to navigate to other menus or to display help.

Table 37
Navigating the menus and displaying help

Command	Result
*	Returns to the previous menu.
/	Returns to the top menu level.
?	Displays help for the commands in the current menu.

When entering a menu option that has parameters defined, the “Modify, Save, or Cancel:” command line displays so that the parameters can be modified, if required.

To modify system parameters and objects, use one or more of the commands in Table 38 and Table 39.

Table 38
Modifying parameters

Command	Result
M	Modifies one or more parameters.
S	Saves modified parameters.
C	Cancels the modification and allows the parameter to keep its previous value.

Table 39
Modifying objects

Command	Result
<cr>	Accepts the current value when the **Enter** key is pressed.
value <cr>	Changes the attribute with a new value when the value is entered and the **Enter** key is pressed.
.	Cancels the modification and allows the object to keep its previous value.

To modify a value or attribute of an object, the program responds with a sequence of prompts: one prompt for each attribute of the object. The prompt defines the name and the current value of the attribute. You can change the value, accept the current value, or cancel the modification as follows:

attribute_a (current_value_a): new_value_a <cr>
attribute_b (current_value_b): <cr>
attribute_c (current_value_c): .

The system can display the current value and a list of available values to select. In the following example, the value of attribute_d changes to bbbb:

attribute_d (current_d, (1-aaaa, 2-bbbb, 3-cccc)): **2**

When executing the command(s), the program provides the option to modify, save, or cancel the changes. When **Save** is entered, the system accepts the changes. After the session ends, use the commands in Table 37 on page 147 to navigate through the menus.

MICB CLI commands

Table 40 shows MICB-specific CLI commands.

Table 40
MICB CLI command summary

Menu and command	Items and commands
System administration: **SA**	System Attributes Editor: **SY** Use the System Attributes Editor for initial card configuration (see Procedure 13 on page 66) and to define the following: • card name – up to 10 characters; appears in top of the initial window if specified. • refresh period – time between updates to CLI window when not in use, from 0 to 60 minutes (default is 5 minutes). 0 disables system status display. • short occupancy – detects short connection time of an MICB port. Connection times less than the threshold can indicate a bad connection of incorrect DN dialed. When this occurs, the system increments a counter. When the system checks counters, it displays those with peg counts as potential problems. disconnect lone participant – time before system disconnects a single participant in a conference (default is 30 minutes).

Table 40
MICB CLI command summary

Menu and command	Items and commands
System Maintenance: **SM**	System Test: **ST** To perform system component tests enter: • i – perform in-service test that do not disrupt service • o – perform out-of-service tests Maintenance Report Browser: **MR** Browse maintenance reports by date. For more information, see "CLI Maintenance (Error) Report" on page 176. Ping Test: Enter a computer's IP address to test IP connectivity with this computer. Short Connection Report: **SC** Browse short connection reports by date (see "CLI Short Connection Report" on page 163 Database Archive: **AR** Backup the customer database (see "Backup" on page 156). Database Restore: **RE** Restore the customer database (see "Restore" on page 159). Card Restart: **CR** Restarts MICB card and begins software reload. Message Analysis Tool: **SHO** Prints information about an error message that is entered. Message Filtering: **ERR** Enables the filtering of error messages. Data Conversion: **CONVERT** Copies the data from the upper PCMCIA, converts to MICB 3 format, and stores it in the lower PCMCIA.
Protected administration: **PA**	Password Editor: **PS** Edit passwords (see "Appendix A: Password security" on page 187). Functionality Upgrade: **FU** Performs a functionality upgrade. *The system prompts for the number of ports and for the keycode that must be entered in three rows of eight characters each.* Software Upgrade: **SW** Performs a software upgrade. *The system first prompts for the source: upper socket or FTP. If FTP is entered, the system then prompts for IP address, path to file, login, and password.* Administrator BUI Reset: **AB** Reset passwords to the default (that is, 000000) of all administrators that use the BUI.
Port maintenance: **PM**	Port Status Display: **PS** Displays status of all MICB ports as follows: Idle, Dialing_out, Ringing, Talking, or Disabled. Port Disconnect: **PD** Disconnect a specific port from the conference.

Table 40
MICB CLI command summary

Menu and command	Items and commands
Report Generation: **RG**	Meetings Log Browser: **ML** Browse the meeting log (see "CLI Meetings Log Report" on page 165). Log ordering: **ORDer_mlog** Prompts for the same parameters (year, month, day) and displays the log contents sorted by access DN. The advantage is that all records of each specific conference appear together.

MICB fault isolation and correction

Alarm clearing procedures for the MICB are the identical to those for other IPE cards.

FOR MORE INFORMATION

Refer to the following documents for additional information about how to clear alarms:

- **Meridian 1** – *Fault Clearing*
- **Meridian SL-100** – *Alarm Clearing Procedures*

Table 41 describes MICB service problems and the test procedures used to solve these problems.

Note: If the problem cannot be solved after using all available diagnostic tools and test procedures, list the symptoms observed and contact your Nortel Networks representative.

Table 41
MICB equipment problems

Symptoms	Diagnosis	Solution
Red card LED on the MICB is permanently on.	Card is disabled or faulty.	Check the card status and perform a self-test on the card by pulling it out and plugging it back in, or from the CLI using the **cr** command under the **SMaint** menu.
Display on the controller card shows fault codes.	Card faulty, failed self-test, or problem communicating with peripheral equipment.	Refer to the *Meridian 1 XII Administration* or *Meridian SL-100 Log Reference Manual* for a description of the fault codes. Based on the description, take the appropriate action to resolve the problem.
Error messages the TTY terminal or the MAP displays.	Hardware or software problems with the MICB.	Note the error messages. Refer to the *Meridian 1 XII Administration* or *Meridian SL-100 Log Reference Manual* for their description. Based on the description, take the appropriate action to resolve the problem.

Card replacement

The MICB uses PCMCIA technology which enables the MICB to be removed from the IPE shelf indefinitely without losing the configuration data. Before replacing the PCMCIA card, back up the data on the card so that it does not have to be re-entered (see "Backup and restore procedures" on page 155). Use Procedure 24 to replace an MICB card.

Procedure 24
Replace a card

1. Prepare for this procedure (see Procedure 1 on page 42).
2. Disable the MICB card.
3. Remove the card from its card slot in the IPE module.
4. Remove all PCMCIA cards from the old MICB card.
5. Transfer all PCMCIA cards to the new MICB card. Keep the packaging material from the new card.

   This procedure moves all software, configuration, and records to the replacement MICB card.
6. Transfer the Security Device from the old MICB to the replacement.

   The new card reuses the keycode. The keycode remains on the PCMCIA card, which was removed from the old MICB.
7. Enable the new card.
8. Package the old MICB card using the packaging material from the new card. Ship the card to the repair center.

This procedure is now complete

Error message handling

The MICB provides enhanced message handling that includes the following:

- Fixed message format and unique message codes.
- Categorization of messages by severity.
- Message analysis tool that provides on-line documentation.
- Message filtering based on such items as severity and firmware component.
- Advanced troubleshooting.

Note: Since the on-line documentation is always available and accurate according to the cards firmware version, this guide does not document specific error messages.

Error messages format

The general format of error messages is as follows:

<serial number> <severity> <error code> <timestamp> <error text>

Table 42 describes the error message fields.

Table 42
Error message field formats

Field	Description
<serial number>	Four digits that provide a sequence for the messages. It starts at 0001 at power-up and increments by one for each message issued. It wraps around when it reaches 9999.
<severity>	Severity levels are as follows: **CRITICAL** – indicates immediate corrective action is required (for example, the application cannot continue and/or the card must be restarted). **MAJOR** – indicates urgent corrective action is required (for example, the BUI doesn't work, but call processing continues to operate). **MINOR** – indicates the existence of a fault condition; corrective action should be taken to prevent a more serious fault. For example, a problem affecting a single channel is minor, so long as the system is still fully operational. **WARNING** – indicates a low level failure that almost does not impact a customer. No corrective action is required, because auto-recovery is performed. Frequent appearance can indicate a more serious problem. **INFO** – shows normal operational event notifications (for example, state changes in hardware or software; time and date changes). **DEBUG** – for use by designers only.
<error code>	Unique identifier of the event being reported. It is made up of the following two parts: • a string of up to six letters indicating the firmware component that originates the message. • three decimal digits comprising the error number within this component
<timestamp>	Date and time of the message in the format **MM-DD hh:mm:ss:ff**, where: MM = month number. DD = day of the month. hh = hour (in 24-hour format). mm = minutes. ss = seconds. fff = fraction of second, in milliseconds.
<error text>	Short description of the problem or event, and related parameters (for example, port number).

Error message procedures

Follow the steps in Procedure 25 to view the on-line error message documentation.

Procedure 25
Access the on-line error message analysis tool

1 Access the CLI **SM** directory and enter the following:

SHO

The CLI prompts you for to enter the error code.

2 Enter the error code for which you want information:

For example, enter:

MNGMMI109

Note: The letters are case sensitive and must be entered exactly as they appear in the error message.

The CLI prints the following related information about the message:

<Syntax> – definition of the message syntax.
Meaning – shows what the message indicates.
Parameters – description of the message parameters (fields).
Action – steps to follow to isolate the problem and/or fix it.
Impact – possible effects of the event.

This procedure is now complete

The entire file of error descriptions is available as a readable text. It can be retrieved from the MICB to a PC for off-line reference. Follow the steps in Procedure 26 to retrieve the error description file to a PC.

Procedure 26
Retrieve the entire error message file to a PC

1 The entire file of error descriptions is a readable text file. From your PC's desktop access FTP.

2 To download the entire file, enter the following path:

a:gnr\errors.txt

This procedure is now complete

The output of messages can be suppressed according to pre-defined criteria. This functionality enables a technician to focus on a specific group of messages to improve productivity. Messages that keep reappearing due to known circumstances which are not necessary to see can be suppressed.

The filtering criteria are as follows:

- Severity of messages – only messages with the selected severity levels appear. Any combination is possible.
- Firmware component – only messages with the selected firmware component appear. Any combination is possible.
- Detailing level:
  - — Low – the message appears without the <error text> part. The full description can be retrieved using the message analysis tool based on the error code.
  - — High – the full message appears.

All filtering criteria can be defined separately for appearance on the CLI and for storage in error log files (that is, a selected group of messages can be defined to appear in the CLI, but not in the error log, or visa versa).

Follow the steps in Procedure 27 to configure message filtering.

Procedure 27
Configure error message filtering

1 Access the CLI **SM** directory and enter the following:

ERR

The CLI displays command inputs in the following three sections:

- *FORMAT*
- *CLI_SEVERITY_FILTER*
- *DISK_SEVERITY_FILTER*

2 You can edit the values as per normal CLI usage.

Note: If you use the second level login command, two more filter sections are available: CLI_FW_COMPONET_FILTER and DISK_FW_COMPONENT_FILTER.

EXAMPLE:

ps

// technician enters err
// MICB displays section name and its parameters, and prompts for action:

```
section [FORMAT]
CLI error message format: long
Disk error message format: short  // default is long for both
Modify, Next section, Cancel:
```

n

// next: go to next section

```
section [CLI_SEVERITY_FILTER]  // filter CLI messages by severity
```

```
Critical: yes // yes means that the message will appear
MAJOR: yes
MINOR: yes
WARNING: yes
INFO: yes
DEBUG: yes
Modify, Next section, Cancel
```

n

// next: go to next section

```
section [DISK_SEVERITY_FILTER] // filter CLI messages in disk file
Critical: yes // yes means that the message will appear
MAJOR: yes
MINOR: yes
WARNING: yes
INFO: yes
DEBUG: yes
Modify, Next section, Cancel://
```

This procedure is now complete

Advanced troubleshooting

The MICB provides the following tools for technicians to troubleshoot and debug problems based on error messages:

- **Automatic trace back** – the system prints an automatic trace back list of predefined error codes. This feature helps software designers solve errors.
- **Automatic E-mail notification** – the system can send an E-mail notification containing a predefined list of error codes to the administrator, or other address.
- **Automatic card restart** – MIBC restarts can be performed for a predefined list of error codes. This feature enhances automatic recovery.

Note: All the actions defined above can be limited to a predefined number of occurrences, with a separate limit for each action.

Backup and restore procedures

Files can be backed up and restored from either the CLI or the Administration BUI.

Backup

An administrator schedules the backup from the administration BUI. Table 43 shows the items to consider when scheduling an automatic backup. Some of these items also apply to an immediate backup.

