Meridian 1

Meridian Integrated Conference Bridge

Description, Installation, Administration, and Maintenance

Document Number: 553-3001-102
Document Release: Standard 4.00
Date: April 2000

Printed in Canada

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 Industry Canada. 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 their own expense.

Revision history

April 2000

Standard 4.00. This is a global document and is up-issued for X11 Release 25.0x.

July 1999

Standard, release 3.00. This release of the document describes the new functionality that is MICB Release 2.0.

March 1998

Standard, release 2.00.

June 1997

Standard, release 1.00.

Contents

About this document

This document is a global document. Contact your system supplier or your Nortel Networks representative to verify that the hardware and software described is supported in your area.

This document provides information about the implementation of the Meridian Integrated Conference Bridge (MICB) in the Meridian 1 system. It describes the MICB operation, installation, configuration, administration, applications, and maintenance.

It focuses on the application and administration of the MICB for scheduling and configuring multiple simultaneous conferences over a single MICB card.

The purpose of this document is to instruct the user how to install, configure, operate, and maintain the Meridian Integrated Conference Bridge (MICB) as a part of the overall Meridian 1 system.

The following describes what you will find in this document:

"Product description" on page 13 describes the MICB functional and physical characteristics.

"Engineering guidelines" on page 47 describes system hardware and software requirements and MICB Release 2.0 configuration options.

"Installation and configuration" on page 57 describes how to prepare the Meridian 1 equipment, how to install the MICB into the Intelligent Peripheral Equipment (IPE) module, how to connect it to the administration terminal, how to configure the MICB using the system TTY, and how to set up the web-based server.

“The Command Line Interface” on page 93 describes the MICB procedures using the Command Line Interface (CLI) for MICB parameter configuration, system administration and maintenance, and report generation.

“The Browser User Interface” on page 121 describes the MICB procedures using the Browser User Interface (BUI), a web-based server, for MICB conference administration and maintenance as well as user administration and maintenance.

“The Telephone User Interface” on page 157 describes the MICB procedures using the Telephone User Interface (TUI) for simple conference reservation.

“Maintenance” on page 173 describes how to perform maintenance functions and how to troubleshoot the MICB card and the associated equipment.

Appendix A on page 181 lists the MICB pin assignment and connector types for external connections to the MICB.

Appendix B on page 185 describes reliability, environmental specifications, product integrity, and regulatory standards for the MICB.

Appendix C on page 191 describes the daily reports that are available with MICB Release 2.0.

Appendix D on page 197 lists the Event Script files, which are audio files that MICB Release 2.0 uses during audio conferences.

Product description

This chapter describes the Meridian Integrated Conference Bridge (MICB) Release 2.0 card, both at a system level and at a card level. It describes functions, specifications, applications, engineering guidelines, and operation of the MICB card.

System overview

The MICB is an Intelligent Peripheral Equipment (IPE) card compatible with Meridian 1 options 21E, 51, 51C, 61, 61C, 71, 81, and 81C. It is also compatible with Option 11E/11C system, SL-1 systems NT and XT upgraded to support IPE cards, and SL-100 systems.

The system software required to support all 32 MICB ports in each MICB card is X11 release 22 or later. System software releases X11 releases 19 through 21 support a maximum of 16 ports per MICB card. The system software must contain the automatic call distribution (ACD) features and routing software modules to support the MICB operation. You must consider the ACD resources in the incremental software management (ISM) of the customer configuration, where each MICB port represents an ACD agent that uses a TN from the system resources.

The MICB communicates with X11 system software by emulating a digital line card, which allows the use of the existing software to control the MICB operation. Each MICB port is defined as an ACD agent. All MICB ports are members of the same ACD DN assigned to the MICB card.

The Conference/TDS card is not used in any application with the MICB card.

You can install multiple MICB cards into the system. Each MICB card can operate independently, providing up to 32 ports to a single conference; or you can combine two MICB cards in a dual-card configuration, which provides up to 62 ports to a single conference.

The MICB card has two PCMCIA sockets. PCMCIA hard drive cards are used to store the MICB voice prompts and firmware code. The MICB is shipped 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.

MICB Release 2.0 OA&M

Certain organization, administration, and management (OA&M) functions of the MICB Release 2.0 system, including initial setup and configuration, are performed through a Command Line Interface (CLI). You can access the CLI either through a TTY terminal that is connected directly to the MICB card or through a PC that emulates a terminal and which is connected to the MICB card via the Ethernet. The CLI can be used by the administrator who must do the following:

- generate reports
- perform port maintenance
- manage system administration, maintenance, and security

Only the administrator can access the CLI. For more information on the CLI, refer to “The Command Line Interface” on page 93.

The OA&M of conferences and users for MICB Release 2.0 is performed on a personal computer via a Browser User Interface (BUI). The BUI resides on a web-based server that can be either embedded in an MICB card, providing a direct point of contact to that particular card, or placed on an external server, providing a single point of contact to several MICB cards. The BUI provides three levels of user access, which are:

- **User** level access, for those who reserve and manage conferences just for themselves

- **Super user** level access, for those who must reserve and manage conferences for others and themselves
- **Administrator** level access, for those who must manage card and user attributes

For more information on the MICB Release 2.0 BUI, refer to "The Browser User Interface" on page 121.

MICB Release 2.0 also provides a Telephone User Interface (TUI), which users can use to reserve conferences over any DTMF telephone. Through the TUI, users can reserve simple conferences; many of the conference attributes are set to their default value. To set *all* of the attributes for a conference, or to modify a conference once you have set it, you must use the BUI. For more information on the TUI, refer to "The Telephone User Interface" on page 157.

MICB Release 2.0 connection to the Ethernet

To conduct conference administration and maintenance for MICB Release 2.0, you must connect a PC to your LAN. The MICB Release 2.0 card connects to your LAN through an Ethernet adapter. The Ethernet adapter provides two connection options:

- Direct terminal connection or modem connection to DB-9 connector (provides *only* access to the CLI)
- Ethernet connection, where multiple terminals connected to the Ethernet can access an MICB card (provides access to the CLI, through telnet, *and* the BUI, through a common web browser)

For the Ethernet connection, you must assign an IP (Internet Protocol) address to the MICB card, thereby enabling access to the MICB through your LAN (Local Area Network). There are two options for connecting MICB Release 2.0 cards to the LAN through the Ethernet adapter:

- Connect each card directly to the LAN. This is the embedded server option, where users access each card separately through a web server that is embedded on each card. This option allows creation of 100 total users and up to 10 simultaneous users on each card.
- Connect each card to the LAN through an external web server. Users point their web browsers to the external server address. From there, they can have access to each card that is attached to the server. The external web server can centrally manage up to ten MICB Release 2.0 cards. You must use this option if you use the dual-card configuration. This option allows the creation of 1000 total users and up to 50 simultaneous users.

Figure 1 shows a Meridian 1 with MICB cards connected directly to the LAN. Figure 2 shows a Meridian 1 with MICB cards connected to the LAN through an external web server. Any PC with access to the LAN can access the MICB cards.

Figure 1
MICB Release 2.0 cards in the Meridian 1 system (Internal server option)

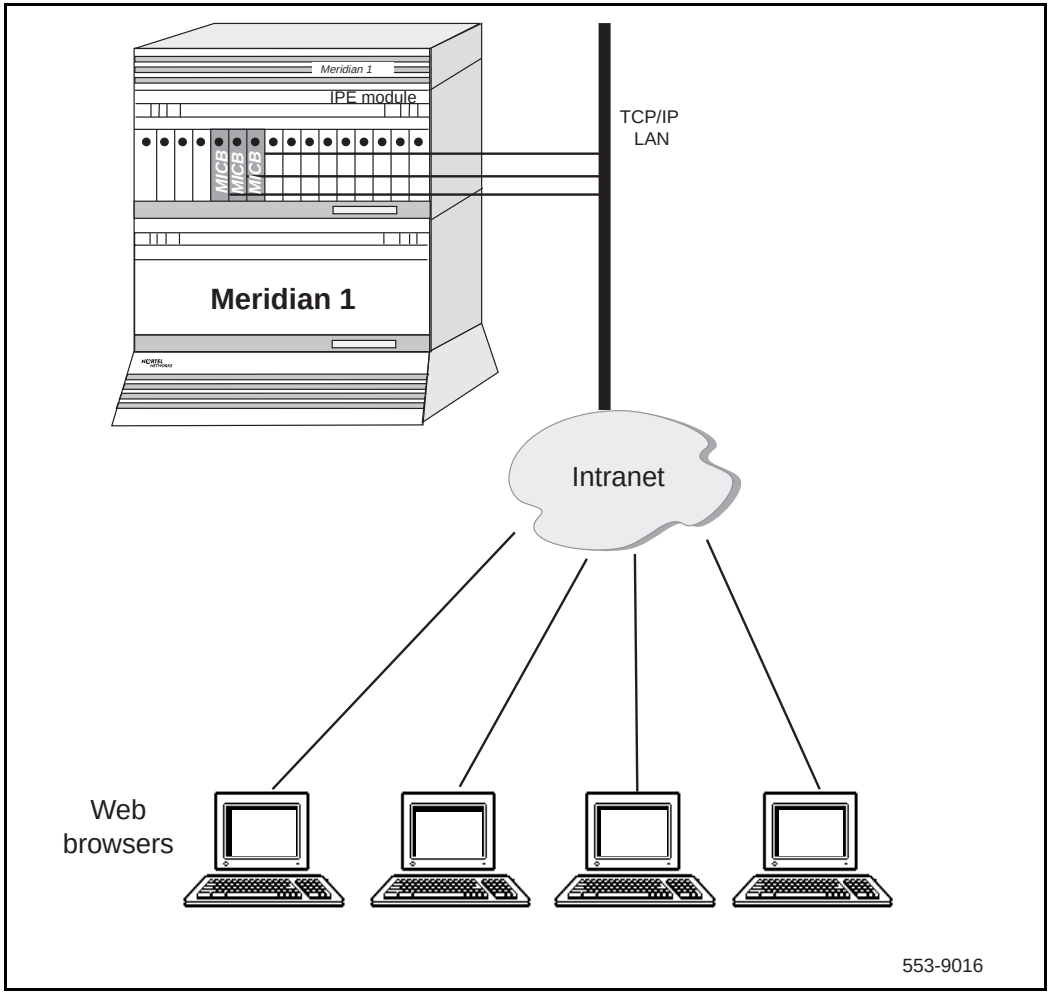
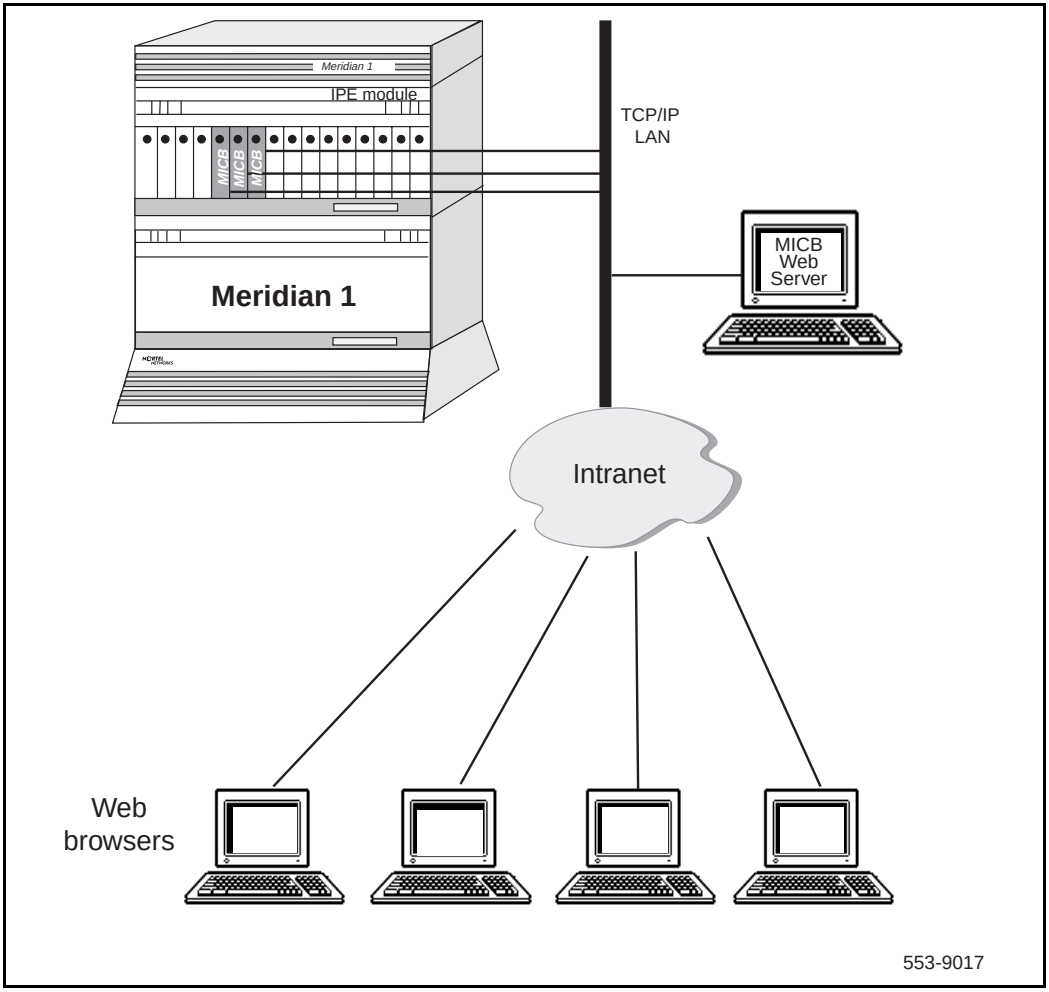


Figure 2
MICB Release 2.0 cards in the Meridian 1 system (External server option)



MICB description

You can install the Meridian Integrated Conference Bridge (MICB) card into any IPE card slot that is associated with full 50-pin I/O cables. For specific information of the possible IPE card slots where the MICB can be installed, refer to Table 4, "MICB installation into card slots in different IPE modules," on page 48.