Table 43
Backup considerations

Item	Description
Content	Specify which of the following items to backup (the default is never; that is, no backup; however, if another option is selected in the “Schedule” section the default contents is data only): • **Data** – configuration, brandline greeting, and scheduling data (future conferences). • **Reports** – includes error logs. • **Customized greetings** – greetings for future meetings. Note, because this item can reach a large file size, a technician may prefer to exclude it.
Time	The database can be backed up immediately, or scheduled as a daily, weekly or monthly backup. For scheduled backups, determine the: • hour of the backup (hours only, no minutes) • day of the week, if weekly • day of the month, if monthly (1-28 only)
Destination	Backup files to one of the following destinations: • The secondary PCMCIA device, inserted in the upper slot of the MICB card. • A remote FTP server. The system compresses (zips) the backup files, before transferring them. Specify the server’s IP address, remote folder path, FTP login, and password for the remote server. The system names the ZIP file according to the date. It does not overwrite previous backups. ***Note:*** The remote folder must be an existing folder in the remote server; if this path is not found, the system puts the backup file in the folder reached directly by FTP. • An E-mail destination. The system compresses (zips) the backup files before sending them. The E-mail address is the same one the system uses for other administration E-mails (for example, reports and aged conferences).

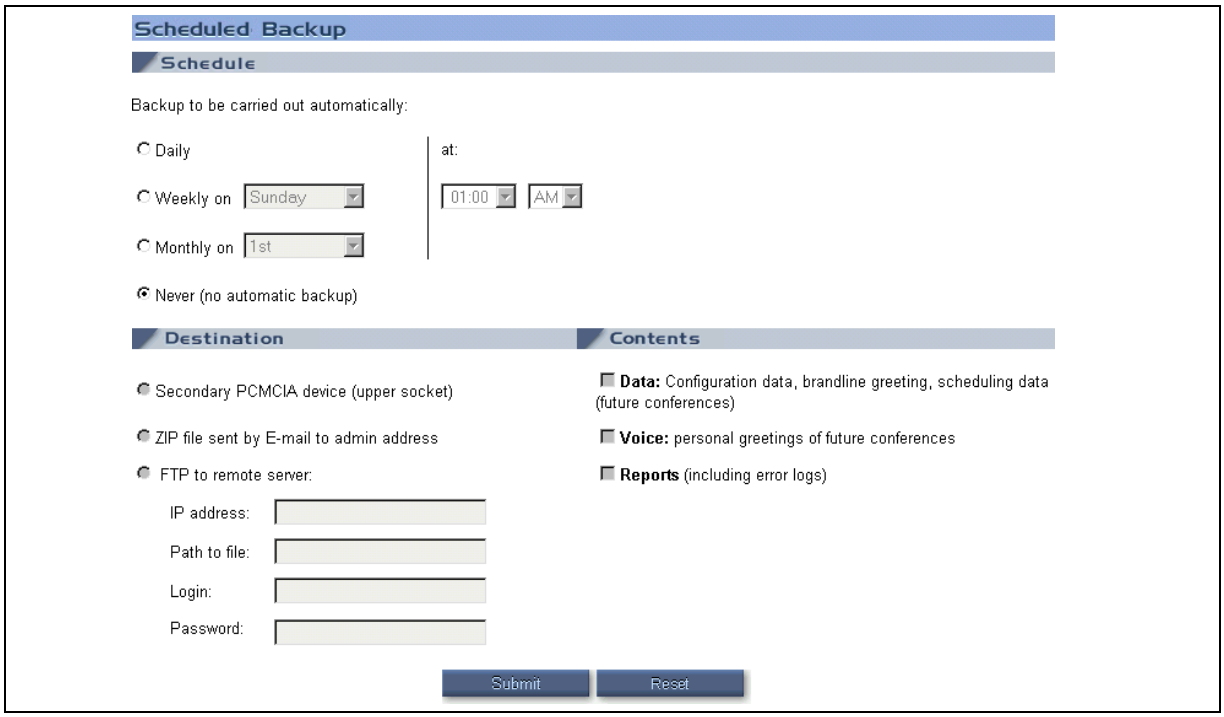
During the backup process the card remains operational. However, the system denies database changes and does not accept the following operations:

- setting up a new conference or modifying an existing conference (allows view only)
- recording a custom greeting
- making configuration changes, including users, always on meeting, and groups

Scheduled Backup

Figure 68 shows the Scheduled Backup window accessed from the MICB Dashboard. For more information about the MICB Dashboard, see "MICB Dashboard" on page 98.

Figure 68
MICB Dashboard – Scheduled Backup window



The administrator defines the time, destination and contents of the backup. Table 44 describes these three sections of the Scheduled Backup window.

Table 44
Scheduled Backup parameters

Section	Description
Schedule	Click on an radio button to define the backup schedule as follows: • **Daily** – every day at the hour specified. • **Weekly** – once a week on the specified day, at the specified hour. • **Monthly** – once a month on the specified day (1-28), at the specified hour. • **Never** – the system does not perform an automatic backup (the default). The hour section is to the round hour (that is, hh:00), AM or PM.

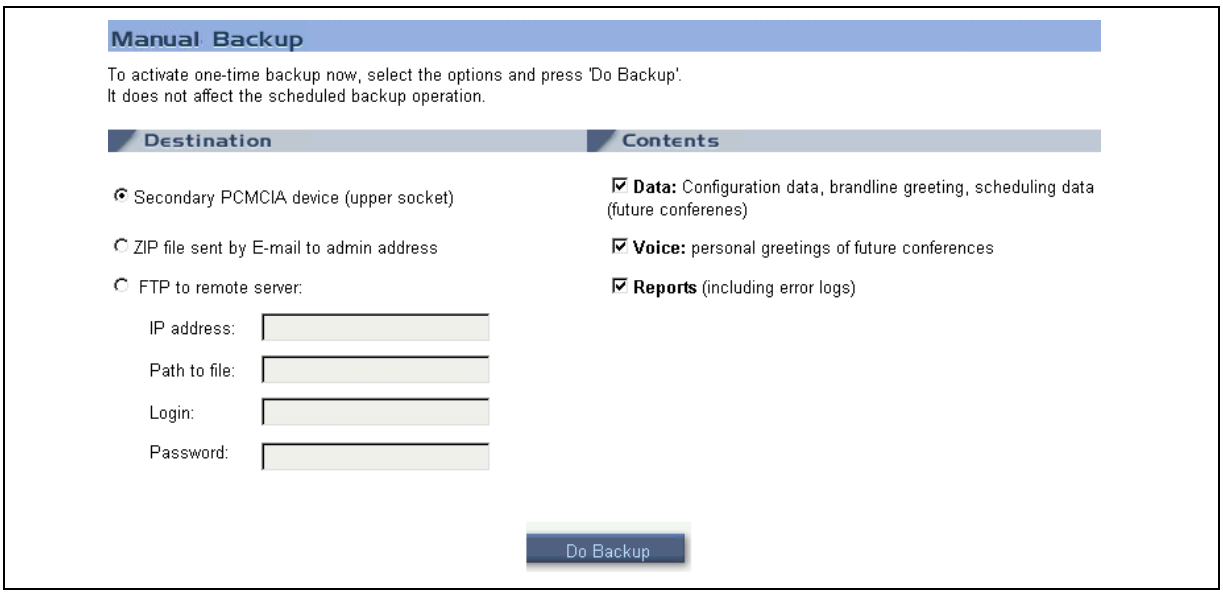
Table 44
Scheduled Backup parameters (Continued)

Section	Description
Destination	Click on an radio button to define the backup destination as follows: • The secondary PCMCIA device, inserted in the upper slot of the MICB card (the default). • An E-mail destination. The system compresses the backup files, before sending them. The administrator defines the Administrator's E-mail address in the General Setting window (see Figure 48 on page 99). • A remote FTP server. The parameters for the FTP session must be defined, as shown in the boxes below the FTP radio button. The system compresses the files, before transferring them. The system names the ZIP file according to date, so that it does not overwrite previous backups.
Contents	Click on one or more box as shown in the window to select the contents of the backup. Data is the default.

Manual Backup

An administrator uses the window in Figure 69 to perform a one-time, manual backup.

Figure 69
MICB Dashboard – Manual Backup window



The Destination and Contents sections are the same as for an automatic backup. Open A CLI window by clicking on the CLI button on the top frame of the dashboard. Click on the **Do Backup** button to activate an immediate backup according to your selected options.

Note: If the **Do Backup** button is clicked with no CLI window open, a pop-up message requests the administrator to open a CLI window.

View Backup History Log

The administrator can view a history log of past scheduled backups to make sure that the backups have taken place as scheduled. The Backup History Log window is a view-only window and shows each backup attempt as one line: time stamp (dd/mm/yyyy hh:mm:ss) and message. The message shows the type of backup (automatic or manual), destination, and success or failure. The events appear with the most recent backup on the top of the list.

View Last Backup Details

The Last backup Details view-only window prints out the details of the last backup attempt (either scheduled or manual). This is the same text that appears on the CLI during a backup.

Restore

Use Procedure 28 to restore the database from the secondary PCMCIA device.

Procedure 28
Restore the database from the secondary PCMCIA

1. Insert the PCMCIA device holding the backed up database in the MICB card's upper slot.
2. Use the CLI **REstordb** command in the SMaint directory.

   The system prompts you for the source of the restore.
3. Select **upper socket** and press the **Enter** key.

   The system restores the database.

This procedure is now complete

Use Procedure 29 to restore the database from a backed-up ZIP file.

Procedure 29
Restore the database from a backed up ZIP file

1. Determine which backed-up ZIP files to restore.
2. Name this file on the file server MICBDATA.ZIP.

3 Run the **REstordb** command with the parameter indicating this is a restore following an FTP download.

The system prompts for the source.

4 Select **FTP**.

The system prompts for the following parameters: IP address, path to file, login, and password.

5 Enter the information as appropriate and press the **Enter** key.

The system restores the data.

This procedure is now complete

During the restore process the card disables itself and does not answer calls. It also does not accept changes from the BUI.

Backup and restore process log

The backup process sends messages to the CLI window. The messages can be viewed while the process is running by accessing the CLI.

The system generates two files that contain information about the backup progress. The backup.log in the USER directory contains one line for each of the last backups, and restorations, up to a maximum of 20. Each line contains the following:

- a time stamp
- whether it was a manual or scheduled backup to
  - disk or
  - E-mail
- whether it was a restoration and from which source
- whether it was successful or failed

The LASTBKP.LOG file in the GNR directory provides a more detailed report. This file contains much of the information that the CLI prints while the process is running. The system keeps this file with the backup database, regardless of how the backup is performed. The system keeps this file on the primary PCMCIA along with the ZIP file, if the ZIP file is required to be saved. The LASTBKP.LOG file can be viewed at the received E-mail location.

Reports

Purpose

This chapter describes the reports that the MICB can generate.

The chapter contains the following sections:

- **“Overview” on page 161** – introduces the types of reports the MICB can generate and describes where to view them.
- **“Short Connection Report” on page 163** – describes the Short Connection Report.
- **“Meetings Log Report” on page 164** – describes the Meeting Logs Report.
- **“Overbooking Report” on page 166** – describes the Overbooking Report.
- **“Billing Report” on page 168** – shows how the MICB handles billing and describes the Billing Report.
- **“Maintenance (Error) Report” on page 175** – describes the Maintenance (Error) Report.

Overview

MICB can be viewed reports from the following:

- **BUI** – arranges report data as a table, in readable format, with column titles. The report can be copied to the local desktop as a raw format file. The report can be printed by using the browser’s print function.
- **CLI** – provides direct access to Short Connection, Meetings Log, and Maintenance reports.

The MICB keeps the files for 32 days or less, depending on the definition of the “report aging days” system attribute.

Note: Records related to dual-card meetings appear in the primary card only.

Table 45 describes the reports that the MICB generates.