A single MICB card provides up to 32 ports that you can partition into groups from 1 to 10, where each group represents an independent conference. Alternatively, you can connect two MICB cards together to provide up to 62 ports for a single conference.

> ***Note:*** Systems with X11 release 22 or higher support 32 MICB ports per card; systems with X11 releases 19 through 21 support only 16 ports per card.

Each MICB port is configured as an ACD M2616 digital telephone set. The Meridian 1 system ACD function routes the incoming calls to the MICB, where each MICB port is treated as an ACD agent. All MICB ports belong to the same ACD queue and are treated as a pool of ports with equal status. For an ACD DN description, refer to "Configuring the MICB ports" on page 33.

The MICB supports several conferences simultaneously. The number of conferences depends on the number of MICB ports available and the number of participants (conferees) in each conference. For an MICB with 32 ports, there can be a maximum of 10 conferences with three or four participants in each conference, 1 conference with a maximum of 32 participants, or any combination in between.

The DNs and the corresponding TNs are system resources, which when assigned to the MICB ports cannot be used for other Meridian 1 stations. For an MICB with 32 ports, a maximum of 10 simultaneous conferences would require 20 ACD DNs for the conferees and chairpersons to dial to enter the conferences, 32 TNs assigned to the ports, and one ADC DN assigned to the MICB card. Please be aware of this use of system resources when configuring the MICB card.

The main hardware and functional characteristics of the MICB card are described in:

- **MICB functional characteristics**
- MICB hardware design characteristics

MICB functional characteristics

The function of the MICB card is to schedule and administer multiple simultaneous conferences. These conferences are scheduled based on time-of-day, duration of each conference, and number of conferees or ports allocated for each conference.

The MICB card provides pre-programmed announcements and tones that correspond to specific events during conferences. These events include advising the chairperson and other conferees of the status of the conference connection, indicating when a conferee joins or leaves the conference, warning the chairperson and the conferees when the scheduled conference time is about to expire, etc.

MICB Release 2.0 card features:

- compatible with the IPE module in any system that supports IPE, including the SL-100
- occupies one slot in an IPE shelf or an Option 11
- emulates an M2616 digital telephone set on each MICB port
- supports both the A-law and the μ-law signal coding/decoding
- provides full duplex communication
- supports DTMF detection
- Command Line Interface (CLI), accessible by direct connection, modem, or telnet for performing certain OA&M functions
- Browser User Interface (BUI), accessible through a common web browser for conference and user administration and maintenance
- Telephone User Interface (TUI), accessible through any DTMF telephone for reserving simple conferences
- dual-card configuration to allow up to 62 ports in a single conference (does not require new software)

- can reserve one port on each card for TUI-only interaction
- provides system reporting

Features supported through the MICB DSP firmware:

- selects two active speakers in a conference of up to 62 conferees
  - — analyzes the loudness of all received signals continuously and selects the two loudest signals to be the two active speakers
  - — the two speakers are not selected globally, but based on the signal strength associated with each timeslot
- handles 2-way conversation in conferences with 3 to 62 conferees
- supports a maximum of 10 simultaneous conferences per card
- normalizes the PCM input samples
- provides gain control on all output samples

MICB expansion options:

- software upgrade using a PCMCIA Flash card
- scalable port options of 12, 16, 24, 32, 42, 50, and 62 ports

MICB conference features:

- one chairperson per conference (two for a dual-card conference)
- provides for one or more permanent bridge configurations
- supports multiple conferences simultaneously
- allows conference extension beyond the scheduled time
- provides automatic conference expansion, allowing additional conferees to join the conference (***Note:*** For the expansion to work, the ports hosting the additional conferees must be both unassigned *and* available. Also, expansion ports are assigned on a first come, first serve basis.)
- supports the following languages for the North American, CALA, and Asia Pacific markets: N.A. English, French, Brazilian Portuguese, L.A. Spanish, Chinese, Japanese, Korean, and U.K. English
- supports the following languages for the European market: U.K. English, N.A. English, French, German, and Italian

- conference password security, requiring the chairperson and/or the conferees to enter a DTMF password before entering the conference
- automatically starts and terminates conferences based on reservations scheduled in advance
- provides email notification to conference scheduler of conference attributes
- provides the ability to reserve a port from each conference for the chairperson
- block-out scheduling for recurrent conferences, up to one year in advance and 15 iterations
- 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)
- 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 option supports a maximum of 32 ports for the emergency bridge. The emergency bridge does not support the dual-card configuration.
- issues 10-minute warning before the conference termination
- entry & 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 conference music turn off and turn on for the first conferee joining the conference
- 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 and tones to ports and conferences by playing pre-recorded files stored on the PCMCIA hard drive card
- supports administration features such as system configuration, scheduling, management, and report generation
- routes conferees to the appropriate conference based on the dialed directory number (DN)
- allows recording of a brand line (custom) greeting for each language
- issues audible responses to conferees based on the conference activity
- provides enhanced CDR and billing options
- provides conference traffic report
- Chairperson command features:
- Dial-out, enabling the chairperson to call a non-participant (The chairperson can then return to the conference with or without the person he or she called.)
- Redial last dialed DN
- Mute/unmute all ports
- Mute/unmute self
- Group call-out, enabling the chairperson to call several people on a pre-defined list simultaneously
- Lock/unlock conference, enabling the chairperson to deny/allow the joining of new participants
- Count conferees and announce names of participants to all participants or just the chairperson
- Drop all conferees
- Drop last dial-out participant
- Drop last dial-in participant
- Conference duration expansion, enabling the chairperson to immediately extend the length of the conference by 15 minutes

- Selective disconnect/mute/unmute/consult, enabling the chairperson to disconnect, mute, unmute, or privately consult with a single participant (The private consultation feature is also known as a side bridge.)
- Stop/start music while waiting
- Help access, enabling the chairperson to play the list of available commands

The conferees can also execute the mute/unmute self, stop/start music while waiting, and help commands.

MICB hardware design characteristics

An MICB card occupies one IPE slot in an IPE module.

The MICB card has the following hardware interface characteristics:

- uses the MPU based on the 25MHz MC68EN360 Integrated Communications Controller
- uses standard interface buses and PCMCIA cards and handles MS-DOS compatible file on the PCMCIA storage device
- accesses all 32 DS-30X voice/signaling timeslots
- provides echo cancelling
- supports automatic gain control
- supports Card-LAN interfaces
- performs X11 signaling protocol messages for input/output
- uses Digital Signal Processor (DSP) for conferencing and DTMF detection
- provides self-test of internal hardware components and allows card monitoring and maintenance through the maintenance port
- provides one RS-232 serial port for initial setup of the card
- provides Ethernet connection to the LAN for web and telnet access
- provides for either an embedded or an external web-based server

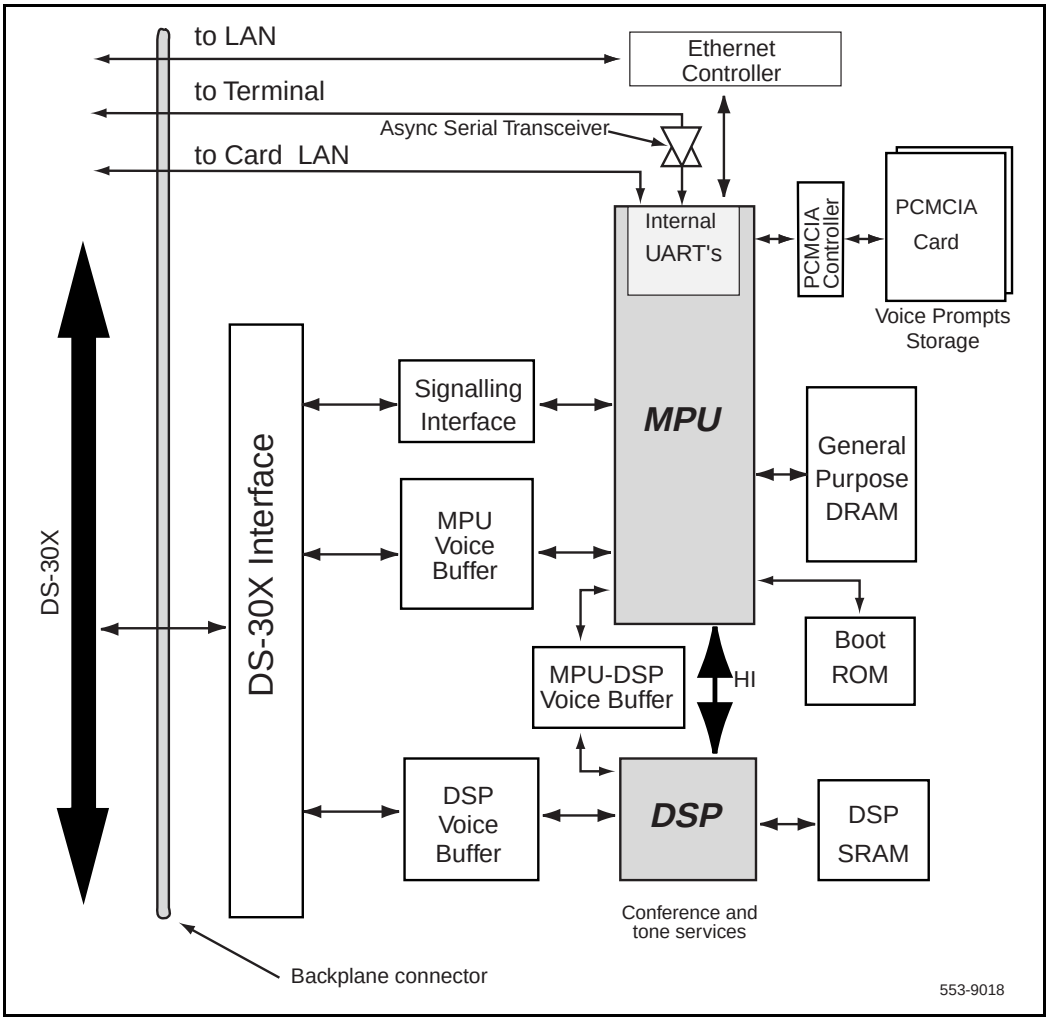
Table 1 describes each hardware component provided for the MICB application. These components are used to connect the MICB to the maintenance terminal locally and remotely.

Table 1
MICB hardware list

Component	Description
NT5D51 MICB Card	An IPE card that provides bridge and conference scheduling for up to 10 simultaneous conferences. (The NT5D51 MICB card, the Security Device, and the PCMCIA hard drive card are packaged together as NT5D32 in N.A./CALA/Asia Pacific and NT1439 in Europe).
PCMCIA Hard Drive Card (NT5D62BB in N.A./CALA/Asia Pacific; NT1438BC in Europe)	This PCMCIA card contains the MICB software and configuration. It must be installed into the lower PCMCIA drive for the MICB to operate.
NT5D52AB Ethernet Adapter card (for IPE module installation)	This adapter card is installed on the IPE module I/O panel for connection to the LAN.
NT5D52BB Ethernet Adapter card (for Option 11C/11E installation)	This adapter card is installed into the Option 11C/11E tip/ring connector for connection to the LAN.
Nullmodem Maintenance cable	This cable has a DB-9 female and a DB-25 male connectors and is used to connect the terminal to the MICB using the Ethernet Adapter card DB-9 male connector. No additional nullmodem is required.

Figure 3 shows a high level block diagram of the MICB card components. It also shows the MICB interfaces at the IPE module backplane connector.

Figure 3
MICB block diagram



Micro Processing Unit (MPU)

The MPU coordinates and controls data transfer and addressing of the peripheral devices. Tasks that the MPU performs depend on the interrupts it receives. These interrupts are prioritized by the importance of the tasks they control.

The MPU is highly integrated and provides most of the decision making logic on the chip. Functions of the MPU include controllers, timers, control logic, address decoding, DRAM and independent direct memory access, Ethernet terminal and Card-LAN input/output ports, and independent full-duplex serial communication channels that support various protocols.

The MPU can be reset by:

- powering up the MICB card
- entering reset command on the MMI
- the watchdog timer

A resident boot code contained in Flash memory starts the process of bringing up the MICB. This boot code loads a start-up program from a fixed location on the PCMCIA disk. The start-up program performs basic diagnostics and loads the main code to the RAM.

Digital Signal Processor (DSP)

The DSP communicates with the MPU over the host interface (HI) and the MPU-DSP voice buffer. It also communicates with the DS-30X interface over the DSP voice buffer. The DSP can access program and data stored in the DSP SRAM. The PCMCIA Flash card must always be installed in the low PCMCIA slot on the MICB.

Memory

The MICB card contains the following memory types:

- general purpose DRAM
- Boot ROM
- DSP SRAM

Additional memory is available when the PCMCIA card(s) are installed into the MICB card.

Card-LAN interface

To implement the Card-LAN interface, the MICB card uses an internal UART device. The UART channel is a serial communication interface to Peripheral Controller card.

The Card-LAN is a 19.2 kbps asynchronous interface. It is used to poll and communicate with the Peripheral Controller card to transmit maintenance messages, which include:

- LED control of the IPE card enable/disable
- MICB card configuration
- MICB card type and version information

DS-30X

A DS-30X network loop is composed of two synchronous serial data buses that transport data:

- One bus transmits data toward the line facility (Tx)
- The other bus receives data toward the Meridian 1 CPU (Rx)

DS-30Y network loops extend between controller cards and superloop network cards and function similarly to DS-30X loops. Essentially, a DS-30Y loop carries the PCM timeslot traffic of a DS-30X loop, but up to four DS-30Y loops form a *superloop* with a capacity of 128 channels (120 usable timeslots).

RS-232 port

A serial port is provided on the MICB card for initial setup of the MICB Release 2.0 card. Access to this port is over the IPE module backplane connector to the I/O panel and from the I/O panel to the terminal.

Ethernet interface

An Ethernet interface on the MICB is provided at the I/O panel by installing the Ethernet adapter. The Ethernet interface is necessary to schedule and maintain conferences and users. This adapter provides an Ethernet RJ-45 and a DB-9 connector. There are two versions of the Ethernet adapter: one for Option 11E/11C and the other for Meridian 1 options 21E, 51, 51C, 61, 61C, 71, 81, and 81C; refer to Table 1 “MICB hardware list” on page 25. Also, refer to “To access the BUI” on page 54. The Ethernet interface provides multiple terminal access to the MICB card through your LAN.

Figure 4 illustrates 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 LED indicators and the slot locations for PCMCIA cards.

Faceplate sockets and indicators

The MICB faceplate provides the following:

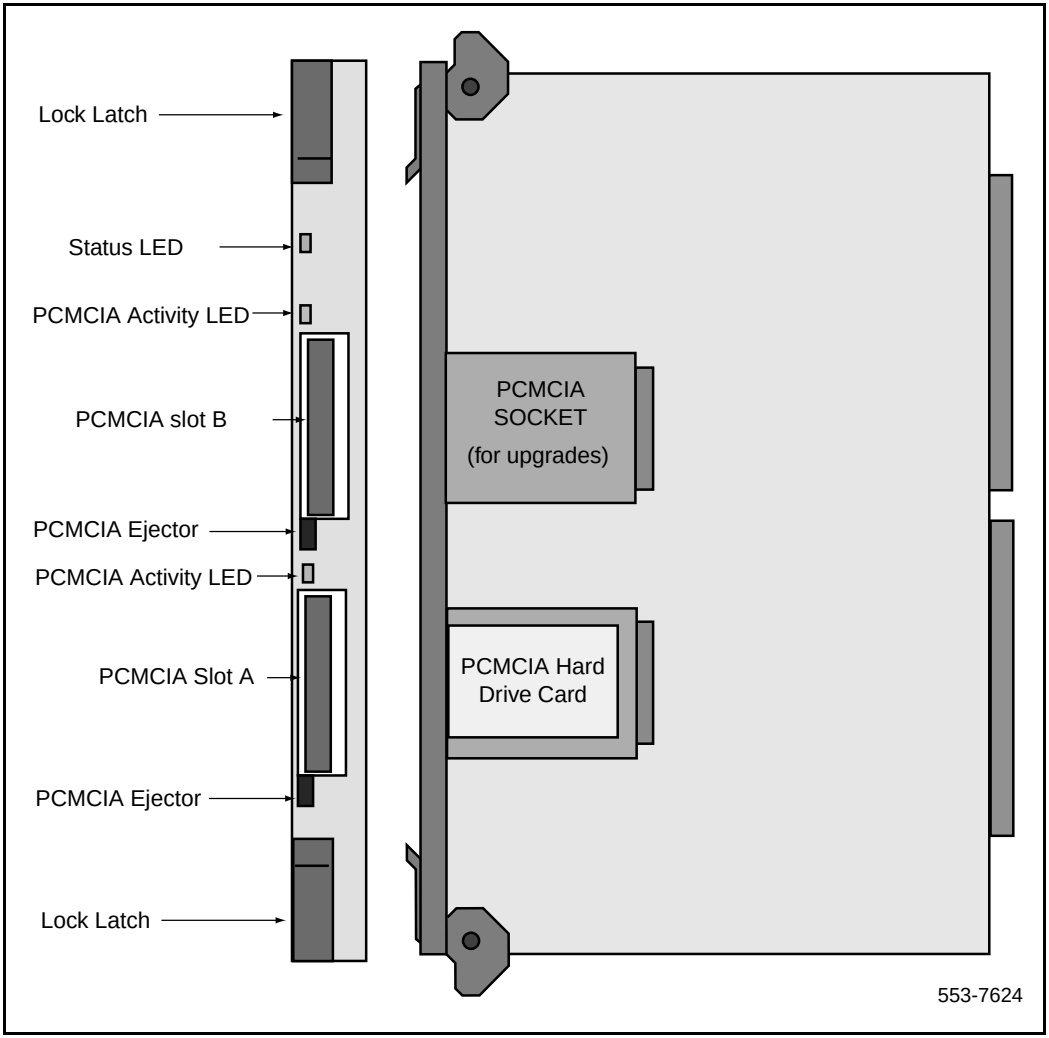
Card LED The MICB faceplate provides a red card LED to indicate the enabled/disabled status of the card and to indicate the self-testing result during power up or card insertion into an operating system. This LED indicates the following:

- LED is ON when the MICB card is disabled
- LED is OFF when the MICB card is enabled and ready for use
- LED is BLINKING three times and stays ON (until is software enabled) when the MICB card has successfully completed self-test

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

- LED is ON when the PCMCIA card is disabled
- LED is OFF when the PCMCIA card is enabled and ready for use
- LED is BLINKING when the PCMCIA card is in use

Figure 4
MICB card



Type II/III PCMCIA slots

The MICB faceplate provides two Type II/III PCMCIA card slots. These slots are use to house the PCMCIA cards. The lower slot is used to install the PCMCIA hard drive card that stores voice prompts and firmware code. The upper slot is used for upgrading the firmware, when required.

MICB operation

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 and/or entry and exit tones that are broadcasted to all conferees when requested by the MPU.

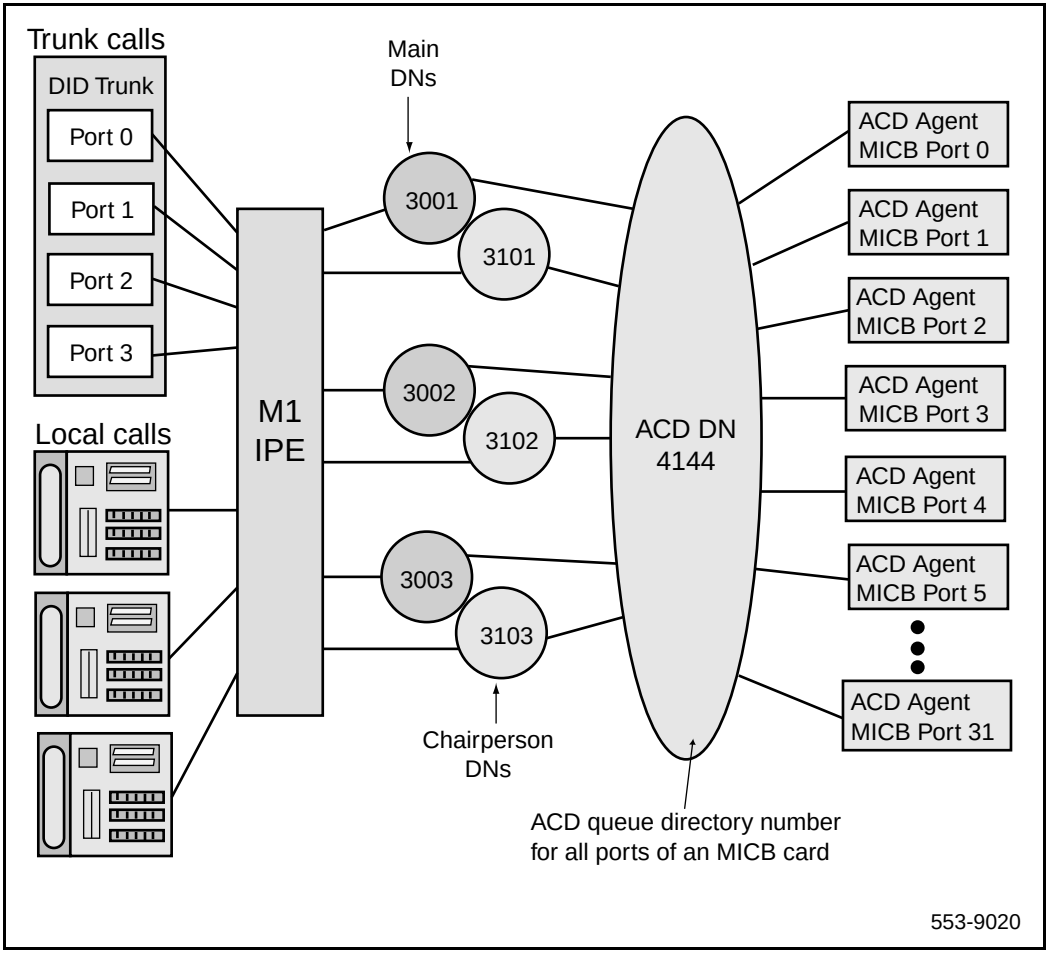
The MICB card uses the system ACD features to schedule multiple simultaneous conferences, to route external incoming trunk and local line conferees to their appropriate conferences, and to provide queuing, chairperson features, and events reporting for each conference.

The ACD features used by the MICB card provide:

- expanded number of ports in the same pool allowing up to 1200 ACD agents for Meridian 1 systems and up to 120 for the Option 11E/11C system
- simple software configuration
- queuing of incoming calls, announcement on arrival, call management, and reporting
- operational statistics reports
- enhanced call routing

Figure 5 illustrates the call routing for three conferences. It shows the conference chairperson access directory number (DN) for each conference and 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 5
Call routing with chairperson access



Configuring the MICB ports

Ports on the MICB card are configured as ACD digital sets, where each port is considered to be an ACD agent. Each port must be assigned a terminal number (TN). All ports on an MICB card belong to an ACD queue (group). This ACD queue is identified with an ACD DN that handles the connection of conferees (ACD agents) to the appropriate conference.

Furthermore, each conference is assigned a main DN and a chairperson DN, where the main DN is the number the conferees dial to get into the conference and the chairperson DN is the number the chairperson dials. The DNs are configured in Meridian 1 at the time the MICB card is installed. The total number of DNs is equal to two times the number of simultaneous conferences you wish to allow. For example, if there are ten conferences, there will be twenty DNs—ten main DNs and ten chairperson DNs.

Joining the conference

When several conferences take place simultaneously in the same MICB card, the conferee dials the DN assigned to a specific conference. The MICB card recognizes the dialed DN and routes the conferee to the appropriate conference represented by that specific DN. All ports belonging to an MICB card are routed to the appropriate conference through the ACD DN assigned to that MICB card, i.e., that ACD queue. The chairperson dials the chairperson DN to access his or her specific conference. This number is different from the DN dialed when the conferees are accessing that same conference.

The MICB performs DTMF detection on all MICB ports so that both the chairperson and the conferees can enter certain commands. A conference can start without the chairperson, and if all allocated ports for a conference are occupied with conferees, the chairperson cannot join the conference unless a port is specifically reserved for the chairperson or conference expansion is allowed and there are free, un-scheduled (floating) ports available.

The first participant joining the conference hears an announcement that indicates that no other conferee has joined the conference yet, and this announcement is followed by 60 seconds of music. This announcement with 60 seconds of music is repeated continuously until at least one more participant joins the conference.

The MICB provides flexibility in configuring conferences. They can be configured as:

- pre-scheduled conference with fixed number of ports and fixed start and stop times
- pre-scheduled elastic conference with variable number of ports, where they are added when required (if available) and subtracted as people leave the conference
- permanent bridge with a fixed number of ports that can be used without pre-scheduling the conference

Expanding the conference

You can allow or deny conference expansion by checking the appropriate box on the MICB Conference Reserver page. If allowed, the number of conferees belonging to a conference can be expanded as long as there are remaining MICB ports that are both unassigned *and* unused.