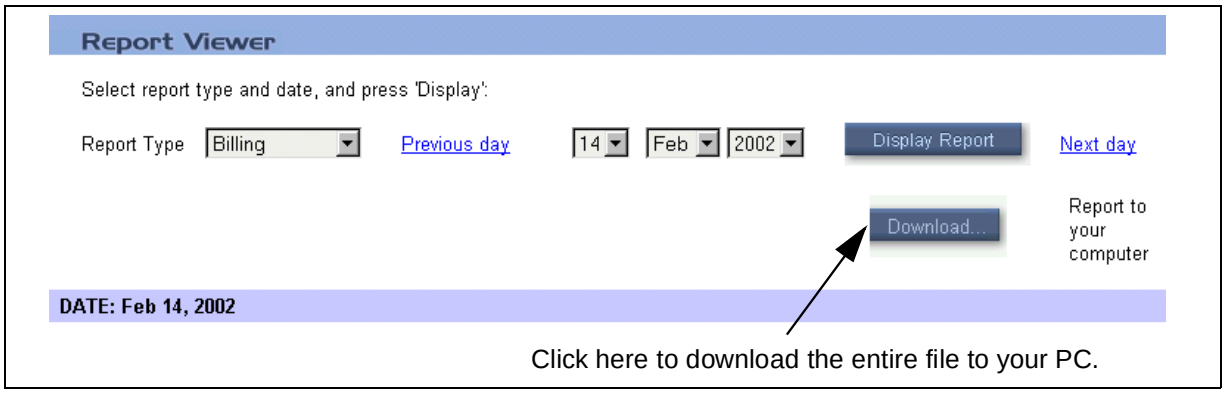
Table 45
Report summary

Report	Purpose	Raw Format	Display	
			CLI	BUI
Short Connection	Detect faulty behavior (users are not serviced).	not a file	SMaint/ SCon	Yes
Meetings Log	Conference activity log.	structured text (see note)	RGen/ MLog	Yes
Overbooking	Track actual usage of ports.	.CSV	N/A	Yes
Billing	Provide billing records.	.CSV	N/A	Yes
Maintenance (Error)	Logs errors.	text	SMaint/ MReport	Yes
Note: Text records have a fixed length of 1024 characters, padded with trailing spaces. The first record is binary.				

BUI Report Viewer

An administrator can view reports from the BUI. Click on **View a Report** on the MICB Dashboard to access the Report Viewer window (see Figure 70).

Figure 70
Report Viewer window



Select the report type from the pull-down menu on the left of the Reports Viewer window. Click on “Previous day” or “Next day” links to change the day of the report. Click on the **Display Report** button to view the report. The format of the report display varies depending on the report type.

An administrator can download the report to their PC by clicking on the **Download** button. The file downloads to the location defined in the local file selection dialog box of the Windows operating system.

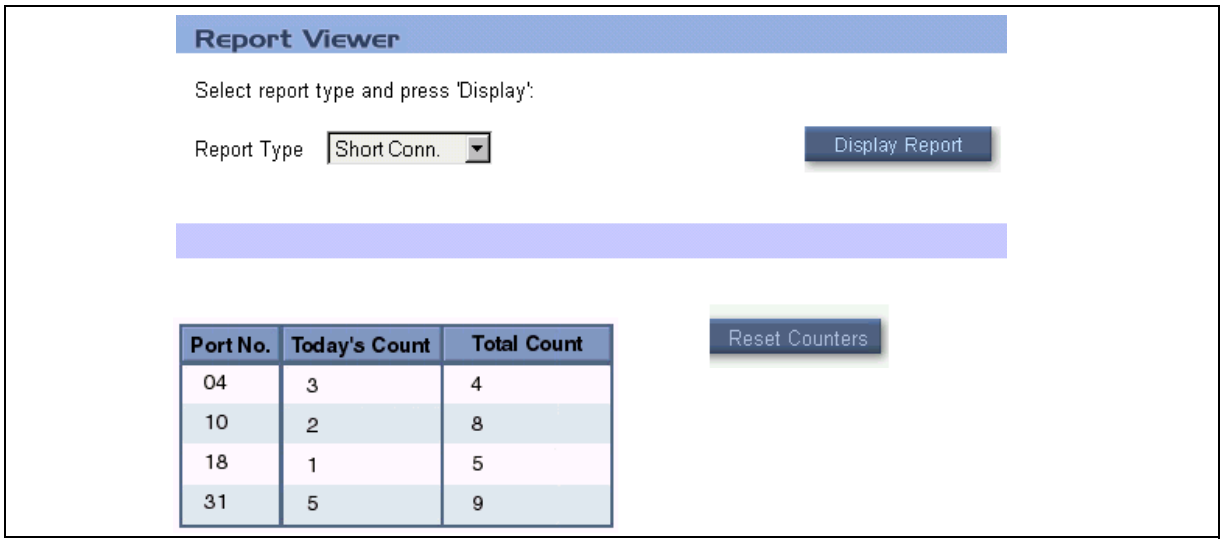
The following sections in this chapter show the report formats.

Short Connection Report

BUI Short Connection Report

Figure 71 shows how the Short Connection Report looks when accessed from the BUI.

Figure 71
Short Connection Report BUI example



Port No.	Today's Count	Total Count
04	3	4
10	2	8
18	1	5
31	5	9

The Short Connection Report always shows the current status; the date cannot be selected. The report displays the same text as what CLI displays after the **SMaint/SCon/Print** command. The window does not shows ports with all zero counters.

The **Reset Counters** button sets all counters back to zero (similar to the CLI **SMaint/SCon/Reset** command).

CLI Short Connection Report

Use the Short Connection Report menu to present or reset the short connection peg-count.

To access the Short Connection Report menu, login as an administrator. Enter the System Maintenance command (**sm**, **SM**, or **SMaint**) and enter the Short Connection Report command (**sc**, **SC**, or **SCon**).

Short port occupancy can indicate a fault condition on a port or can indicate that a user is dialing the incorrect DN. Set the short occupancy range in the System Attributes Editor menu, which can range from 0 to 30 seconds.

From the Short Connection Report menu, the option is available to print (p) or reset (r) the counter to zero. When printing the short connection peg-count, the system presents all ports with a count in the following format:

port # today's_count total_count

The counts have the following meanings:

- **today's count** – count of short connections that occur this day.
- **total count** – cumulative count of all short connections since the MICB was last reset, or the system reset the short connection counters.

If all counters are zero, the system prints the header followed by the message "all counters are zero".

Short Connection Report CLI example

```
STest, MReport, SCon, ARchivdb, REstordb, CRestart, ?: sc
Print, Reset: p

Port #     today's_count    total_count
10              2                4
18              1               10
31              5               34

Print, Reset: r
Reset all short connection counters? (Yes, (No)) Yes
Counters reset.
Print, Reset: *
STest, MReport, SCon, ARchivdb, REstordb, CRestart, ?:
```

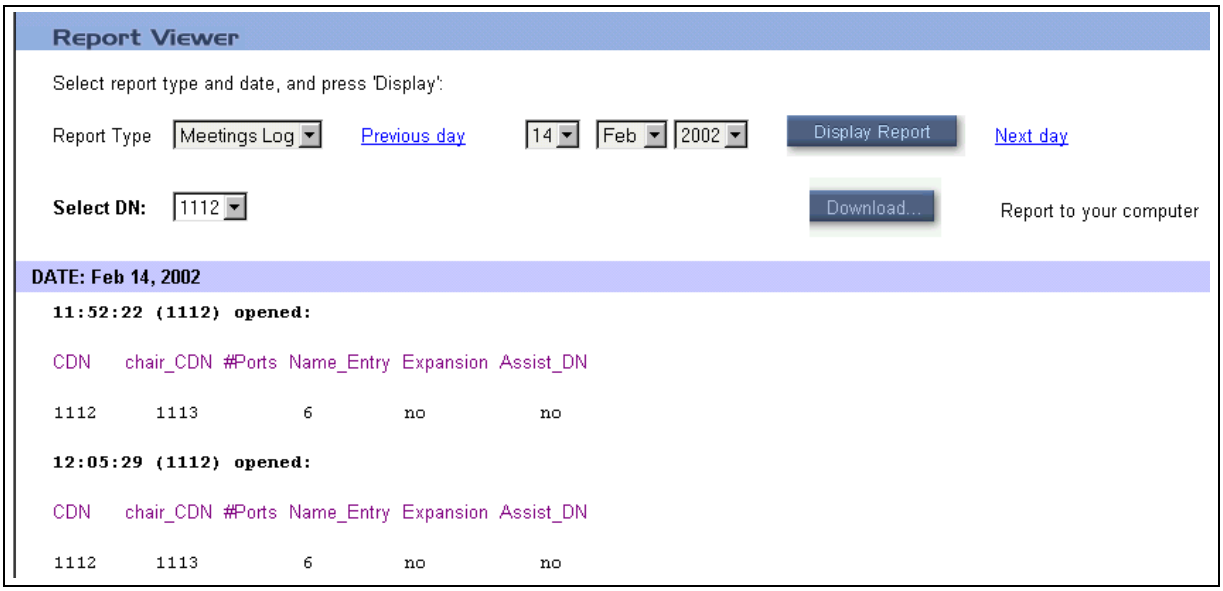
Meetings Log Report

BUI Meetings Log Report

The BUI sorts the Meetings Log Report by DN. The BUI displays the report with events grouped by meeting. Therefore, the window shows a "Select DN" pull-down menu to enable the selection of the particular DN's records to appear in the report. Figure 72 on page 165 shows how the BUI displays the report, which has the same text lines that the CLI prints when **RGen/MLog** is entered. The BUI adjusts the font to make this report easier to read.

If the report does not fit on one window, click on the **Next Page** button to display more information.

Figure 72
Meetings Log Report BUI example



CLI Meetings Log Report

The CLI Meeting Log Browser menu displays a log of conference events for a specified date. After the system displays data, it returns to the year-month-day prompt using the last selected date as default. To interrupt the log display, enter ***** and press the **Enter** key.

Each event report starts with the time stamp and the main DN in the following format:

hours:minutes:seconds (DN) <description of event>

The date selected to display the conference log must be in the past.

The system deletes old log files after exceeding the predefined report aging time. The system indicates if there are no log files for the specified date. To access the Meeting Log Browser menu, login as an operator or administrator. Enter the Report Generation command (**rg**, **RG**, or **RGen**) and enter the Meeting Log Browser command (**ml**, **ML**, or **MLog**).

Meetings Log Report CLI example

```
Log: ml
year (1996): 1995
month (02): 03
day (20): 15
14:55:06 (2230) opened:
DN    chair_DN    #Ports    Name_Entry    Expansion    Assist_DN
```

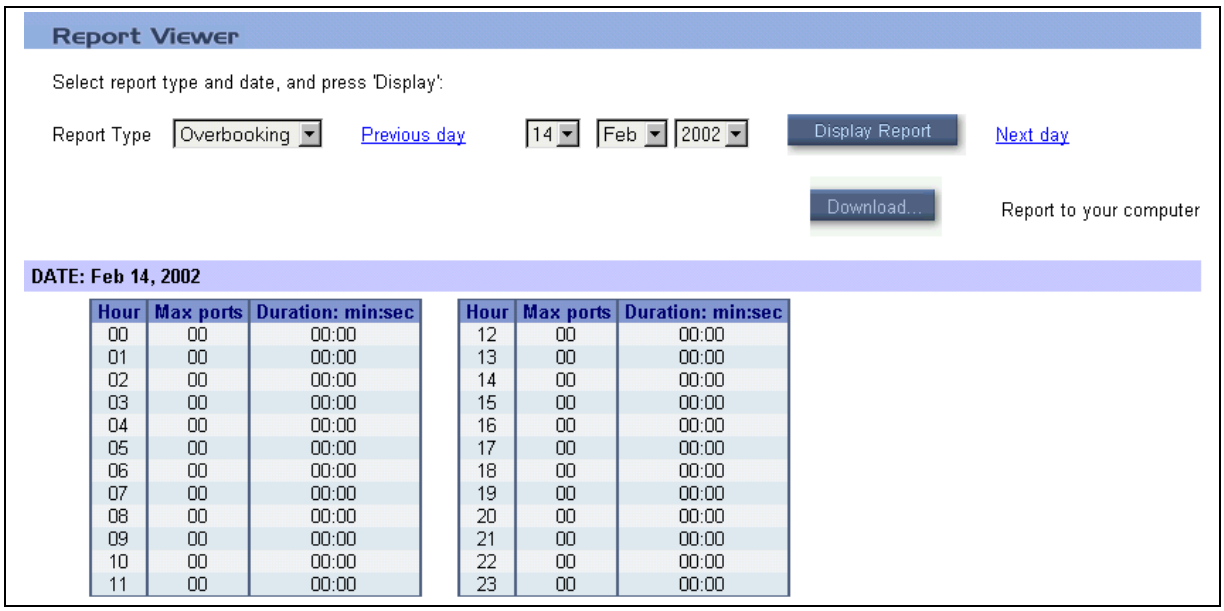
```
2230 2001        3        yes                no        1000

15:00:45 (2220) expanded
15:01:00 (2220) entry: 24        //Conferee entered conference on port 24//
15:03:23 (2230) ch_entry: 4        //Chair joined conference on port 4//
15:03:56 (2220) exit: 14        //Conferee left conference from port 14//
16:35:09 (2230) mmi_op lock        //Conference locked//
16:44:15 (2220) mmi_op unlock        //Conference unlocked//
16:45:00 (2220) closed
16:56:02 (2230) ch_com dial_out: 395945        //Chair dials out DN//
16:57:00 (2230) ch_com return        //Chair returns without called party//
16:58:20 (2230) ch_com redial: 395945 //Chair redialed last dialed DN//
16:59:16 (2230) ch_com ret with_party //Chair returns with called party/
16:58:45 (2230) ch_com count        //Chair counts conferees//
17:00:54 (2230) mmi_op num_of_ports: 2        //New number of ports is 2//
17:01:44 (2230) mmi_op duration: 4:00        //New duration is 4 hours//
17:02:54 (2230) mmi_op expansion: yes        //Port expansion is allowed//
17:03:45 (2230) ch_com lock        //Chair locks conference//
17:05:45 (2230) ch_com unlock        //Chair unlocks conference//
17:08:26 (2230) ch_com drop last d_in        //Drops last dial in conferee//
17:08:56 (2230) ch_com drop last d_out        //Drops last dial out conferee//
17:09:16 (2230) ch_com drop all        //Chair drops all conferees//
```

Overbooking Report

BUI Overbooking Report

Figure 73 shows how the Overbooking Report appears when accessed from the BUI.