When reserving the MICB ports for each simultaneous conference, specific ports are not tagged for a specific conference. The MICB counts the number of reserved ports and compares them against the total number of ports provided by the MICB card and makes sure that the reserved ports do not exceed the total number of ports provided by the MICB card.

> ***Note:*** If you enable the conference over-booking option, the total number of ports reserved for conferences can equal, but not exceed, 125% of the port capacity.

If additional (not scheduled) callers attempt to join a conference, but they are not allowed due to lack of floating ports or locked conference, the MICB card will issue an overflow tone and then disconnect the call.

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

The minimum duration of a conference is 15 minutes and the maximum duration of a time-limited conference is 12 hours. Schedule conference starting times and conference durations in increments of 15 minutes.

Ending the conference

When a conference is scheduled, the conference's number of ports, start time, and duration are specified. The conference ends at the predetermined time, which is determined by 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 must terminate in 10 minutes.

When the conference time is up, the MICB card issues the final warning to the conferees. The MICB also sends the release message to Meridian 1 for all the associated MICB ports. These ports now become available for the next pre-scheduled conference, or if not scheduled, they become floating ports not reserved for any other conference and are available to expand conferences in progress.

Individual conferees can leave a conference in progress at any time. The MICB detects a conferee leaving the conference and inserts an exit prefix announcement in the conference and the conferee's name is announced, if this feature is enabled.

> ***Note:*** A conference can begin and end two minutes before the specified time. This feature allows the system to close all terminating conferences two minutes earlier and start all conferences that should be started immediately after the terminating conferences are closed. This feature is important when terminating and starting conferences use some of the same DNs.

Chairperson's function

To become a chairperson, you must be the first to dial the chairperson DN. The chairperson can control conference activities by executing commands on his or her DTMF telephone. These commands consist of a star (*) followed by one or two digits. If only a star (*) is dialed, after 5 seconds the command times out.

Dual-card conferences require two chairpersons, one for the primary card and one for the secondary card. The primary card chairperson can control conference activities only on the primary card. Therefore, a secondary card chairperson is necessary for controlling conference activities on the secondary card. One exception to this restriction is the Group Call-out feature. The primary chairperson can activate a group call-out to all participants in a dual-card conference.

These following paragraphs detail the chairperson commands.

Dial-out

The chairperson can dial out and call a new party outside of the conference, with the intention to confer only with the party or to bring the party into the conference. To do this, the chairperson dials *0DN# to dial a party outside the conference, or *0# to access the operator. The chairperson can then decide to bring the party into the conference by dialing *2 or disconnect the call by dialing *3. If you dial the wrong number, you can dial *3 and re-dial. To redial the last number dialed, the chairperson dials *#.

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. The port can also be available if all the reserved ports are occupied for that conference, but there are some un-reserved ports available on the MICB card and the port expansion feature is enabled for that conference. If all reserved ports are occupied and there are no unscheduled ports available, the call cannot be completed.

All ports mute/unmute toggle

The chairperson can place all conference participants on mute, excluding him or herself, by dialing *10. While on mute, the participants can still 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.

Self mute/unmute toggle

Any conference participant, including the chairperson, can put himself or herself on mute by dialing *19. While on mute, the participant can still 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 not only to those participants who enter the conference by dialling in, but also to those participants who are brought into the conference through the chairperson’s dial-out command.

Group call-out

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

The administrator defines these lists through the web-based server. The information is saved on the MICB PCMCIA disk.

The administrator also defines the following three options for each group list:

- Wait time for an answer (range: 15 - 90 seconds), default is 30.
- Number of call attempts (range: 1 - 3), default is 1.
- Time period between attempts (range: 5 - 30 seconds), default is 10.

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

When two MICB cards are involved 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, over the TCP/IP LAN, to the secondary card. The secondary card then dials the seconds group of numbers. Both groups of numbers are dialed simultaneously.

The MICB card dials out by allocating a free port and originating the call on it. The port is not connected to the meeting until the call is completed successfully. The MICB card needs an external input to indicate successful completion of the call. This input comes from the called party. After the MICB card originates the call, it plays a specific prompt and keeps repeating it for a pre-defined number of seconds (determined by the administrator). In this time, the called party must respond by dialing * (the star symbol). When the MICB card detects the proper response, the MICB card connects the call to the meeting. If the MICB card does not detect the proper response after the pre-defined timeout time and the pre-defined number of retries, the MICB card disconnects the call.

Group call-out is limited to the number of available ports on a conference. For example, if the chairperson uses a group call-out list that contains 61 numbers, and the meeting he is using has only 20 free ports at the moment, the MICB card dials only the first 20 phone numbers of the list.

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 by dialing *4 again and thereby allow new conferees to join the conference. A caller attempting to join a locked conference hears an announcement indicating that the conference is locked, and the call is disconnected. The chairperson can dial-out and include a conferee even if 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 execute one of two commands to count the conferees and play a list of all of the participants. With the execution of either of these commands, the MICB card issues a string of voice prompts, one for each conferee in the conference. If a new conferee joins the conference after the chairperson activates either command, the MICB card does not count that new conferee.

> ***Note:*** To announce the names of the conferees through either command, the conference scheduler must define an Entry & Exit Indication that requires entry by name.

The two options for counting conferees are:

- Chairperson dials *60 to count the conferees and play the list of participants for *all* of the participants. When the list is over, the conference returns to normal state.
- Chairperson dials *69 to count the conferees and play the list of participants for *only* the chairperson. Dialing *69 puts the chairperson into a “scrolling state” where he or she can execute the following commands:

Chairperson dials...	In order to...
#	Stop and start the playlist (Chairperson must dial # after dialing *69 to start the playlist.)
0	Consult privately with the conferee
1	Mute/unmute the conferee
2	Announce the current conferee’s name greeting
4	Select and announce the previous conferee
6	Select and announce the next conferee
9	Disconnect the current conferee
k3	Return to the conference
kk	Start and stop the help menu

When the playlist is over, the MICB automatically returns the chairperson to the conference unless the chairperson dials #.

Drop all conferees

The chairperson can drop all conferees from the conference except the chairperson by dialing *90. No announcement is issued to the conferees before disconnecting them. The MICB card issues an announcement to the chairperson indicating that no conferees are connected to the conference, followed by 60 seconds of music. The conference is still active, so conferees can dial in again.

Drop last dialed conferee

The chairperson can drop the last conferee to join the conference through chairperson 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. The chairperson receives the voice message, “Your meeting duration has been expanded” if the expansion is successful. If the duration expansion is not successful due to a lack of resources, such as ports or DNs that have already been reserved for other meetings, the chairperson receives the voice 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 that is scheduled to end within three minutes of the expansion request.

Chairperson 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 someone and then dials **, the chairperson hears the list of commands relevant to dialing out. And if the chairperson dials *69 to count conferees, and then dials **, the chairperson hears the list of commands relevant to counting conferees.

Conferees can also dial ** to hear a list of command options available to conferees. Only the participant who dials **, whether the chairperson or a conferee, hears the relevant list of commands.

Summary of chairperson commands

Table 2 lists conference commands that one can execute on the telephone set while the conference is in progress.

Table 2
Conference commands

Chairperson Command	Description
k0<DN>#	Dials out to a DN (called party directory number, which is not a conference participant)
k0#	Dials out to the assistant DN
k#	Redials last dialed DN
k10	All ports mute/unmute toggle
k19	Self mute/unmute toggle
k2<GN>#	Group call-out, where GN is the group number to call
k2	Returns to the conference with dialed party
k3	Returns to the conference without dialed party
k4	Locks or unlocks the conference
k60	Counts conferees and plays list of participants and their port numbers to *all* participants
k69	Counts conferees and plays list of participants and their port numbers to chairperson *only.* Refer to Table 3 on page 43 for scrolling-state commands.
k90	Drops all ports except the chairperson's port
k91	Drops the last dialed-out port

Table 2
Conference commands

Chairperson Command	Description
k92	Drops the last dialed-in port
k98	Extends the conference by 15 minutes
k99	Stops or starts the initial conference music by the chairperson. This is possible only when the chairperson is the first person to join the conference. The first entry stops it, the second entry starts it.
k	Aborts current command
kk	Starts or stops help menu
Conferee command	**Description**
k19	Self mute/unmute toggle
k99	Stops or starts the initial conference music. This is possible only when the conferee is the first person to join the conference. The first entry stops it, the second entry starts it.
k	Aborts current command
kk	Starts or stops help menu

Table 3 list commands the chairperson can execute after he or she dials *69.

Table 3
Chairperson's scrolling state commands

Chairperson Command	Description
#	Stop and start the playlist of participants
0	Consult privately with the participant
1	Mute or unmute the participant
2	Announce the current conferee's name greeting
4	Select and announce the previous conferee
6	Select and announce the next conferee
9	Disconnect the current participant
k3	Return to the conference
kk	Start or stop the help menu

MICB capacity expansion

You can configure each MICB card to provide a maximum of 12, 16, 24, or 32 ports. Dual-card configurations are available in 42, 50, and 62 port options. To activate a different number of ports than are currently active, you must enter the CLI, then access the General Administration commands *Functionality Upgrade* menu and select *Modify* to change the maximum number of ports available, and then *Save* to save the changes.

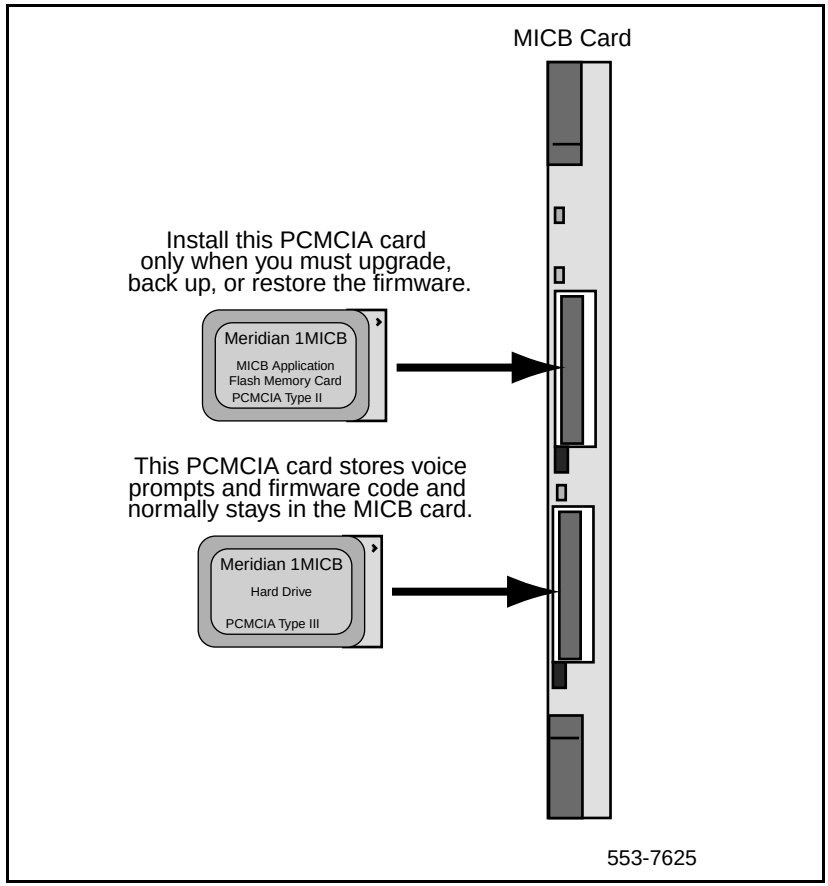
> ***Note:*** If you are expanding from a single-card configuration to a dual-card configuration, you also need an external server and the corresponding software CD-ROM.

After you save the changes, you must enter the correct keycode that allows the changes to occur. The keycode is 24 characters long, and you enter it in three sets of 8 digits each called key-code1, key-code2, and key-code3. Refer to “The Command Line Interface” on page 93 of this document for details.

External memory expansion, new voice announcements, and firmware upgrades occur by inserting a PCMCIA card into the top PCMCIA slot accessible through the MICB faceplate.

Figure 6 illustrates how PCMCIA cards are loaded into the MICB faceplate slots to upgrade the MICB capacity.

Figure 6
Installing a PCMCIA card into the MICB faceplate slot



Security

A keycode is implemented to protect against unlawful MICB feature usage, because industry-standard PCMCIA cards are used as the software medium on the MICB. All upgrades of either port capacity or application software are restricted to a given MICB card and are accurately tracked to allow for satisfactory handling of field repairs and incremental upgrades.

Security is required for the following upgrades:

- port capacity upgrades
- feature enhancements
- new applications

Security is not required for the following upgrades:

- backup and restore operations
- application patching/bug fixes

Nortel Networks provides the customer with a keycode to enable installation of any desired upgrade. The keycode is entered through the CLI under “Functionality Upgrade”. The keycode is 24 characters long and is entered in three sets of 8 digits each called key-code1, key-code2, and key-code3.

Keycodes can enable additional functionality within an existing application (adding ports, features, etc.) or can be used with a PCMCIA card to provide new software or pre-recorded announcements.

Engineering guidelines

Meridian 1 general system engineering guidelines are described in *System Engineering* (553-3001-151). The following information deals specifically with engineering guidelines for the MICB planning and implementation. For system integrity and standards, refer to Appendix B: “Product integrity” on page 185.

MICB real time impact

The MICB real time impact on the Meridian 1 system is comparable to a Digital Line Card (DLC), as the call holding time is longer for conference ports than for typical two-party calls. For more information on real time impact, refer to *Capacity Engineering* (553-3001-149).

System compatibility

Each MICB port emulates a digital set assigned to an ACD agent. All ports on an MICB card belong to an ACD queue, which is controlled by the ACD DN assigned to that specific MICB card. Conferees and chairpersons calling into their conferences are routed to the ACD queue if the ACD DN assigned to the MICB card is entered at the Night Call Forward (NCFW) prompt at the time the main and chairperson DNs are defined in Overlay 23 (see Table 9, “Configuring the ACD DNs using Overlay 23,” on page 62). This programming is the same as that used for Meridian Mail.

To support a maximum of 32 ports per card, the Meridian 1 system must be running on X11 Release 22 or later software. X11 software Releases 19, 20, and 21 support a maximum of 16 ports per card. Starting with X11 Release 22, the software provides for flexible voice and data TN features, allowing configuration of up to 32 ports per card.

MICB Release 2.0 comes in port-size options of 12, 16, 24, 32, 42, 50, and 62 ports. Options of 42, 50, and 62 ports require the dual-card configuration, which involves connecting two MICB Release 2.0 cards. Each card requires one slot in the IPE shelf.

The MICB is supported by the following systems:

- Meridian 1 options 21, 21E, 51, 51C, 61, 61C, 71, 81, and 81C
- SL-1 systems NT and XT upgraded to support IPE cards
- SL-100 systems
- Option 11E, 11C

Table 4 lists the Meridian 1 modules and the card slots suitable for MICB installation.

Table 4
MICB installation into card slots in different IPE modules

Meridian 1 modules	MICB card slots
NT8D37BA/EC IPE modules, NT8D11BC/ED CE/PE modules	All available IPE card slots.
NT8D37AA/DC IPE modules	Slots 0, 4, 8, and 12
NT8D11AC/DC CE/PE modules	Slot 0

Note: MICB cards in a dual-card configuration *do not* need to reside next to each other in an IPE shelf. Software accomplishes the audio connections between the two cards. There is no hardware connection between the two cards.

Note: Power requirements *do not* limit the number of MICB card you can place in an IPE shelf. However, power requirements *do* limit the number of MICB cards in an Option 11 cabinet to six.

MICB Release 2.0 requires access to a customer LAN. The MICB card connects to the LAN through the Ethernet adapter at the I/O panel. The customer manages conferences and users through a web server.

System resources

You must consider the use of system ACD resources. If applicable, you must review Incremental Software Management (ISM) for the specific Meridian 1 system option. Each MICB card requires an ACD DN that defines the ACD queue; each MICB port represents an ACD agent that requires a TN; and each potential conference requires two ACD DNs.

For example, an MICB card in a single-card configuration that is configured to the maximum capacity of 32 ports and 10 simultaneous conferences requires the following system resources:

- 1 ACD DN assigned to the MICB card
- 32 TNs assigned to the 32 ports
- 20 ACD DNs for dialing into the potential conferences
- Therefore, a total of 21 ACD DNs and 32 TNs required for a maximally configured MICB card

  Note: If you want to use the telephone user interface (TUI) to schedule conferences, you must configure an extra (22nd) ACD DN.

A 62-port dual-card configuration has the following system requirements:

- 1 NACD DN assigned to act as the main (conference) DN for a dual-card conference
- 20 ACD DNs for the primary card (1 DN to be the ACD DN for the card, 1 DN to be the primary card chairperson DN, and 18 DNs to handle 9 potential non-dual-card conferences)
- 22 ACD DNs for the secondary card (1 DN to be the ACD DN for the card, 1 DN to be the secondary card chairperson DN, 18 DNs to handle 9 potential non-dual-card conferences, and 2 other DNs for dual-card conference purposes)
- 64 TNs assigned to the 64 ports on the dual-card configuration
- Therefore, a total of 1 NACD DN, 42 ACD DNs, and 64 TNs required for a maximally configured dual-card configuration

> ***Note:*** If you want to use the telephone user interface (TUI) to schedule conferences, you must configure an extra ACD DN for *each* card in the dual-card configuration.

These resources 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. Refer to “Engineering multiple simultaneous conferences” on page 50 for the system resource allocation.

> ***Note:*** If you use agent IDs on your system, remember that MICB *must* use successive agent IDs (e.g., 3000-3023 for 24 agent IDs). Ensure that a suitable block of agent IDs is available before you assign them.

Required software packages

In addition to the standard X11 release software, the system must be equipped with the following software packages to allow the MICB card to operate as intended:

- 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

Engineering multiple simultaneous conferences

You can configure MICB Release 2.0 to provide a maximum of 12, 16, 24, 32, 42, 50, or 62 ports. The dual-card configuration is required for 42, 50, or 62 ports. To activate the selected number of maximum ports, a keycode consisting of 24 digits is required. Refer to “The Command Line Interface” on page 93 of this document for details.

For the list of MICB features and functions, refer to “MICB functional characteristics” on page 20.

To provide multiple simultaneous conferences on one MICB card, you must specify the following system resources:

1 Activate the maximum number of MICB ports required for your site. If the current number of active ports is sufficient to meet the requirements, or if all ports are enabled, skip this step.

2 Assign one ACD DN (automatic call distribution directory number including its queue and data block). One ACD DN is required for each MICB card.

3 Specify main and chairperson DNs (directory numbers) and their data blocks. All DNs should be accessible by DID trunks. To determine the number of DNs:

a Determine the maximum number of simultaneous conferences you want to schedule on the MICB card.

Note: The more simultaneous conferences you schedule, the more system resources (i.e., available DNs) you consume. Ten simultaneous conferences per MICB card is the maximum.

b Multiply the number of conferences by 2 to determine the number of DNs required. Each conference requires 2 DNs - one for the chairperson and one that conferees call to access the conference. For example, 10 simultaneous conferences require 20 DNs.

4 Assign TNs (terminal numbers) and corresponding digital set data blocks. Each configured MICB port appears as a digital set of an ACD agent. The number of TNs is equal to the maximum number of ports provided by the MICB card. For an MICB with 32 ports active, you require 32 TNs.

Environmental and power requirements

The environmental requirements for the MICB must meet or exceed the overall Meridian 1 system requirements. The power provided for each card slot in the IPE module exceeds the power requirements for an MICB. This means there is no power limitation for the number of MICB cards you can place in an IPE shelf.

Note: Power requirements limit the number of MICB cards in an Option 11 cabinet to six.

Environmental requirements

Table 5 shows the operating and storage environmental specifications. Ideally the system should operate in a stable environment at 22° C (72° F). However, the system is designed to operate in the temperature and humidity ranges specified in Table 5.

Table 5
Environmental requirements

Condition	Environmental specifications
Operating	
Temperature	0° to 40° C (32° to 104° F)
Relative humidity	5% to 90% noncondensing
Altitude	3,048 meters (10,000 feet) max
Storage	
Temperature	–40° to 70° C (–40° to 158° F)
Relative humidity	20% to 55% noncondensing

Power requirements

Power to the MICB is provided by the IPE module power supply (AC or DC). Refer to Table 6 for a display of the MICB power requirements and also to the *Power Engineering* (553-3001-152).

Table 6
MICB power requirements

Voltage	Source	Current
+5 V	Backplane	3.0 A
+15 V	Backplane	0.25 A
Total maximum power		18.75 W

The maximum IPE module per slot power budget is 30 Watts, with an effective limitation of 20 Watts for thermal compensation. The MICB card does not exceed the power allocated for each card slot in the IPE module. This means there is no power limitation for the number of MICB cards you can place in an IPE shelf.

> ***Note:*** Power requirements limit the number of MICB cards in an Option 11 cabinet to six.

Table 7 lists the transmit and receive analog signal levels as measured at the transmitter output and receiver input in the MICB card.

Table 7
Voice signal level specifications

Signal Direction	Minimum Power	Maximum Power
Transmit signal	-55 dBm0	0 dBm0
Receive signal	-55 dBm0	0 dBm0

Note: For other signal characteristics, refer to *Summary of Transmission Parameters* (553-2201-182)

External equipment requirements

There are three interfaces available to interact with the MICB Release 2.0 card. They are:

- The Command Line Interface (CLI), for performing initial setup and configuration, performing upgrades, and generating certain reports
- The Browser User Interface (BUI), which uses a common web browser to create and manage conferences and users
- The Telephone User Interface (TUI), which enables the scheduling of simple conferences over the telephone

The following paragraphs describe the external equipment necessary to use each of these interfaces.

To access the CLI

A VT100 terminal or a personal computer emulating a terminal is used to perform certain MICB administration, configuration, maintenance, and diagnostic functions through the CLI.

For initial setup and configuration, connect the terminal to the MICB RS-232 interface or to the DB-9 connector on the NT5D52 Ethernet Adapter card installed on the I/O panel. For long-term administration and maintenance (through the CLI) telnet to the card over your LAN. Telneting requires the connection of the MICB card to the LAN through the RJ45 jack on the Ethernet adapter.

The terminal interface must be set to 9600 baud, 8 data bits, 1 stop bit, and no parity. The flow control is hard wired (never use XON/XOFF flow control).

To access the BUI

Access to the Browser User Interface (BUI) requires three things:

- a Local Area Network (LAN)
- a web server to house the BUI
- a web browser on a PC to access the BUI

LAN characteristics

Ethernet implementation over the MICB has the following LAN characteristics:

- The MICB Ethernet connection is separated from the external LAN traffic by a firewall.
- The Ethernet adapter options for MICB are:
  - NT5D52AB for the IPE module application
  - NT5D52BB for the Option 11E/11C application
- The LAN administrator assigns the IP address for the MICB. The IP address is entered over the VT100 terminal during initial setup.

Web server characteristics

The web server houses the BUI and can be either an *embedded web server* or an *external web server*.

The embedded web server

is a web server that already resides on the MICB Release 2.0 card (see Figure 1 on page 17). Setup of the embedded web server is simple and does not require any external equipment. The administrator must simply assign an IP address for the users to point their browsers to. The embedded web server supports the following user levels:

- a maximum of 100 total users configured for the card
- a maximum of 10 simultaneous users of the BUI

Note: You cannot use the embedded server option with the dual-card configuration; you must use the external server option.

The external web server

option provides a means of managing up to ten MICB Release 2.0 cards from a common point (see Figure 2 on page 18). The external web server requires the following external equipment:

- a PC to act as the web server
- a CD-ROM that houses the web server software
- a hub to connect the MICB Release 2.0 cards to the server

The PC has the following requirements:

- **Hardware requirements**
  - minimum of 200 MHz PC Pentium processor
  - minimum of 64 MB RAM
  - minimum of 1 GB for the hard drive
  - CD_ROM drive
- **Software requirements**
  - Windows NT 4.0 Server (or later)
  - Microsoft NT Service Pack 3 (or later)
  - Microsoft Internet Information Server 3.0 (or later)

The CD-ROM comes with the MICB Release 2.0 package when you select the external web server option.

The administrator must assign an IP address to each MICB card *and* to the PC server. The users point their browsers to the server's IP address, and from there have easy access to each of the MICB card in the network. With the external server option, the administrator need log in only once to access multiple cards. The external server option supports the following user levels:

- a maximum of 1000 users configured in any combination for the cards in the network (You can assign a user access to one card only.)
- a maximum of 50 simultaneous users of the BUI

Web browser characteristics

The BUI operates from a Java 1.1 level. This requires the user to have one of the following web browsers on his or her PC:

- Netscape 4.5 (or later)
- Internet Explorer 4.01 (or later) with Service Pack 1 (SP1)

To access the BUI, the user simply opens the browser and enters in the URL field the address of the MICB web server.

To access the TUI

To access the Telephone User Interface (TUI), you can use any DTMF telephone, either internal or external to your telephone system. The TUI uses a simple DTMF menu-driven system for scheduling simple conferences.

For TUI access, the administrator must designate a DN in both the BUI and the X11 system software. The administrator can choose to reserve a port for the TUI on the MICB card. If you reserve a port for the TUI, that port is not available for conferences. However, if you do not reserve a port for the TUI, and all of the ports are in use for conferences, a user cannot access the TUI.

Installation and configuration

This chapter describes the installation and configuration of the Meridian Integrated Conference Bridge (MICB) card. It describes how to configure the system software, install the MICB card, connect the MICB card to a terminal for access to the Command Line Interface (CLI), and connect the MICB card to a web server for access to the Browser User Interface (BUI). It also describes the basic MICB card configuration procedures.

Overview of system configuration and MICB installation

The following two sections provide an overview of the procedures for configuring the system software and installing the hardware for MICB. Details of each procedural step follow in this chapter.