Figure 73
Overbooking Report BUI example



Hour	Max ports	Duration: min:sec
00	00	00:00
01	00	00:00
02	00	00:00
03	00	00:00
04	00	00:00
05	00	00:00
06	00	00:00
07	00	00:00
08	00	00:00
09	00	00:00
10	00	00:00
11	00	00:00

Hour	Max ports	Duration: min:sec
12	00	00:00
13	00	00:00
14	00	00:00
15	00	00:00
16	00	00:00
17	00	00:00
18	00	00:00
19	00	00:00
20	00	00:00
21	00	00:00
22	00	00:00
23	00	00:00

The table in the report shows the contents of the Overbooking Report which the BUI translates from a .CSV file. The columns in the table are as follows:

- **Hour** – The hour of the day, from 0 to 23 where:
  - 00 = 0:00 o'clock to 1:00 o'clock
  - 01 = 1:00 o'clock to 2:00 o'clock etc.
- **Max Ports** – The maximum ports busy, by actual calls, during this hour.
- **Duration: min:sec** – The total duration in which all ports are busy during this hour. When the value is greater than 0, the value in the "Max Ports" column shows that card's capacity. The duration field in .CSV format appears as two separate columns; the BUI combines the columns for easy viewing.

There is one line in the table for each hour of the day, so this window does not require a **Next Page** button.

Overbooking Report (.CSV)

The system generates the Overbooking Report on a daily basis. Each line of the over-booking report contains the following information:

- 1st field: hour (00-23)
- 2nd field: maximum number of ports (00-32)
- 3rd field: duration in minutes (00-60)
- 4th field: duration in seconds (00-59)

The total number of lines is 26. The first line is for the date, the second line is for the field names, and 24 lines are for every hour as follows:

```
DATE: <month name> dd yyyy,,,
hour,max ports,duration minutes,duration seconds
00,<max port>,<duration minutes>,<duration seconds>
01,<max port>,<duration minutes>,<duration seconds>
02,<max port>,<duration minutes>,<duration seconds>
03,<max port>,<duration minutes>,<duration seconds>
04,<max port>,<duration minutes>,<duration seconds>
05,<max port>,<duration minutes>,<duration seconds>
06,<max port>,<duration minutes>,<duration seconds>
07,<max port>,<duration minutes>,<duration seconds>
08,<max port>,<duration minutes>,<duration seconds>
09,<max port>,<duration minutes>,<duration seconds>
10,<max port>,<duration minutes>,<duration seconds>
11,<max port>,<duration minutes>,<duration seconds>
12,<max port>,<duration minutes>,<duration seconds>
13,<max port>,<duration minutes>,<duration seconds>
14,<max port>,<duration minutes>,<duration seconds>
15,<max port>,<duration minutes>,<duration seconds>
16,<max port>,<duration minutes>,<duration seconds>
```

17,<max port>,<duration minutes>,<duration seconds>
18,<max port>,<duration minutes>,<duration seconds>
19,<max port>,<duration minutes>,<duration seconds>
20,<max port>,<duration minutes>,<duration seconds>
21,<max port>,<duration minutes>,<duration seconds>
22,<max port>,<duration minutes>,<duration seconds>
23,<max port>,<duration minutes>,<duration seconds>

Billing Report

Introduction

Users can be charged for conference reservations and dial-out calls during a conference. The system stores billing reports in database files which can be retrieved from the card by FTP. Dial-out calls must be charged through the Meridian system billing records.

Billing charges are based on the following:

- The duration of the meeting, including any extension of the conference from either the BUI or by the chairperson using the **98* command from the keypad.
- The number of ports booked for the meeting. The figure includes any increase in the number of ports during the conference from the BUI or a port increase provided automatically by the MICB.

Note: The system charges users for the number of ports booked for the conference. This charge does not depend on how many conferees participated in the meeting or the duration of each input call.

BUI configuration

The Billing Account ID for every user must be defined through the MICB Dashboard (see "Users List" on page 107). The Billing Account ID is the account number of the user, up to nine digits, for billing purposes. This number appears in MICB billing reports for conferences owned by the user.

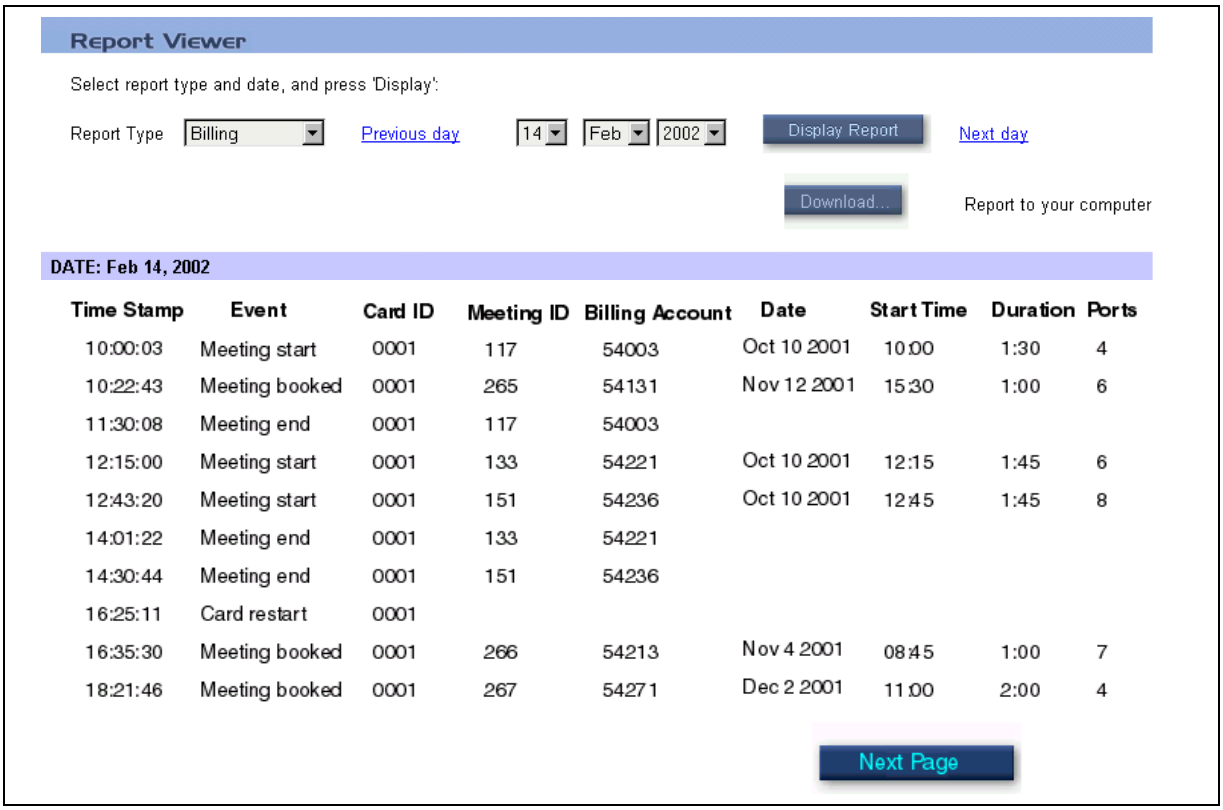
The following options are available for generating billing reports (see "General Settings window" on page 99):

- **No billing** – the system does not generate billing reports.
- **Billing Reports** – the system generates billing reports.
- **Billing Reports & CDR** – the system generates billing reports and Call Detail Records. This option is only available on the Meridian 1.

BUI Billing Report

Figure 74 shows how the Billing Report appears when accessed from the BUI. The table in the window shows the contents of the Billing Report which the BUI translates from the .CSV file.

Figure 74
Billing Report BUI example



Time Stamp	Event	Card ID	Meeting ID	Billing Account	Date	Start Time	Duration	Ports
10:00:03	Meeting start	0001	117	54003	Oct 10 2001	10:00	1:30	4
10:22:43	Meeting booked	0001	265	54131	Nov 12 2001	15:30	1:00	6
11:30:08	Meeting end	0001	117	54003				
12:15:00	Meeting start	0001	133	54221	Oct 10 2001	12:15	1:45	6
12:43:20	Meeting start	0001	151	54236	Oct 10 2001	12:45	1:45	8
14:01:22	Meeting end	0001	133	54221				
14:30:44	Meeting end	0001	151	54236				
16:25:11	Card restart	0001						
16:35:30	Meeting booked	0001	266	54213	Nov 4 2001	08:45	1:00	7
18:21:46	Meeting booked	0001	267	54271	Dec 2 2001	11:00	2:00	4

The “Event” field values appear as code numbers in the .CSV file. In the BUI, the system displays them as event names.

If the report does not fit on one window, click on the **Next Page** button to display more information.

Billing Report (.CSV)

The system saves MICB Billing Reports automatically in files on a daily basis. These files use the a:\OAM\BILLING directory on the PCMCIA for the period defined by the report aging feature. The default period is 32 days.

The file's names consist of capital letter "B" and the date of the report (year, month and day) in the following format: Byyymmdd and have the extension CSV, where:

- **yyy** – indicates the year (for example, "099" for 1999, "100" for 2000, "101" for 2001).
- **mm** – indicates the month
- **dd** – indicates the day

For example, B0990720.CSV has the Billing Report for July 20, 1999 and B1010203.CSV contains the Billing Report for February 03, 2001.

Note: To retrieve billing files, transfer the files by FTP over the TCP/IP LAN using a fixed password.

Each Billing Report consists of 14 fields separated by commas. Table 46 shows the information that the Billing Report contains.

Table 46
Billing Report contents

Field	Contents
1st	Time stamp in hours (00-23).
2nd	Time stamp in minutes (00-59).
3rd	Time stamp in seconds (00-59).
4th	Event as follows: **1** Meeting booked **2** Meeting modified **3** Meeting start **4** Active meeting modified **5** Meeting cancelled before being started **6** Active meeting cancelled (after being started) **7** Meeting schedule time has ended 8 Card restart
5th	Card ID (up to a four-digit number).
6th	Meeting ID (up to a 10-digit number).
7th	Billing account (up to a nine-digit number).
8th	Meeting date.
9th	Meeting start time in hours (00-23).

Table 46
Billing Report contents (Continued)

Field	Contents
10th	Meeting start time in minutes (00-59).
11th	Meeting start time in seconds (00-59).
12th	Duration in hours (01-12).
13th	Duration in minutes (00-59).
14th	Ports (02-40).

Note: For a permanent bridge the meeting date, start time, and duration fields are irrelevant and always appear as zero. The first line is for the date, the second line is for the field names, and all other lines are for the events.

The daily billing report format is as follows:

```
DATE: <month name> dd yyyy,,,,,,,,,,,,
<1st field name>, <2nd field name>,.....,<14th field name>
<1st field>,<2nd field>,....,<14th field>
<1st field>,<2nd field>,....,<14th field>
<1st field>,<2nd field>,....,<14th field>
<1st field>,<2nd field>,....,<14th field>
```

BIlling Report .CSV example

In this example, the meeting ID is 32, user billing account is 999, and card ID is 7.

```
First line – at 8am meeting has been booked to start on Aug 8 1998 at 10:30am,
    duration of 02:15, 6 ports.
Second line – at 9am meeting modified to 8 ports.
Third line – at 10.28am meeting started.
Fourth line – at 11am active meeting modified to 3 hours duration.
Fifth line – at 01:28pm meeting ended (time has ended).
Sixth line – at 04:00pm card restarted.
DATE: Aug 7 1998
time stamp hours, time stamp minutes, time stamp seconds, event, card ID,
meeting ID, billing account, date, start time hours, start time minutes, start time
seconds, duration hours, duration minutes, ports
08,00,00,01,7,32,999,Aug 8 1998,10,30,00,02,15,06
09,00,00,02,7,32,999,Aug 8 1998,10,30,00,02,15,08
10,28,00,03,7,32,999,Aug 8 1998,10,30,00,02,15,08
11,00,00,04,7,32,999,03,00,08
```

A billing file includes the following records:

- Date stamp, for example: DATE: Aug 7 1998
- Header: time stamp hours, time stamp minutes, time stamp seconds, event, card ID, meeting ID, billing account, date, start time hours, start time minutes, start time seconds, duration hours, duration minutes, and ports
- Billing event record

Table 47 shows example billing records for all events. The card ID is 1234 and the user's billing account is 999.

Table 47
Event examples

Example	Description
Meeting Booked – In this example, the time stamp, card ID, meeting ID, billing account, start time, duration, and ports information was available.	
08,00,00,01,1234,7,999,Aug 8 1998,10,30,00,02,15,06	This record indicates that the meeting has been booked at 8 am to start on August 8 1998 at 10:30 am, duration 2 hours 15 minutes, with 6 ports.
Meeting Modified – In this example, the time stamp, card ID, meeting ID, billing account, start time, duration, and ports information was available.	
09,00,00,02,1234,7,999,Aug 8 1998,10,30,00,02,15,08	This record indicates that a BUI user changed the meeting to include eight ports at 9 am, before the meeting began.
Meeting Started – In this example, the time stamp, card ID, meeting ID, billing account, start time, duration, and ports information was available.	
10,28,00,03,1234,7,999,Aug 8 1998,10,30,00,02,15,08	This record indicates that the meeting started at 10:28 am. ***Note:*** The meeting's start time is 10:28 am and not 10:30 am as scheduled. Meetings always start two minutes before the scheduled start time to guarantee timely entry of users.
Active Meeting Modified – In this example, the time stamp, card ID, meeting ID, billing account, duration, and ports information was available.	
11,00,00,04,1234,7,999,03,00,08	This record indicates that at 11 am a user expanded the duration of the active meeting to three hours. The original duration was 2 hours 15 minutes.

Table 47
Event examples (Continued)

Example	Description
Meeting Ended – In these examples, the time stamp, card ID, meeting ID, and billing account information was available. Examples report this event for three different cases:	
The meeting was cancelled before it began. 10,05,00,05,1234,7,999,00	This record indicates that a user cancelled the meeting reservation at 10:05 am from the BUI, before the scheduled start time. The number of ports is 0, because none of participants entered the meeting.
The active meeting was cancelled after it began. 12,48,00,06,1234,7,999,06	This record indicates that the meeting ended at 12:48 pm from the BUI, before the scheduled meeting time elapsed. The number of ports shows how many participants entered the conference. This number can be greater than the number of ports booked for the meeting, because the meeting person booking the meeting enabled the option for expansion.
The meeting's scheduled time elapsed. 13,28,00,07,1234,7,999,10	This record indicates that the meeting ended at 01:28 pm, because the scheduled time elapsed. The number of ports shows how many participants entered the conference. This number is greater than the number of ports booked for the meeting, because of expansion during the meeting.
Card Restarted – In this example, the time stamp, and card ID information was available.	
16,08,30,**08**,1234,	This record indicates that there was a card restart at 16:08:30. The event ID appears in bold letters. 1234 is the card's ID, 7 is the meeting's ID, and 999 is the customer's billing ID.

Meridian 1 Call Detail Recording

The Call Detail Recording (CDR) feature enables the MICB to charge users for out-going calls based on CDR reports the Meridian 1 system generates. The reports are generated even if the call is unanswered. The Meridian 1 must have the following software packages: Call Detail Recording (CDR) package 4; and CDR with Charge Account (CHG) package 23.

Note: CDR is not available on the Meridian SL-100.

To enable the CDR feature, select "Billing and CDR Reports" from the Billing options pull-down menu in the MICB Dashboard – General Settings window (see Figure 48 on page 99).

Charge Account feature

To define the CDR with Charge Account feature, refer to *Meridian 1 Call Detail Recording* and *Meridian 1 X11 Features and Services*.

When a user dials out with the Billing and CDR Reports option selected, the MICB card takes the Charge Account key (consisting of the first eight digits of the user's account ID), the call ID, and the meeting ID from the charge account field for the CDR record.

The Charge Account key

In the Meridian 1, the Charge Account key for every port of the MICB card must be defined in LD 11 (see Table 48 for an example).

Table 48
LD 11 – Define the Charge Account key for an MICB port

Prompt	Response
REQ	chg
TYPE	4 0 2 0
TYPE	2616
TN	4 0 2 0
ECHG	yes
ITEM	key 9 chg

CDR record format

CDR records are printed on Meridian 1 system TTY terminal defined as a CDR user. When defining the CDR with Charge Account feature, the Charge Account data is included in CDR records for each MICB outgoing call, as in the following examples:

1. The following record appears on CDR TTY as outgoing call is started:

   C 040 00 5211 T095019 1203 11.25 0000009991234000000007

   & 0000 0000

   where:

   first 9 digits: 000000999 is the billing account,
   next 4 digits: 1234 is the card ID,
   next 10 digits: 0000000007 is the meeting ID.

2. The following record appears on CDR TTY as outgoing call is ended:

   N 041 00 5211 T095019 1203 11.47 00:22:08 A 333

   & 0000 0000

CDR example scenarios

The conference call was booked using the BUI by a user whose billing account is 9134513, on July 19, 1999 at 06:15 p.m., for July 20, 1999 from 08:00 a.m. to 09:00 a.m. The number of ports booked is six.

The conference call was started as scheduled on July 20, 1999 two minutes before 08:30 a.m. During the call at 08:36 a.m. (after eight minutes), the chairperson calls out once to a long distance number and brings a user into the call. After 47 minutes the dialed out person drops off. No record is stored in the MICB card in relation to this event.The following record appears in the Meridian 1 CDR:

C 040 00 5211 T095019 20/07 08:36 00913451312340000000007
& 0000 0000
N 041 00 5211 T095019 20/07 09:23 00:47:08 A 333
& 0000 0000

At 08:55 a.m. the chairperson calls out to a long distance number and after two minutes returns to the meeting without the dialled party. The following record appears in the Meridian 1 CDR:

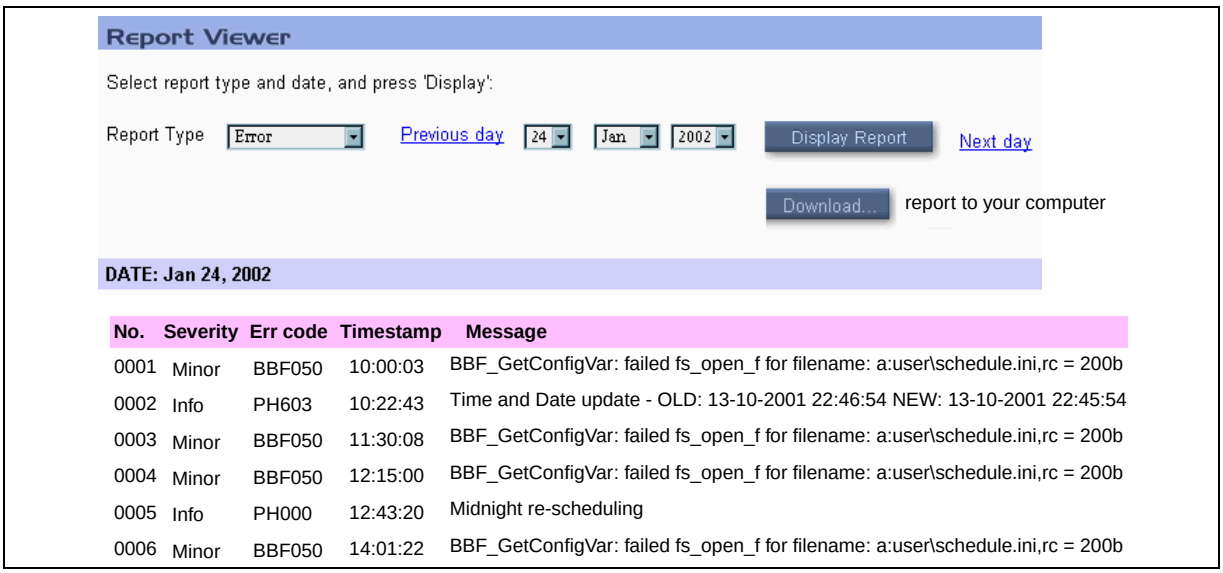
C 040 00 5215 T095019 20/07 08:55 00913451312340000000007
& 0000 0000
N 041 00 5215 T095019 20/07 08:57 00:02:12 A 333|
& 0000 0000

Maintenance (Error) Report

BUI Maintenance (Error) Report

Figure 75 shows how the BUI Maintenance Report.

Figure 75
Maintenance (Error) Report BUI example



No.	Severity	Err code	Timestamp	Message
0001	Minor	BBF050	10:00:03	BBF_GetConfigVar: failed fs_open_f for filename: a:user\schedule.ini,rc = 200b
0002	Info	PH603	10:22:43	Time and Date update - OLD: 13-10-2001 22:46:54 NEW: 13-10-2001 22:45:54
0003	Minor	BBF050	11:30:08	BBF_GetConfigVar: failed fs_open_f for filename: a:user\schedule.ini,rc = 200b
0004	Minor	BBF050	12:15:00	BBF_GetConfigVar: failed fs_open_f for filename: a:user\schedule.ini,rc = 200b
0005	Info	PH000	12:43:20	Midnight re-scheduling
0006	Minor	BBF050	14:01:22	BBF_GetConfigVar: failed fs_open_f for filename: a:user\schedule.ini,rc = 200b

The Maintenance (Error) Report appears in the table in this window. The window shows the same text lines as those generated by the CLI **SMaint/MReport** command.

If the report does not fit on one window, click on the **Next Page** button to display more information.

For more information about how the MICB handles error reporting, see "Error message handling" on page 151.

CLI Maintenance (Error) Report

The Maintenance Report Browser menu enables maintenance reports to be displayed according to date. These reports analyze system problems based on error messages compiled on that date. To access the Maintenance Report Browser menu, login as the administrator. Enter the System Maintenance command (**sm**, **SM**, or **SMaint**) and enter the Maintenance Report Browser command (**mr**, **MR**, or **MReport**).

All reports are time stamped and contain information about the cause of the problem. After the system displays the data, it returns to the "year-month-day" prompt using the last selected date as default.

The selected date must be in the past. The system discards old files that exceed the report aging number of days. If the date entered is too old, an error message appears. If the date is within the correct date range, but there are no report entries for that day, a message indicating there are no messages appears. To interrupt the report display, enter ***** and press the **Enter** key.

The maintenance reports have the following format:

<serial number>: <MON_REPORT_ID> <channel #> <time> <Applic_Manager_cycle> <Message Body>

Maintenance Report (Error) CLI example

The following example displays the maintenance report for March 15, 1996:

```
STest, MReport, SCon, ARchivdb, REstordb, CRestart, ?: mr
year(1996): 1996
month (11): 03
day (22): 15
1234:timer101 ch01 16:16:18:111 9000 "Num: 100 Timing Stop. 00."
1235: sig100 ch00 16:17:05:234 9900 "SIG: Q_APP in msg:0000005A"
0001:HW PCMCIA001 ln0077 ch01 16:25:29:836 PCMCIA card
inserted in socket 1
year (1996): .
STest, MReport, SCon, ARchivdb, REstordb, CRestart, ?:
```

Upgrades

Purpose

This chapter provides procedures for upgrading your system to MICB 3 from previous releases and for upgrading sub-issues of MICB 3. The chapter contains the following sections:

- **“Overview” on page 177** – introduces the MICB upgrade strategy.
- **“Planning for an upgrade” on page 179** – provides information to help prepare for an upgrade.
- **“Upgrade procedures” on page 180** – provides system upgrade procedures.

Overview

The MICB can be upgraded to MICB 3 from MICB 2, but not from MICB 1. An MICB 2 can be upgraded running on the card version AC on the same card. If upgrading from an older version (that is, AA or AB), the card must be replaced with vintage AC. A new keycode is required when upgrading from MICB 2 to MICB 3. Table 49 shows the upgrade paths regarding the conversion of hardware and customer data.