Quick X11 system software configuration

Use the following procedure to configure the X11 system software for MICB. You can configure the system software before the installation of any of the MICB hardware.

1 Load Overlay 23 and define an ACD DN for the MICB card. Refer to Table 8, “Defining an ACD data block using Overlay 23,” on page 61.

2 Still in Overlay 23, define a block of ACD DNs that Night Call Forward (NCFW) to the ACD DN assigned to the MICB card. These are the DNs that the chairpersons and conferees dial to enter their respective conferences. Refer to Table 9, “Configuring the ACD DNs using Overlay 23,” on page 62.

Note: In addition to the chairperson and conferee DNs, you also configure the TUI DN in this step. For a dual-card setup, you also configure the transfer and link DNs in this step. To configure the conferee (or main) DN for dual-card conferences, refer to Table 11, “Configuring the main DN for dual-card conferences using Overlay 23,” on page 68.

3 Load Overlay 11 to configure the MICB ports as digital (2616) sets. Refer to Table 10, “Configuring MICB ports as digital sets using Overlay 11,” on page 63.

Quick MICB hardware installation and configuration

Use the following procedure to install the hardware for the MICB.

1 Take inventory of the MICB equipment by comparing the received equipment against the shipping documents. Ensure that the security device is in place in the MICB card.

2 Identify the card slot(s) in the IPE module or Option 11C or 11E cabinet where you intend to install the MICB card(s).

3 Install the NT5D52AB Ethernet Adapter onto the IPE module I/O panel or the NT5D52BB into Option 11C/11E tip/ring connector cutout. Refer to “Installing the Ethernet Adapter” on page 71.

4 Install the MICB card(s) in the designated card slot(s). For available card slot locations, refer to Table 4, “MICB installation into card slots in different IPE modules,” on page 48.

5 Connect a VT-100 terminal (or a PC emulating a VT-100 terminal) to the MICB card through the Ethernet adapter.

— Refer to “Connecting the terminal to an MICB card in the IPE module” on page 73 and select the appropriate connection option based on your requirements.

— Refer to “Connecting the terminal to Option 11E or 11C cabinet” on page 76 and select the appropriate connection option.

— Refer to “Configuring the VT100 terminal for CLI access” on page 84.

6 At the VT-100 terminal, enter the keycodes for the MICB cards. Refer to “Functionality Upgrade” on page 111 for keycode entry.

7 Still at the VT-100 terminal, login to the CLI as the administrator and set the IP address for the MICB card and whether the card will use the embedded server configuration or external server configuration. After this, restart the MICB card.

8 Connect the MICB card to the LAN through the RJ-45 connector on the Ethernet Adapter. You can connect the MICB card to the LAN either directly, for the embedded server configuration, or through a hub and a server, for the external server configuration. Refer to “Connect the external web server” on page 81.

Note: If you plan to use the dual-card configuration, you must use the external server.

9 Verify that the PCMCIA hard drive is installed and properly seated.

10 At the system terminal, load Overlay 32 to enable the MICB card (**ENLC l s c**).

Note: If you are using ADS data blocks, then the agent IDs must be defined in the MICB system attributes menu as described in “Cards administration” on page 127. Note that the agents IDs must be consecutive numbers within the lower and upper limit starting with the number assigned to the first agent ID.

11 Refer to “The Browser User Interface” on page 121 to schedule conferences, establish bridges, and perform administration tasks.

X11 system software configuration for the MICB

Prior to installing any of the MICB hardware, you can configure the X11 system software for the MICB card(s) through the system TTY terminal. Remember, for MICB, your Meridian 1 must be running X11 Release 19 or later for 16 ports per card or X11 Release 22 or later for 32 ports per card. Also, the Meridian 1 must have the optional software packages listed in “Required software packages” on page 50.

To configure the X11 system software for an MICB card:

1 Define an ACD data block. This defines the ACD DN that you will assign to the MICB card in Step 3 below. (Refer to Table 8.)

2 Define main and chairperson DN blocks. The Night Call Forward (NCFW) DN in all DN blocks of an MICB card must be the ACD DN (defined in the ACD block) assigned to the MICB card. (Refer to Table 9.)

Note: In addition to the chairperson and conferee DNs, you also configure the TUI DN in this step. For a dual-card setup, you also configure the transfer and link DNs in this step. To configure the conferee (or main) DN for dual-card conferences, refer to Table 11, "Configuring the main DN for dual-card conferences using Overlay 23," on page 68.

3 Define each MICB port as a digital telephone set M2616. MICB ports are defined as ACD agents in the ACD data block. (Refer to Table 10.) The digital set keys should be defined as follows:

— Key 0 - ACD with the ACD DN, CLI, and position ID

— Key 1 - Single Call Ringing (SCR) with a dedicated DN

— Key 2 - Not Ready (NRD)

— Key 3 - Make Set Busy (MSB)

— Key 4 - Call Transfer (TRN)

You must define Agent IDs in the MICB system attributes menu as consecutive numbers within the lower and upper limit. Refer to "Abnormal BUI operation" on page 154.

Defining the ACD data block

To configure the ACD data block, load Overlay 23 using the system TTY and enter the appropriate responses to the prompts listed in Table 8. This defines the ACD DN assigned to the MICB card.

Table 8
Defining an ACD data block using Overlay 23

Prompt	Response	Description
REQ	NEW	New control data block
TYPE	ACD	ACD data block
CUST	0-99	Customer number
ACDN	<ACD DN>	ACD DN assigned to the MICB card
MAXP	32	Maximum number of ACD agent positions

Note: Leave the NCFW prompt blank when defining the ACD DN assigned to the MICB card.

Defining ACD DN data blocks

To assign ACD DNs to the ACD data block that you just completed, use Overlay 23 and enter the appropriate responses to the prompts listed in Table 9. These ACD DNs serve as the DNs that the chairpersons and the conferees dial to enter their respective conferences. You also use Table 9 to define the TUI DN for each card. For a dual-card configuration, you also use Table 9 to define the primary and secondary chairperson DNs, the transfer DN, and the link DN.

Table 9
Configuring the ACD DNs using Overlay 23

Prompt	Response	Description
REQ	NEW	New control data block
TYPE	ACD	ACD data block
CUST	0-99	Customer number
ACDN	<DN#>	Conferee (main) or chairperson DN
MAXP	1	Maximum number of ACD agent positions
NCFW	<ACD DN>	ACD DN assigned to MICB card
Note: Repeat commands in this table for each ACD DN you wish to configure.		

Note: The number of DNs defined for each MICB card 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.

Defining MICB ports as digital sets

Each MICB port represents an ACD agent with the digital set 2616. Table 10 shows how to use Multi-line Telephone Administration program, Overlay 11, to configure these features.

Table 10
Configuring MICB ports as digital sets using Overlay 11

Prompt	Response	Description
REQ	NEW	Add a new data port
TYPE	2616	Digital telephone set M2616
TN	l s c	Terminal number of the MICB card
CUST	0-99	Customer number
CLS	FLXA, VCE, WTA	ACD agent (Use FLXA with X11 rls 22 and up for ports 16 through 31.)
KEY	0 ACD <ACD DN> <CLI> <pos ID>	ACD DN plus CLI plus position ID (CLI = 0 usually)
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.		

Note: 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, you must 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.

Figures 7 and 8 show a sample Overlay 20 printout of a built MICB port.

Figure 7
Overlay 20 MICB configuration (part 1 of 2)

```
>LD 20

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
```

Figure 8
Overlay 20 MICB configuration (part 2 of 2)

```
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
```

Configuring 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. Secondary, the meeting is booked on the secondary card allocating the rest of free ports for the dual-card conference. The user defines the 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 9 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. You must define for each card an ACD data block with an ACD DN in Overlay 23 as Table 8, “Defining an ACD data block using Overlay 23,” on page 61 shows.

For the primary card, configure the following DNs as Table 9, “Configuring the ACD DNs using Overlay 23,” on page 62 shows:

- DN pairs (up to 9)—These pairs serve as chairperson and conferee DNs for single-card conferences (less than 32 ports) on the primary card.
- TUI DN—This is the DN that users dial to set up single-card conferences on the primary card. You do not need to configure this DN if you don’t want to use the TUI.
- Primary chairperson DN—This is the DN that the primary chairperson of a dual-card conference dials to enter a dual-card conference. You *must* configure this DN for dual-card setup.

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

For the secondary card, configure the following DNs as Table 9, "Configuring the ACD DNs using Overlay 23," on page 62 shows:

- DN pairs (up to 9)—These pairs serve as chairperson and conferee DNs for single-card conferences (less than 32 ports) on the secondary card.
- TUI DN—This is the DN that users dial to set up single-card conferences on the secondary card. You do not need to configure this DN if you don't want to use the TUI.
- 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.) You *must* 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. You *must* configure this DN for dual-card setup.
- Secondary chairperson DN—This is the DN that the secondary chairperson of a dual-card conference dials to enter a dual-card conference. You *must* configure this DN for dual-card setup.

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

You must also configure the main DN 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 forward 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. To configure the main DN for dual-card conferences, load Overlay 23 using the system TTY and enter the appropriate responses to the prompts that Table 11 shows.

Table 11
Configuring the main DN for dual-card conferences using Overlay 23

Prompt	Response	Description
REQ	NEW	New control data block
TYPE	ACD	ACD data block
CUST	0-99	Customer number
ACDN	<DN#>	The main DN for dual-card conferences
MAXP	1	Maximum number of ACD agent positions
Note: Carriage return to the end and start again.		
REQ	NEW	New control data block
TYPE	NACD	Network ACD data block
CUST	0-99	Customer number
ACDN	<DN#>	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 12 shows a sample dialing plan for a 62-port dual-card configuration.

Table 12
Sample dialing plan for a 62-port MICB Release 2.0 configuration

Description of DNs	DNs for the primary card	DNs for the secondary card	Configure in...
ACD DN	7000	8000	Table 8
Pair DNs for single-card conferences	7001-7018 (NCFW=7000 in LD 23)	8001-8018 (NCFW=8000 in LD 23)	Table 9
TUI DNs	7019 (NCFW=7000)	8019 (NCFW=8000)	Table 9
Chairperson DNs	7020 (NCFW=7000)	8020 (NCFW=8000)	Table 9
Transfer DN	N/A	8021 (NCFW=8000)	Table 9
Link DN	N/A	8022 (NCFW=8000)	Table 9
Main DN	7021(TRGT=7000 0)	7021 (TRGT=8000 2)	Table 11

Note: Because of the number and variety of DNs that you must program for the dual-card setup, it is recommended that you create a dialing plan chart similar to Table 12. Refer to this chart when configuring the primary and secondary card attributes, including the dual-card settings, in the administration BUI.

Finally, you must also configure each port on the primary and secondary cards as a digital set. Refer to Table 10, “Configuring MICB ports as digital sets using Overlay 11,” on page 63.

MICB hardware installation and configuration overview

The MICB service can exist on Meridian 1 system options 21E, 51, 51C, 61, 61C, 71, 81, and 81C as well as Option 11E/11C and SL-1 systems that supports IPE cards.

The MICB can be installed into:

- A previously installed Meridian 1 system upgraded to run on generic software X11 Release 22 or higher to support all 32 MICB ports per card, or X11 Releases 19 to 21, which support a maximum of only 16 MICB ports per card
- A newly installed system using the latest generic X11 software

To install a new Meridian 1 system or expand an existing one, refer to *System Installation Procedures* (553-3001-210). This document provides the information on how to install, verify, and maintain the Meridian 1 system.

To complete the installation and configuration of an MICB card, you must follow the general procedures listed below.

These procedures include:

- Preparing the site
- Unpacking, inspecting, and taking inventory of the equipment
- Installing the MICB card in the selected IPE card slot, if not already installed
- Connecting the MICB card to the LAN, either directly or through the external web server
- Configuring the MICB card, including entering the keycode and defining the IP address

Installation preparation

The preparation consists of unpacking and inspecting components, taking inventory, and locating the IPE card slot(s) where you will install the MICB card(s).

Unpacking and inspection

Unpack and inspect the equipment for damage. When unpacking, follow general precautions recommended by computer and telephone equipment manufacturers:

- Remove from the installation site items that generate static charge.
- Use antistatic spray if the site is carpeted.
- Ground yourself before handling any equipment.
- Remove equipment carefully from its packaging.
- Visually inspect the equipment for obvious faults or damage. Report any damaged component to your sales representative and the carrier who delivered the equipment.

Taking inventory

After you have unpacked and visually inspected the equipment, verify that all the equipment is at the site before the installation begins. Check equipment received against the shipping documents. Note any shortages and report them to your sales representative.

MICB equipment installation

Start the installation of the MICB card and the external equipment connections associated with the MICB after:

- verifying that the preinstallation preparation has been completed (this includes verifying that all the equipment has been received undamaged)
- planning your MICB equipment, port configuration, and external equipment connection configuration (refer to “Engineering guidelines” on page 47)

Installing the Ethernet Adapter

To install the Ethernet Adapter on to the Option 11C/11E tip/ring connector:

1 Identify the 50-pin tip/ring connector at the bottom of the cabinet, which corresponds to the card slot position where the MICB will be installed.