Table 49
MICB upgrade paths

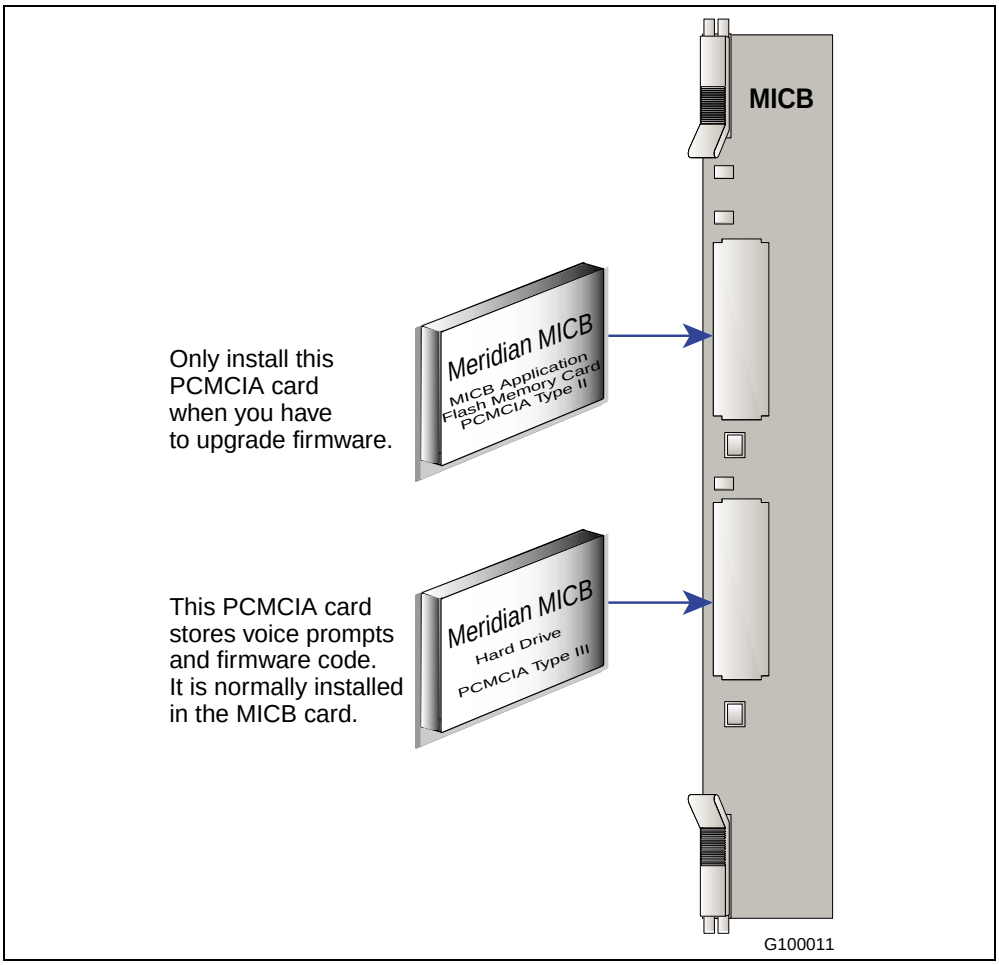
From ...		Upgrade	
NT5D51 Vintage	**Firmware**	**Same hardware**	**Data conversion**
AC	MICB 2	Yes	Yes
AB	MICB 2	No	Yes
AB	MICB 1	No	No
AA	MICB 1	No	No

Note: There is no upgrade from MICB 1 to MICB 3. This is the same as a new installation.

Insert a PCMCIA card into the top PCMCIA slot accessible through the MICB faceplate for external memory expansion, new voice announcements, and firmware upgrades.The available storage for voice prompts on the PCMCIA disk is 130 Mbytes, providing 260 minutes of voice recording. The MICB uses the PCMCIA ATA, Type II and Type III Flash cards for MICB software upgrade and backup.

The MICB card has two PCMCIA sockets. PCMCIA hard drive cards store MICB voice prompts and firmware code. The MICB ships with the PCMCIA hard drive. The bottom socket houses the PCMCIA hard drive card that contains the current firmware and customer data. Use the top socket to upgrade the firmware. Figure 76 shows how to load PCMCIA cards into the MICB faceplate slots to upgrade the MICB capacity.

Figure 76
Installing a PCMCIA card into the MICB faceplate slot



Keycode security

A keycode protects against unauthorized MICB feature use. The keycode restricts upgrades of either the number of ports or application software to a given MICB card. Nortel Networks tracks the keycodes to allow for accurate handling of field repairs and incremental upgrades.

Keycodes are required for the following upgrades:

- feature enhancements
- new applications
- port additions

Keycodes are not required for the following:

- backup and restore operations
- application patching/bug fix

Nortel Networks provides the customer with a keycode to enable installation of any required upgrade. Enter the keycode using the Command Line Interface from the local maintenance port on the MICB card. The keycode is 24 characters long; enter it in three sets of eight digits each called keycode1, keycode2, and keycode3.

Planning for an upgrade

When preparing for an upgrade, consider the following items:

- Always back up the site data, before beginning an upgrade.
- The BUI IP address will change during a card upgrade. Make sure that you are using the new MICB IP address entered from the maintenance terminal when accessing the BUI after an upgrade.
- The password policy has been modified for MICB3. For more information, see “Appendix A: Password security” on page 187.
- If the upgrade requires the replacement of an NT5D51AB card with an NT5D51AC card, the card should be replaced first. The new card must be tested with Release 2 software. Once the tests are completed, the MICB can be upgraded to Release 3.

Managing the user community during an upgrade

An important part of planning an upgrade is managing the user community. Table 50 lists items that will impact the user community during an upgrade to MICB3.

Table 50
User community upgrade considerations

Item	Description
BUI access	Users need to know how to reset their browser to access the MICB and when to do that. This is required because the address they previously used in the browser to access MICB had an extension of micb.htm. Users need to remove the extension.
User training	Provide users with the *MICB3 User Guide* and information about the following: • Custom greeting. • How to access and use chairperson control. • How to delegate chairperson control (that is, acquire and release chairperson control). • Volume control. How to use the feature from the TUI or the BUI control screen. • If single DN access is to be implemented, the changes to existing conferences (that is, already booked) and future meetings need to be communicated to the users.
E-Mail format	Changes to the E-Mail format should be reviewed and made visible to people who will be creating meetings.

Upgrade procedures

Card upgrade

Use Procedure 30 to upgrade your MICB card from Release 2 to Release 3.

Procedure 30
MICB 2 to MICB 3 card upgrade

1. Disable the operational MICB 2 card.

   Note: Meridian SL-100 customers must Bsy the MICB card at the PM level, before starting the procedure and RTS the card once the upgrade is complete.

2. Remove the MICB 2 PCMCIA from the lower socket.
3. Insert a new MICB 3 PCMCIA in the lower socket. This PCMCIA should be as shipped from the factory, with no customer data on it.
4. Reset the card by pulling it out and plugging it back in.
5. Enter the new keycode.

6 When the card is activated as MICB 3, enter the CLI and login as an administrator. Enter:

name: **admin**
Password: **<CR>**

Where CR is an empty password.

7 Insert the old MICB 2 PCMCIA in the upper socket.

8 From the CLI enter:

sm and then **convert**

The MICB copies the data from the upper PCMCIA, converts to MICB 3 format, and stores it in the lower PCMCIA.

Note: If the conversion is done from a primary or secondary MICB 2, the system does not copy “administrator” users. Instead the system creates one default administrator, “admin” with a password of “000000”.

9 Remove the PCMCIA from the upper socket. Nortel Networks recommends that you keep it, in case the customer wants to revert back to MICB 2.

10 You can now enter the administration BUI to review or modify parameters and options.

11 Enable the card.

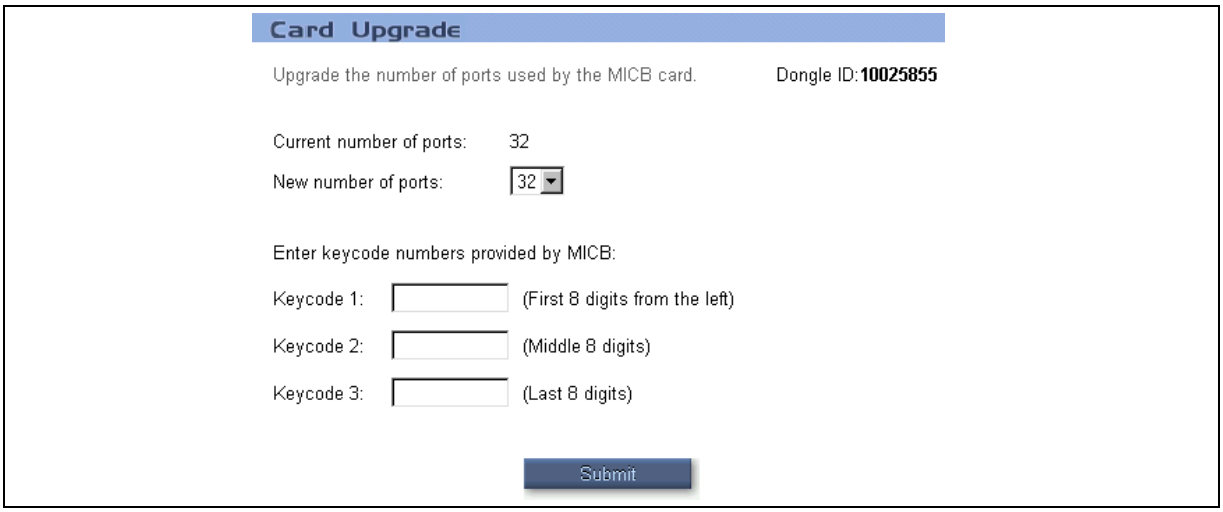
This procedure is now complete

Port Upgrade

The MICB card can be configured to have port sizes ranging from 12 to 62; however, systems requiring more than 32 ports require a dual-card configuration. To activate a different number of ports than currently active, login to the BUI as an administrator. Keycodes are required. Under the Upgrades section of the MICB Dashboard click on the Number of Ports link (see Figure 77 on page 182).

Note: The Meridian SL-100 only supports 32- and 64-port MICB cards. This procedure is not supported for Meridian SL-100 customers.

Figure 77
MICB Dashboard – Card Upgrade window



A ports upgrade is purchased from Nortel Networks, it comes with a new keycode for the card. Follow the steps in Procedure 31 to perform the port upgrade.

Procedure 31
Upgrade ports from the administrator's MICB Dashboard

1. From the pull-down menu, select the new number of ports in the combo-box. The current number of ports appears as view-only above this box.
2. Enter the keycode. The keycode is 24 digits. To simplify input, the system divides the keycode into three sets of eight digits each.

   The system displays the input characters they are entered.
3. Click on the **Submit** button.

   The system submits the change only if the keycode entry is correct. If the entry is incorrect, the following message appears: "Keycode is incorrect! Re-enter the keycode."

   Before clicking on the **Submit** button, operation can be cancelled by clicking on the **Dashboard** button on top of the window.

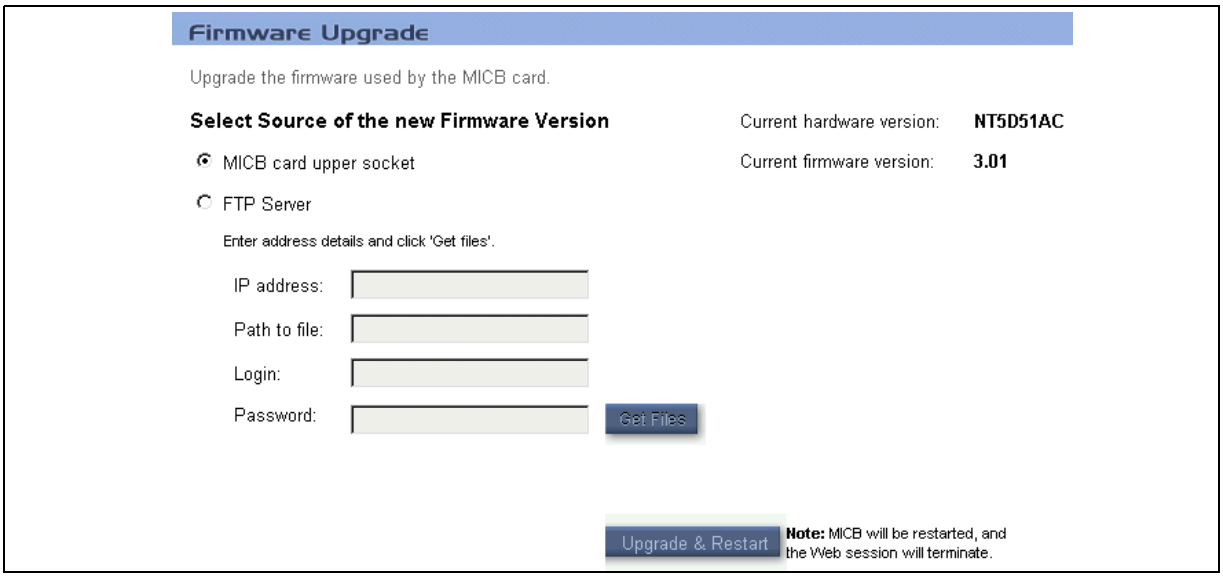
   Note: Ports must be configured in the switch in order for them to be operational.