2 Plug the 50-pin connector on the NT5D52BB Ethernet Adapter into the 50-pin tip/ring connector on the Option 11C/11E cabinet.

3 Secure the Ethernet Adapter to the cabinet.

To install the Ethernet Adapter on the IPE module I/O panel:

1. Remove the cover plate from the I/O panel at the rear of the IPE module.
2. Lift the I/O panel from the module by removing all the retaining screws.
3. Disconnect the backplane cable 50-pin connector from the I/O panel filter connector.
4. Remove the existing filter connector from the I/O panel and save the retaining screws. This filter connector corresponds to the card slot designated for the MICB card installation.
5. Install the NT5D52AB Ethernet Adapter into the designated I/O panel connector cutout using the saved retaining screws.
6. Secure the I/O panel onto the module using the retaining screws previously removed. Replace the module's cover plate.

Installing MICB cards

When installing MICB cards, follow these steps:

1. Identify the IPE card slots selected for MICB card(s). Refer to Table 4, "MICB installation into card slots in different IPE modules," on page 48.
2. Pull the top and bottom extractors away from the MICB faceplate.
3. Insert the MICB card into the card guides and gently push it until it makes contact with the backplane connector.
4. Push the top and the bottom extractors firmly towards the faceplate to insert the MICB card into the faceplate connector and to lock it firmly in place.
5. Ensure that the PCMCIA hard drive card is properly seated in the lower faceplate PCMCIA slot.
6. Observe the red LED at the top of the faceplate (the card LED). This LED should blink three times after the self-test is successfully completed and then stay ON until the MICB is software enabled.
7. Repeat steps 1 through 6 for each additional MICB card.

Connecting the terminal to an MICB card in the IPE module

You can connect the MICB terminal locally using a direct cable connection or remotely using a modem connection to provide access to the Command Line Interface (CLI) on the MICB card. You can connect the terminal to the MICB as a:

- local connection through the Ethernet Adapter DB-9 connector using a cable and a nullmodem
- remote connection through the Ethernet Adapter DB-9 connector using a cable and a modem for remote access
- remote multi-terminal access through the Ethernet Adapter RJ-45 jack and a RJ45 modular cable to the Ethernet hub

Local terminal connection through Ethernet Adapter

To connect a local terminal through the NT5D52AB Ethernet Adapter, connect the Ethernet Adapter DB-9 connector to the terminal using a direct cable. Refer to Figure 9 for the connection illustration.

1 Position the terminal on a desk near the system.

2 Verify that the Ethernet Adapter has been installed onto the I/O panel as described in "Installing the Ethernet Adapter" on page 71.

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

4 Plug the DB-9 or DB-25 male connector at the other end of the terminal cable into the RS-232 connector on the terminal. (No nullmodem is necessary). If the connection requires a gender changer, you can obtain one at your local electronics store. (Refer to "Configuring the VT100 terminal for CLI access" on page 84 for further information.)

Remote terminal connection using Ethernet Adapter and modem

Remote terminal connection can be established by connecting the DB-9 Ethernet Adapter connector through a modem to a distant terminal. Refer to Figure 9 for the connection illustration.

1 Verify that the Ethernet Adapter has been installed onto the I/O panel as described in "Installing the Ethernet Adapter" on page 71.

2 Plug the terminal cable DB-9 female connector into the DB-9 male connector on the Ethernet Adapter 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 DB-25F/DB-25M nullmodem adapter.

4 Plug the DB-25 male connector of the nullmodem adapter DB-25F/DB-25M into the DB-25 female connector on the modem.

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.

Remote multi-terminal connection through Ethernet

You can access the MICB card from multiple terminals through the Ethernet. See Figure 9 for the connection illustration.

1 Verify that the Ethernet Adapter has been installed onto the I/O panel as described in "Installing the Ethernet Adapter" on page 71.

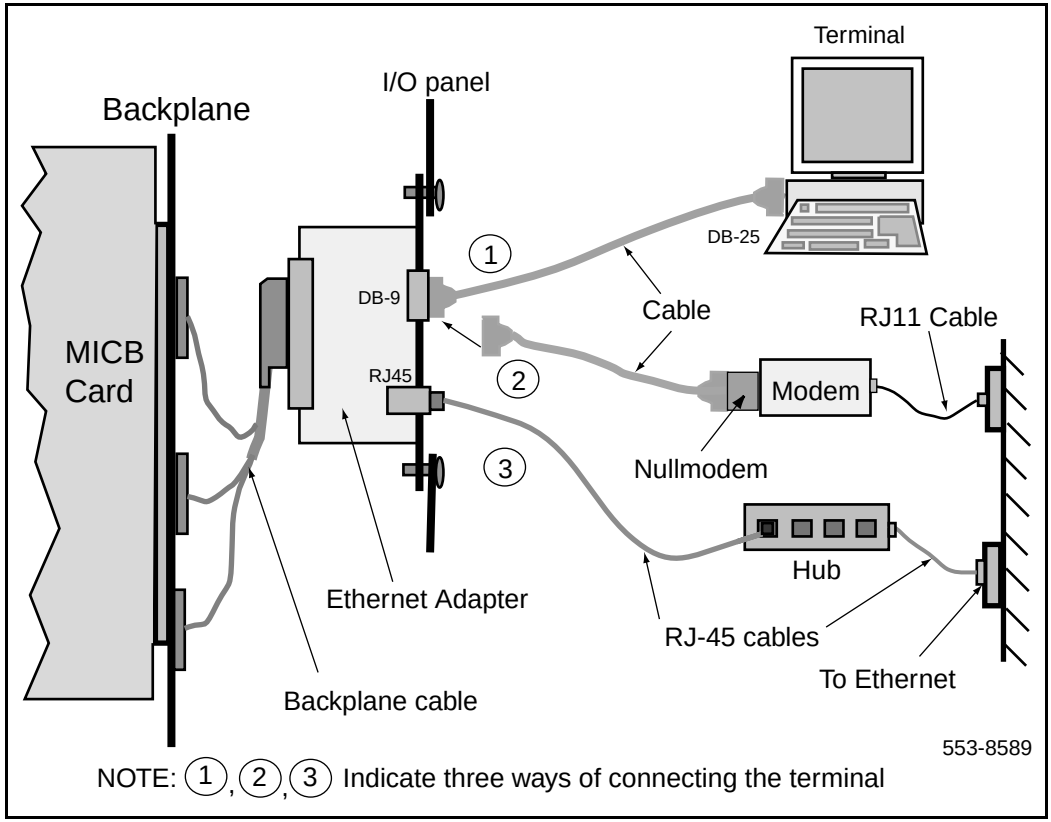
2 Plug the modular cable RJ-45 plug into the RJ-45 jack on the Ethernet Adapter.

3 Plug the RJ-45 plug at the other end of the modular cable into the Ethernet hub.

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

Figure 9 illustrates the I/O connector bracket connection to the MICB card, the terminal, and the Ethernet.

Figure 9
Terminal connection through the Ethernet Adapter



Connecting the terminal to Option 11E or 11C cabinet

You can connect the MICB terminal locally using a direct cable connection or remotely using a modem connection to provide access to the Command Line Interface (CLI) on the MICB card. You can connect the terminal to the MICB as a:

- local connection through the Ethernet Adapter DB-9 connector using a cable and a nullmodem
- remote connection through the Ethernet Adapter DB-9 connector using a cable and a modem for remote access
- remote multi-terminal access through the Ethernet Adapter RJ-45 jack and a RJ45 modular cable to the Ethernet hub

Local terminal connection through Ethernet Adapter

To connect a local terminal through the Ethernet Adapter on the Option 11C or 11E, connect the Ethernet Adapter DB-9 connector to the terminal using a direct cable. Refer to Figure 9 “Terminal connection through the Ethernet Adapter” on page 75 for the connection illustration.

1 Position the terminal on a desk near the system.

2 Verify that the Ethernet Adapter has been installed onto the Option 11C or 11E.

3 Plug the terminal cable DB-9 female connector into the DB-9 male connector on the Ethernet Adapter 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. (No nullmodem is necessary). If the connection requires a gender changer, you can obtain one at your local electronics store.

Remote terminal connection using Ethernet Adapter and modem

Remote terminal connection to the Option 11C or 11E can be established by connecting the DB-9 Ethernet Adapter connector through a modem to a distant terminal. Refer to Figure 9 “Terminal connection through the Ethernet Adapter” on page 75 for the connection illustration.

1 Verify that the Ethernet Adapter has been installed onto the Option 11C or 11E system.

2 Plug the terminal cable DB-9 female connector into the DB-9 male connector on the Ethernet Adapter 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 DB-25F/DB-25M nullmodem adapter.
4. Plug the DB-25 male connector of the nullmodem adapter DB-25F/DB-25M into the DB-25 female connector on the modem.
5. Plug the modular 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.

Remote multi-terminal connection through Ethernet

You can access the MICB card in the Option 11C or 11E from multiple terminals through the Ethernet. Refer to Figure 9 “Terminal connection through the Ethernet Adapter” on page 75 for the connection illustration.

1. Verify that the Ethernet Adapter has been installed into the Option 11C or 11E.
2. Plug the modular cable RJ-45 plug into the RJ-45 jack on the Ethernet Adapter.
3. Plug the RJ-45 plug at the other end of the modular cable into the Ethernet hub.
4. Make the rest of the Ethernet connections as required using standard Ethernet connection rules.

Dual-card installation and setup

A feature that is new for MICB Release 2.0 is the ability to combine two MICB Release 2.0 cards together in a “dual-card configuration”. This dual-card configuration enables a single conference to take place on two cards and have up to 62 participants. In the dual-card configuration, we refer to one card as the *primary* card and the other as the *secondary* card. Each of these cards can host “single-card conferences” of three to 32 participants; or you can schedule a “dual-card conference”, which occupies ports on both cards.

> ***Note:*** MICB cards in a dual-card configuration *do not* need to reside next to each other in an IPE shelf. Software accomplishes the audio connections between the two cards. There is no hardware connection between the two cards.

To set up a dual-card configuration, do the following:

1 Install the two cards and their ethernet adapters the same as for normal, single-card installation. Refer to “Installing the Ethernet Adapter” on page 71 and “Installing MICB cards” on page 72.

Note: The two cards do not need to reside next to each other in the shelf or cabinet. There is no physical connection between the two cards in the dual-card configuration. Software handles all of the communication between the cards.

2 Enable the two cards through Overlay 32. Refer to “Enabling the MICB card” on page 83.

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**), and enter the following:

— the subnet mask, the gateway address, and the IP address (in the System Attributes Editor—enter **sa** then **sy**)

Note: After you enter the Ethernet information, the CLI asks whether you want to restart the card. Select **No** at this point.

— “EXTSRV” for the external server configuration (in the Modify Software Functionality—enter **pa** then **sf**)

Note: After you select the external server configuration (EXTSRV), the CLI asks whether you want to restart the card. Select **Yes**.

5 From a PC terminal, “ping” each MICB card to ensure that they have a proper connection to the LAN. To ping an IP card, do the following:

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

— In the “Open:” field, enter “ping <IP address>” where <IP address> is the IP address of one of the MICB cards.

— 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 properly and you can proceed. 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. Refer to "Configuring DNs for a dual-card conference" on page 66 for detailed instructions.

7 Configure each port on the two cards as a digital set. Refer to "Defining MICB ports as digital sets" on page 63 for detailed instructions.

8 Set up the external server. Refer to "Connect the external web server" on page 81 for detailed instructions.

9 Open up your web browser on your PC. In the URL field of the browser, enter the following: **<server IP address>/micb/micb.html**. <server IP address> is the IP address of the external server.

10 Log into the BUI on the external server (defaults: **admin** and **000000**) and select the Cards page of the MICB Administration Utility (Figure 18 on page 126).

Note: Refer to "Cards administration" on page 127 for details on configuring a cards parameters.

11 Click on an empty field in the 'Card Name' list and enter the card name and card ID for the primary card. Enter the primary card's IP address in the card details section. Click **Apply**. This establishes the external server's connection to the primary card.

12 Click on **Display Details** and enter the rest of the attributes for the primary card, including the card type as "Primary", the TUI DN (if applicable), and the DN pairs for single-card conferences. Click **Apply**.