This procedure is now complete

Firmware Upgrade

Upgrade the MICB 3 firmware from the following two sources: the secondary PCMCIA device or a remote FTP server. Use a BUI administration window for the upgrade process, which supports both options (see Figure 78 on page 183). The CLI can also be used.

Figure 78
MICB Dashboard – FIrmware Upgrade window



The top-right corner of the window shows the current hardware and firmware versions. The firmware version takes the form of “3.xx”, where 3 is the MICB release and xx is the firmware version number.

The MICB can retrieve firmware upgrade files from the following two sources:

1 A PCMCIA disk in the upper socket of the card.

2 A remote FTP server.

The first step is to specify the upgrade source by clicking on one of the radio buttons. Depending on the source selected, the following procedures describe how to perform the firmware upgrade.

Procedure 32
Firmware upgrade from MICB card upper socket

1 Click on the **MICB card upper socket** radio button.

2 Insert the PCMCIA disk in the upper socket of the MICB card.

3 Click on the **Upgrade & Restart** button.

The MICB copies the files from the upper socket and performs a restart. When the restart is complete, the current BUI session is lost. Login again as an administrator. When returning to this window, the new firmware version should appear in the top-right corner of the window.

This procedure is now complete

Procedure 33
Firmware upgrade using FTP

1 Click on the **FTP Server** radio button.

2 Enter the FTP parameters in the fields the window provides as follows:

   a **IP address** – the remote FTP server where the upgrade files are stored.

   b **Path to file** – path of the folder on the computer where the upgrade files are stored (for example, c:\micb\3_07).

   c **Login** – login name for FTP.

   d **Password** – password for FTP login.

3 Click on the **Get Files** button to start the FTP transfer session.

4 After the previous steps finishes, click on the **Upgrade & Restart** button.

The MICB copies the files from the FTP server and performs a restart. When the restart is complete, the current BUI session is lost. Login again as an administrator. When returning to this window, the new firmware version should appear in the top-right corner of the window.

This procedure is now complete

Upgrade to the single DN access method

Follow the steps in Procedure 34 to upgrade an existing MICB 2 card to MICB 3 configured with single DN access.

Procedure 34
Upgrade to single DN access

1 Follow Procedure 30 on page 180 to upgrade an MICB 2 card to an MICB 3 card.

2 Configure the DNs.

   a Remove the DN pairs from the switch datafill. For more information, if your system is a Meridian 1 or CSE 1000, see "Assign ACD DNs" on page 43; if your system is a Meridian SL-100 see "Single-card configuration" on page 50.

   Note: DN pairs can be left in the MICB. Callers to existing conferences configured with direct access DNs will be requested to enter the access DN to reach the meeting.

   b Configure the single access DN in the switch. For more information, if your system is a Meridian 1 or CSE 1000, see "Assign ACD DNs" on page 43; if your system is a Meridian SL-100 see "Single-card configuration" on page 50.

   Note: This DN should be forwarded to the MICB card main ACD DN.

3 Access the MICB Installation Wizard and perform the following (see "Step 2 – Access Numbers" on page 70):

   a Click on the first Radio button for the single DN access method.

   b Enter the new single-access DN.

   c Click on the **Submit & Continue** button.

   The new single DN access method now applies.

4 Instruct users to dial the single DN for future conferences.

Note: Make sure the notification E-mail content is still valid.

This procedure is now complete

Upgrade from a stand-alone to a dual-card MICB

This section describes how to upgrade an MICB 3 card operating as a stand-alone MICB to be either the primary or secondary card in a dual-card configuration.

The main issue to consider is the DN pairs: a single card can have up to 10 DN pairs, whereas a dual card can have only nine DN pairs, plus the dual-card meetings DN.

When upgrading or configuring a dual-card MICB 3 configuration, the secondary card must be configured before the primary card. Therefore, Procedure 35 must be performed before Procedure 36.

Procedure 35
Stand-alone card to secondary card

1 Access the MICB Installation Wizard: Step 1 – Basic Card Settings window (see "Step 1 – Basic Card Settings" on page 67). In the "Type" field, select the radio button "Dual Card – Secondary."

2 Click the **Submit & Continue** button.

If 10 DN pairs are configured, the system deletes one automatically. The MICB first attempts to delete a DN pair that has no conferences scheduled against it. If no such DN pair is found, the MICB deletes the DN pair with the least number of conferences using it. All associated conferences are deleted.

Note: A DN pair used by a permanent conference is not deleted.

If a DN pair is deleted in direct-access dialing mode, a pop-up message appears. Note the deleted DN pair, as it can be removed from the Meridian switch configuration.

3 The system displays Step 2 of the Installation Wizard (see "Step 2 – Access Numbers" on page 70). If the automatic change, as described above, took place, this is reflected in the DN table. If the direct access dialing mode is used, only nine DNs appear.

4 Click the **Submit & Continue** button. The system saves the change and the screen returns to the MICB Dashboard.

5 Logout of this card and proceed to the primary MICB configuration.

This procedure is now complete

Procedure 36
Stand-alone card to primary card

1 Access the MICB Installation Wizard: Step 1 – Basic Card Settings window (see "Step 1 – Basic Card Settings" on page 67). In the "Type" field, select the radio button "Dual Card – Primary."

2 Click the **Submit & Continue** button.

If 10 DN pairs are configured, the system deletes one automatically. The MICB first attempts to delete a DN pair that has no conferences scheduled against it. If no such DN pair is found, the MICB deletes the DN pair with the least number of conferences using it. All associated conferences are deleted.

Note: A DN pair used by a permanent conference is not deleted.

If a DN pair is deleted in direct-access dialing mode, a pop-up message appears. Note the deleted DN pair, as it can be removed from the Meridian switch configuration.

3 The system displays Step 2 of the Installation Wizard (see "Step 2 – Access Numbers" on page 70). If the automatic change, as described above, took place, this is reflected in the DN table. If the direct access dialing mode is used, only nine DNs appear.

4 Click the **Submit & Continue** button.

5 The system displays Step 4 of the Installation Wizard (see "Step 4 – Dual Card Meetings" on page 71).

If a DN pair was automatically deleted as described above, it appears in the fields "Conference access number" and "Chairperson number in primary card." You can change these numbers; they must be configured in the Meridian switch as well.

Fill in all the fields as described in the installation instructions, and click the **Finish** button.

6 Logout of this card and proceed with the Meridian switch configuration change (see Procedure 37).

This procedure is now complete

Procedure 37
Meridian switch configuration changes

1 If a DN pair was deleted from the secondary or primary card, delete it from the switch datafill.

2 Configure the DNs defined in the Installation Wizard Step 4 window of the primary MICB. Define them as described in the dual-card MICB installation instructions (for the Meridian 1 or CSE 1000 see "Configure DNs for a dual-card conference" on page 47; for the Meridian SL-100 see "Dual-card configuration" on page 55).

This procedure is now complete

Appendix A: Password security

Purpose

This chapter describes MICB 3 password protection and access restrictions.

The chapter contains the following sections:

- **“Access permissions” on page 188** – lists the security options available with the MICB 3 system.
- **“Unsuccessful login attempt handling” on page 189** – describes how the MICB handles unsuccessful logins.
- **“Password parameters summary” on page 190** – summarizes the default login names and passwords, and their parameters
- **“Reset passwords” on page 191** – provides procedures for resetting passwords.

Access permissions

MICB 3 provides strict password protections and other mechanisms to restrict access from unauthorized personnel (see Table 51).

Table 51
Access permissions

Access type	Description of permissions
BUI (HTTP server web access)	**1** Login name and password. The login name is a combination of letters and digits up to 10 characters in length. The password consists of digits only. Define the length according to the parameter “minimum password length”. Users and administrators can change their passwords at any time. **2** The system does not permit multiple, simultaneous BUI sessions for the same user. When a user logs into the BUI, no one else can login with the same user ID, until the session terminates (that is, the user logs out). The system permits only one administration session at a time. Therefore, if there is an active administrator session, the system does not permit another administrator log in. **3** You can access only the initial login window when you enter the BUI’s URL from your web browser. You cannot access any other page or file directly. **4** The system times out and closes the session after a period of inactivity. The administrator defines the time-out parameter.
CLI (direct connection)	**1** There are two login levels. Each level has a login name and password, both of which are changeable through the CLI. The name and password can contain letters and digits. **2** The CLI does not print the password when it is being entered. **3** The system records every successful login as an information message in the error log. **4** Upon a successful login, the CLI prints the login date and time. **5** The system times out and closes the session after a period of inactivity. The administrator defines the time-out parameter.
Telnet (server access)	**1** Remote access using telnet requires a dedicated login name and password. Successful login provides access to the CLI, which, in turn, requires its own access and login as described above. The name and password can contain letters and digits. **2** The system records every successful login as an informational message in the error log. The CLI terminal prints this message. **3** The system times out and closes the session after a period of inactivity. The administrator defines the time-out parameter.

Table 51
Access permissions (Continued)

Access type	Description of permissions
FTP (server access)	**1** Remote access using FTP requires a dedicated login name and password. The name and password can contain letters and digits. **2** The system records every successful login as an informational message in the error log. The CLI terminal prints this message. **3** The system times out and closes the session after a period of inactivity. The administrator defines the time-out parameter.
General	**1** The system always encrypts files containing passwords. **2** An administrator defines the minimum length of the login name and password. The system enforces the minimum requirement when a user changes their login name or password. This rule applies to all the passwords that this table describes. It does not apply to the conference and chairperson passwords set up in the BUI scheduling window. **3** The maximum password length is 16 characters, which is hard-coded. **4** The IP/LAN connectivity provides access through the LAN using HTTP, Telnet and FTP only.

Unsuccessful login attempt handling

Procedure 38 shows how the system handles unsuccessful login attempts.

Procedure 38
Unsuccessful login operation

1 No action is required for this procedure. However, observe the activities in the following steps and report any system discrepancies to your support technician.

2 For each faulty login, the system issues a message in the error log and the CLI. This applies to all access types: BUI; TUI; CLI; and Telnet. The following is an example of the message format (for more information on error messages, see "Error message handling" on page 151).

0024: WARNING MNGMMI114 12-06 15:42:55:612 FTP login FAILED from 152.217.111.234

3 The MICB counts consecutive login attempts. When the count reaches the "maximum faulty login attempts" parameter set by the administrator, the system performs the following:

- **a** **BUI user and administrator access** – After five consecutive faulty login attempts in which the login name is correct, but the password is wrong, the system blocks this login name. The administrator must reset the name to resume normal login operation.
- **b** **CLI access** – After the maximum allowed login attempts, the system blocks the CLI for a period of time. The administrator can define the blocking time period.

c **Telnet access** – After the maximum allowed login attempts, the system closes the connection. An administrator can define the “new connection refused” time period.

d **TUI access** – After three unsuccessful login attempts, the system disconnects the call.

This procedure is now complete

Password parameters summary

Table 52 shows the MICB 3 default login names and passwords.

Table 52
Default login names and passwords

Access type	Default login name	Default password
User BUI login (multiple users)	No default	000000
Administration BUI login (multiple administrators)	No default (see Note 1)	000000
TUI login (multiple users)	No default	Equal to BUI password
CLI first level	admin	_ (see Note 2)
CLI second level	debug	–
Telnet	micb	admin
FTP	micb	admin
Note 1: Initially, one administrator account exists: “admin”. ***Note 2:*** The CLI’s default passwords are empty (that is, no password).		

Table 53 summarizes the security parameters and their defaults.

Table 53
Security parameters summary

Parameter	Range	Default value
Minimum login name length	4-10	4
Minimum password length	1-16	4
Maximum password length	Hard-coded	16
CLI maximum unsuccessful login attempts	1-10	5
CLI blocking period after “Maximum unsuccessful login” is exceeded	1-1440 seconds	0
CLI inactivity time-out	1-1440 minutes	15

Table 53
Security parameters summary (Continued)

Parameter	Range	Default value
Telnet blocking period after “maximum unsuccessful login:” is exceeded	1-1440 seconds	20
Telnet maximum unsuccessful login attempts	1-10	5
Telnet inactivity time-out	1-1440 minutes	15
FTP inactivity time-out	1-1440 minutes	15
BUI inactivity time-out	1-1440 minutes	30

Reset passwords

Follow the steps in Procedure 39 when a user forgets their password.

Procedure 39
Reset forgotten passwords

1. The administrator can reset any BUI password through the user management BUI. One administrator can also reset another administrator’s password.
2. When an administrator forget’s their BUI password, and there is no other administrator, the password can be reset from the CLI by entering the following command:

   PAdmin/ABreset (or abbreviated **pa/ab**)

   The system resets all administrator passwords, if more than one exist.
3. When system passwords are forgotten (that is, Telnet, FTP, and CLI first level), the passwords can be viewed from the second level of the CLI.
4. When the second level CLI password is forgotten, perform the following steps.
   - **a** Connect a CRT (or terminal emulation on a PC) directly to the back of the card’s serial port.
   - **b** Perform a manual power-up as follows:
     - **i** Pull the card out of the slot.
     - **ii** Plug the card back into the shelf.

       The MICB starts the power-up process.

c Wait for the following banner to appear:

```
*****************************************
************************
*            Running MAIN CODE!!!            *
```

d Enter the token **default**. This token must be entered within 15 seconds of the banner's appearance.

The restart process continues and more lines of text may appear.

e When the power-up process completes and the CLI is ready for input, enter the factory-default second level password (that is, login = debug; password = no password).

f Access the password editing command to display or modify the CLI name and password (see Procedure 40).

After logging out from the CLI, normal login resumes.

This procedure is now complete

Follow the steps in Procedure 40 to edit or view a password from the second level of the CLI.

Procedure 40
Use the second-level CLI edit password command

1 Enter the second-level login name and password.

2 Enter **PA Admin** (or **pa**).

The CLI displays a list of available commands.

3 Enter the following command:

PSweditor (or **ps**).

The MICB displays passwords and related parameters and prompts for values. The system groups the parameters by sections, to allow faster steps. The sections are: [MIN_LENGTH], [CLI], [TELNET], [FTP], and [BUI}.

This procedure is now complete

CLI Password Editor editing session

The following is a example of using a CLI password editing session to change an FTP password. Table 54 shows the font conventions that the example uses.

Table 54
Password example font conventions

Font	Description
Mono	Prompts of text displayed by the CLI.
Bold	**User input.**
// Italics	*Explanations and comments.*

Values in the examples are not necessarily the defaults.

CLI change to FTP Password example

ps

// Administrator entered PSweditor
// MICB displays section name and its parameters, and prompts for action:

```
section [MIN_LENGTH]
MIN_NAME_LENGTH: 4
MIN_PASSWORD_LENGTH: 8
Modify, Next section, Cancel:
```

// Actions description:
// Modify - modify this section; MICB prompts values one by one
// Save - save pending changes and continue to next section
// Next - continue to next section
// Cancel - discard all pending changes and exit the command

n

// 'next' action selected
// MICB displays section name and its parameters, and prompts for action:

```
section [CLI]
1st level user name: admin
1st level password:
2nd level user name: debug
2nd level password:
Maximum allowed login attempts: 5
Blocking period (minutes) after login failures: 60
CLI idle timeout in minutes: 30
Modify, Next section, Cancel:
```

n

// next: go to next section

```
section [TELNET]
Telnet user name: micbtln
Telnet password: xyzu1234
Maximum allowed Telnet login attempts: 3
Blocking period (minutes) after login failures: 60
Telnet idle timeout in minutes: 20
Modify, Next section, Cancel:
```

n

// next: go to next section

```
section [FTP]
FTP user name: micbftp3
FTP password: abcd1234
FTP idle timeout in minutes: 5
Modify, Next section, Cancel:
```

m

// modify this section

```
section [FTP]
FTP user name: micbftp3 (4-30 chars): <cr> // empty input
FTP password: abcd1234 (8-30 chars): efgh5678 // new pswd
FTP idle timeout in minutes: 5 (1..1440): <cr>
```

// Section is re-displayed with modified values for confirmation (not saved yet)

```
section [FTP]
FTP user name: micbftp3
FTP password: efgh5678
FTP idle timeout in seconds: 900
Modify, Save, Next (section), Cancel: // re-prompt for action
```

s

// save changes

```
File “a:user\bindata.ini” was saved.
```

// Next section is displayed

```
section [BUI]
BUI idle timeout in minutes: 30
Modify, Save, Cancel: // re-prompt for action
```

// Command terminated (section FTP is last), current CLI menu is displayed:

```
PSWeditor, FUpgrade, SWupgrade, ?
```

Appendix B: Product integrity

Environmental specifications

MICB environmental requirements meet, or exceed, Meridian system requirements. The power provided for each card slot in the IPE module exceeds the power requirements for an MICB. Table 55 shows the range of acceptable temperatures and humidity for the MICB.

Table 55
MICB environmental specifications

	Specification	Minimum	Maximum
Normal Operation	**Recommended**		
	Temperature	15° C	30° C
	Relative humidity	20%	30% (non-condensing)
	Absolute		
	Temperature	0° C	40° C
	Relative humidity	5% to	90% (non-condensing)
	Rate of change	Less than 1° C per 3 minutes	
Storage	**Long Term**		
	Temperature	- 40° C	70° C
	Relative humidity	20%	55% (non-condensing)
		- 40° C to 70° C, non-condensing	
	Short Term (less than 72 hr.)		
	Temperature	- 40° C	70° C

Table 55
MICB environmental specifications (Continued)

	Specification	Minimum	Maximum
Temperature Shock	In three minutes	- 40° C to	25° C
	In three minutes	25° C to	70° C
		- 40° to 70° C, non-condensing	

Regulatory standards

The following tables list the safety and electro-magnetic compatibility regulatory standards for the MICB, by geographic region. Specifications for the MICB meet, or exceed, the standards listed in the regulations for these regions.

Safety

Table 56 provides a list of safety regulations met by the MICB, and the type of regulation and the country or region covered by each regulation.

Table 56
Safety regulations

Regulation Identifier	Regulatory Agency
UL 1459	Safety, United States, CALA
CSA 22.2 225	Safety, Canada
EN 41003	Safety, International Telecom
EN 70950/IEC 950	Safety, International
BAKOM SR 784.103.12/4.1/1	EMC/Safety (Switzerland)
AS3260, TS001 - TS004, TS006	Safety/Network (Australia)
JATE	Safety/Network (Japan)

Electro-magnetic compatibility (EMC)

Table 57 lists electro-magnetic emissions regulations met by the MICB card, along with the standard that lists each regulation.

Table 57
Electro-magnetic emissions

Regulation Identifier	Regulatory Agency
FCC part 15 Class A	United States Radiated Emissions
CSA C108.8	Canada Radiated Emissions
EN50081-1	European Community Generic Emission Standard
EN55022/CISPR 22 CLASS B	Radiated Emissions (Basic Std.)
BAKOM SR 784.103.12/4.1/1	EMC/Safety (Switzerland)
SS-447-20-22	Sweden EMC standard
AS/NZS 3548	EMC (Australia/New Zealand)
NFC 98020	France EMC standard

Table 58 lists electro-magnetic immunity regulations met by the MICB card, along with the standard that lists each regulation.

Table 58
Electro-magnetic immunity

Regulation Identifier	Regulatory Agency
CISPR 22 Sec. 20 Class B	I/O conducted noise
IEC 801-2 (level 4)	ESD (Basic Standard)
IEC 801-3 (level 2)	Radiated Immunity (Basic Standard)
IEC 801-4 (level 3)	Fast transient/Burst Immunity (Basic Standard)
IEC 801-5 (level 4, preliminary)	Surge Immunity (Basic Standard)
IEC 801-6 (preliminary)	Conducted Disturbances (Basic Standard)
BAKOM SR 784.103.12/4.1/1	EMC/Safety (Switzerland)
SS-447-20-22	Sweden EMC standard

Table 58
Electro-magnetic immunity (Continued)

Regulation Identifier	Regulatory Agency
AS/NZS 3548l	EMC (Australia/New Zealand)
NFC 98020	France EMC standard

List of terms

ACD
Automatic Call Distribution.

Browser User Interface
An interface that allows the administration of OA&M functions on conferences, users, and cards through a standard web browser.

BUI
See Browser User Interface.

Chairperson DN
The directory number the conference chairperson dials to enter the conference.

CLI
See Command Line Interface.

Command Line Interface
An interface that allows the administration of OA&M functions on cards through telnet or through a standard VT100 terminal.

CPU
Central Processing Unit. A chip that performs logic, control, and arithmetic functions. The part of the switch that performs these functions and any others necessary to process calls.

DN
Directory Number.

DRAM
Dynamic Random Access Memory. A high density type of semi-conductor memory. It typically has slower access time than SRAM and requires external memory refresh circuitry.

DSP
Digital Signal Processing. A specialized computer chip that performs speedy and complex operations on digitized waveforms. Useful in processing sound and video.

DTMF

Dual Tone Multi-frequency. A term describing push-button or touch-tone dialing.

EMC

Electro-Magnetic Compatibility. Refers to equipment units that perform their functions without causing or suffering unacceptable electromagnetic interference from other equipment in the same environment.

EMI

Electro-Magnetic Interference. Unwanted electromagnetic coupling, such as a ham radio heard on an electric organ or church music heard in hearing aids. Also known as “static”.

Firmware

Hardwired logic, software, data, and programming instructions such as that stored by threading wires through ferrite cores. May also refer to software programmed in the factory or burnt in the field, and is semi-permanently stored within ROM.

Flash memory

Electrically erasable memory that is non-volatile (not affected by power disruptions).

IP

Internet Protocol.

IPE

Intelligent Peripheral Equipment. A range of cards that contain micro-processors that provide off-loading of the CPU function and the flexibility to make changes to the system's parameters without revising the hardware.

LAN

Local Area Network.

LED

Light Emitting Diode.

LEN

Line Equipment Number (Meridian SL-100 equivalent of TN).

Main DN

The directory number that conferees dial to enter the conference when using direct access.

MMI

Man-Machine Interface.

MTBF

Mean Time Between Failure. A measure of reliability: the time that a user may reasonably expect a device or system to work before an incapacitating fault occurs. Also, the average number of hours between one random failure and the next under stated conditions.

OA&M

Operations, Administration, and Maintenance.

PBX

Private Branch Exchange. A telephony switch that is privately owned.

PCMCIA

Personal Computer Memory Card International Association. This organization has defined a credit card sized plug-in board for use in PCs. These cards are the only way to get to a laptop bus without using a docking station. In addition, application software can be stored on the card into system address space so that the software can run directly from the card, resulting in a faster start and less memory required from the host computer.

SCSI

Small Computer System Interface. A device that enables computers to cable-connect to networks or external tape units/hard drives.

SDI

Serial Data Interface. For some Meridian switches, provides ports between the CPU and external devices such as a teletype or maintenance telephone. More generally, an SDI is a mechanism for changing the parallel arrangement of data within computers to the serial form used on transmission lines and vice versa.

Telephone User Interface

An interface that allows the scheduling of simple conferences over a DTMF telephone.

TN

Terminal Number (Meridian 1 equivalent of LEN).

TUI

See Telephone User Interface.

.WAV

File format used for storing voice files created under Microsoft Windows.

Meridian 1 and Succession Communications Server for Entreprise 1000/
Meridian SL-100

Meridian Integrated Conference Bridge

Service Implementation Guide

Copyright © 2002 Nortel Networks,
All Rights Reserved

NORTEL NETWORKS CONFIDENTIAL: The information contained in this document is the property of Nortel Networks. Except as specifically authorized in writing by Nortel Networks, the holder of this document shall keep the information contained herein confidential and shall protect same in whole or in part from disclosure and dissemination to third parties and use same for evaluation, operation, and maintenance purposes only. Changes or modifications to the Meridian switch without the express consent of Nortel Networks may void its warranty and void the user's authority to operate the equipment.

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules, and the radio interference regulations of the Canadian Department of Communications. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at the user's own expense. Allowing this equipment to be operated in such a manner as to not provide for proper answer supervision is a violation of Part 68 of the FCC Rules, Docket No. 89-114, 55FR46066.

*Nortel Networks, the Nortel Networks logo, MAP, Meridian, Meridian 1, MSL, Nortel, Northern Telecom, NT, SL-1, SL-100, Succession, and SuperNode are trademarks of Nortel Networks.

Publication number: 553-3001-102/555-4001-135
Product release: MICB 3
Document release: Standard 01.06
Date: June 2002
Printed in the United States of America.