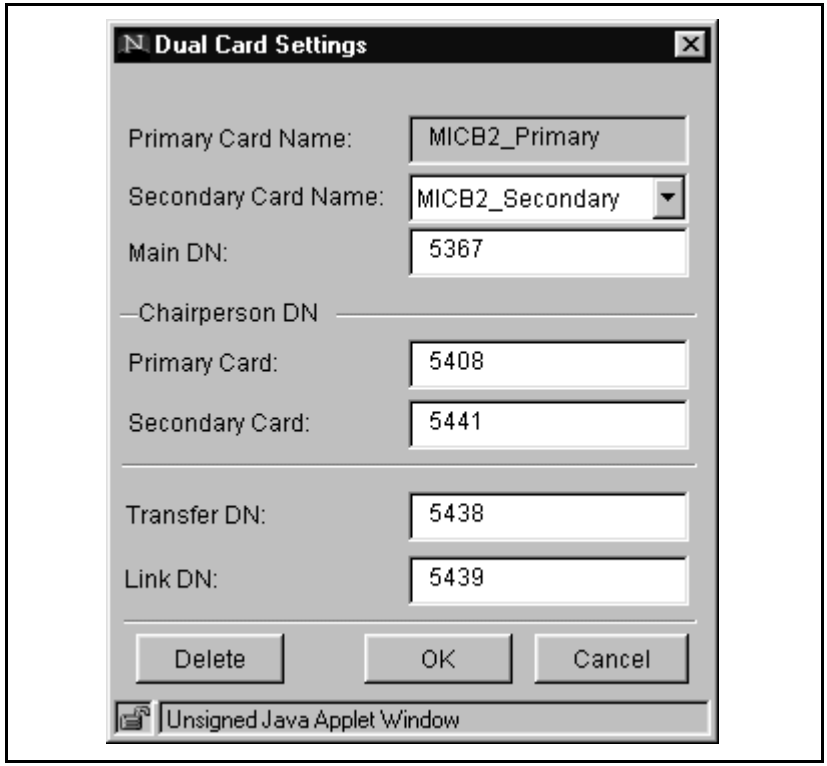
Note: Do not set the "Dual Card Settings" yet. You must first define the secondary card's attributes.

13 Click on another empty field in the 'Card Name' list and enter the card name and card ID for the *secondary* card. Enter the secondary card's IP address in the card details section. Click **Apply**. This establishes the external server's connection to the secondary card.

14 Click on **Display Details** and enter the rest of the attributes for the secondary card, including the card type as "Secondary", the TUI DN (if applicable), and the DN pairs for single-card conferences. Click **Apply**.

15 Click on the primary card's name in the 'Card Name' list and click on the **Display Details** button. Click on the **Dual Card Settings...** button to open the "Dual Card Settings" dialog box. Select the 'Secondary Card Name' from the combo box. Enter the main DN, the primary and secondary chairperson DNs, the transfer DN, and the link DN that you configured on the X11 system in step 6. Click **OK** to save these parameters and close the dialog box. Figure 10 shows an example of "Dual Card Settings..." for a primary card.

Figure 10
Sample dual card settings



16 At the top-left of the MICB Administration Utility, click on the **Properties** button to open the “System Properties” dialog box (Figure 23 on page 138). Enter the ‘Mail server IP address’ and click **OK** to establish email notification to users.

Note: For email notification to work, the mail server IP address *must* be ‘unrestricted’ and able to send email to everyone on the network.

17 Define users for the cards as “Users administration” on page 130 describes. Users can then begin scheduling dual-card conferences.

Connect the external web server

The external server configuration supports up to 1000 users and 50 simultaneous users. You must download the server software to an external server via a CD-ROM. The external server is a PC with the following specifications:

- **Hardware requirements**
  - minimum of 200 MHz PC Pentium processor
  - minimum of 64 MB RAM
  - minimum of 1 GB for the hard drive
  - CD_ROM drive
- **Software requirements**
  - Windows NT 4.0 Server (or later)
  - Microsoft NT Service Pack 3 (or later)
  - Microsoft Internet Information Server 3.0 (or later)

Note: You *must* use the external server configuration to have the ability to link two MICB cards together for a 62-port configuration.

External server setup

To set up the external web server, do the following:

1. Obtain an IP address for the PC from your network administrator. You must also know the IP addresses for the MICB cards that your server will serve.
2. Connect the PC to the LAN and start the PC.
3. Place the MICB Server CD-ROM in the CD-ROM drive or your server. Wait for the "MICB Server Setup" window. (The setup program runs automatically.)
4. Follow the instructions until the setup program finishes. For example:
   - — At the "Welcome" window, click **Next** to continue.
   - — At the "Choose Destination Location..." window, click **Next** to continue.
   - — At the "Information" window, click **OK**.

   At this point, setup is complete.
5. Start the MICB Server program in *one* of the *three* following ways:
   - — Select **Start->Programs->Micb Server Application->Micb Server** from the server desktop.
   - — In the "C:\WINDOWS\Start Menu\Programs\MICB Server Application" window, double-click on the "MICB Server" icon.
   - — Restart the PC. The MICB Server program runs automatically after you restart the PC.
6. Minimize the "MICB Server" window. DO NOT close the window, because the program must run at all times. You can close any other windows that are open.

Configure cards and users through the external server

Once the MICB Server program is set up and running, do the following to configure cards and users through the external server:

1. Run your browser, either Netscape or Internet Explorer.
2. In the URL field, type: **http://<server IP address>/micb/micb.html**, where **<server IP address>** is the IP address of your external server.
3. Login as an administrator. The default login ID and password are **admin** and **000000** (six zeros), respectively.

4 Define all available cards and users. For more information, refer to “Cards administration” on page 127 and “Users administration” on page 130.

Upgrade the MICB PC server

To upgrade the external server to a new release, do the following:

1 Shut down the MICB Server program.

2 Place the upgrade CD-ROM in the CD-ROM drive of your PC server.

3 Follow steps 4-6 of the external server setup procedure.

Note: If you receive the “ComponentMoveData Error Information” message during setup, the MICB Server program is running. You must close the MICB Server window and start the setup again.

Enabling the MICB card

To enable the MICB, load the Network and PE Diagnostic program Overlay 32 into the system memory using the system TTY to execute the **ENLC l s c** command, where **l** is the loop, **s** is the module or shelf, and **c** is the card to be enabled.

Configuring MICB

Before you can proceed with conference administration through the BUI, you must:

1 Configure a VT100 terminal for CLI access.

2 Enter the keycode information.

3 Set the LAN parameters, including IP address, gateway address, and subnet mask.

4 Restart the card.

5 Define card and user details through the BUI.

The following sections describe each of these steps.

Note: “The Browser User Interface” on page 121 describes the use of the BUI in configuring and administering of all MICB conference functions.

Configuring the VT100 terminal for CLI access

To access the CLI, you must use a VT100-type terminal. Refer to "Connecting the terminal to an MICB card in the IPE module" on page 73 or "Connecting the terminal to Option 11E or 11C cabinet" on page 76 for instructions on connecting the VT100 terminal to the MICB. Specify the VT100-type terminal interface characteristics to ensure compatibility with the MICB RS-232 interface.

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.

Enter the keycode information

When you first connect a VT100 terminal to your MICB card, the CLI appears and prompts you to enter keycode information. To enter the keycode information, do the following:

1 At the "Modify, Save, Cancel:" prompt, enter **m** to **Modify**.

2 At the "max conf_ports (0):" prompt, enter the number of ports that corresponds to your MICB Release 2.0 keycode (e.g., 32).

3 At the "Card Feature (BASIC, (1-ADVANCED)):" prompt, press **Return** for BASIC functionality.

Note: The ADVANCED option is in place for future call accounting capability. This capability is not available at the time of the printing of this document.

4 At the "Modify, Save, Cancel:" prompt, enter **s** to **Save** your modifications.

5 At the keycode prompts, enter "key-code1", "key-code2", and "key-code3" (eight characters each) for MICB Release 2.0 functionality.

Set the LAN parameters

If the keycode entry is successful, the CLI notifies you and presents you with a login prompt. You can now enter the LAN parameters for your MICB with the following procedure:

1 Once the system successfully registers the MICB Release 2.0 keycode, log into the CLI as **admin**.

2 At the “SAdmin, SMint, PAdmin, PMaint, RGen, LOgout, ?:” prompt, enter **sa** to access **System Administration**.

3 At the “SYstem, REcorder, ?:” prompt, enter **sy** to access **System Attributes**.

4 Enter the system attributes of the MICB Release 2.0 card, including the IP address, gateway, and subnet mask. Refer to “System Attributes Editor” on page 100 for details.

5 At the “Modify, Save, Cancel:” prompt, enter **s** to **Save** the system attributes.

Note: If you are connecting your MICB to an external web server, you must also select the external server option (EXTSRV). You can find this option in the Modify Software Functionality section in the CLI. Refer to “Modify Software Functionality” on page 113 for more information.

6 At the “Restart MICB?” prompt, enter **Yes**.

7 From a PC terminal, “ping” the MICB card to ensure that it has a proper connection to the LAN. To ping an MICB card, do the following:

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

— In the “Open:” field, enter “ping <IP address>” where <IP address> is the IP address of the MICB card.

— 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 properly and you can proceed. If you receive the message, “Request timed out.”, there is a problem with the LAN connection.

Define card and user details through the BUI

Note: You are now ready to access the Browser User Interface (BUI) to configure card attributes, users, and conferences. To access the BUI, you must have Netscape Communicator 4.5+ or Internet Explorer 4.01+ with service pack 1.

Before you can administer conferences on an MICB card, you must first define the card's details through the BUI. To define an MICB Release 2.0 card's details, do the following:

1 Open your web browser on your PC, enter the following in URL field:

<MICB card IP address>/micb.htm for an embedded server, or **<PC server IP address>/micb/micb.html** for an external server,

and press **Return**.

2 At the MICB Release 2.0 login page, enter **admin** for the login and **000000** (six zeros) for the password. This brings you to the MICB Administration Utility. (See "Abnormal BUI operation" on page 154.)

3 Click on the **Cards** tab of the MICB Administration Utility to configure card attributes.

4 Click on an open field in the "Card Name" column and enter a name for the card, up to 20 characters.

Note: If you entered a card name in the System Attributes of the CLI, *and* you are using the embedded server option, the name of the card will already be in the "Card Name" column.

5 Click on the "Card ID" field next to the card name and enter the appropriate card ID.

6 Click on the **Display Details** button at the bottom-left of the screen. This displays (at the right side of the screen) the details of the selected card.

Note: If you use the embedded server option, certain details of the card already appear at the right, such as hardware and software information and the card's IP address.

7 In the card details section, enter the appropriate details for the selected card, including the card type, the TUI DN, and the conference DN pairs.

Note: If you use the external server option, you must first enter the card's IP address and select the appropriate card type; then click **Apply**. This establishes the external server's connection to the card. You can then proceed to configure the rest of the card attributes.

8 Be sure to configure any necessary **Group Calls** and **Weekdays** settings.

9 Program any permanent bridges from the original MICB in the **Permanent Conferences** settings.

10 Click **Apply** to save all of the card attributes.

11 At the top-left of the MICB Administration Utility, click on the **Properties** button to open the "System Properties" dialog box (Figure 23 on page 138). Enter the 'Mail server IP address' and click **OK** to establish email notification to users.

Note: For email notification to work, the mail server IP address *must* be 'unrestricted' and able to send email to everyone on the network.

12 Click on the **Users** tab of the MICB Administration Utility to configure users for your MICB card.

13 Click **Apply** after you define each user to save all of the user attributes.

14 Notify the users of their user (login) ID and passwords so that they can access the BUI and TUI.

Note: Refer to "Cards administration" on page 127 and "Users administration" on page 130 for further details.

Users can now access the BUI and the TUI to define and manage conferences.

MICB password security

To protect functional and software upgrades, the MICB provides the *Protected Administration* menu, accessible in the CLI. This menu allows you to edit passwords and perform functional and software upgrades.

For details of how to upgrade the MICB functions and software, refer to "Protected Administration menu" on page 110.

Upgrade MICB to MICB Release 2.0

This section describes how to upgrade the original MICB to the new MICB Release 2.0. The upgrade to MICB Release 2.0 requires the following:

- the newer NT5D51AC card, if you have the older NT5D51AA card (The NT5D51AB card supports MICB Release 2.0.)
- an Ethernet adapter cable—NT5D52AB for IPE modules and NT5D52BB for Option 11s (Order this if you don't already have one.)
- an NT5D62BB PCMCIA disk (NT1438BC in Europe), which comes with your upgrade kit
- a new keycode to activate MICB Release 2.0 functionality, which comes with your upgrade kit

We can look at this upgrade procedure as a collection of six short procedures. The six procedures, which this section describes in detail, are:

- Procedure 1—upgrade the hardware
- Procedure 2—enter the keycode information in the CLI
- Procedure 3—configure the system attributes in the CLI
- Procedure 4—configure the card attributes in the BUI
- Procedure 5—configure the users in the BUI
- Procedure 6—configure the conferences in the BUI

To upgrade MICB to MICB Release 2.0, do the following:

Procedure 1—upgrade the hardware

1 Access the MICB Command Line Interface (CLI) and print out or make note of *all* scheduled conferences and permanent ("forever") bridges.

Note 1: You *must* reenter the scheduled conferences and permanent bridges as part of the upgrade process; this information does not transfer during the upgrade.

2 Make note of the MICB card's IP address, Gateway, and subnet mask.

Note 1: If you connected the original MICB to the LAN, you can obtain this information from the "System Attributes" in the CLI. Refer to "System Administration menu" on page 100.

Note 2: If you *did not* connect the original MICB to the LAN, you must obtain this information from your network administrator.

Note 3: You must connect MICB Release 2.0 to your LAN for BUI access. You must enter (or reenter) this Ethernet information as part of the upgrade process.

3 If you haven't already done so, connect the Ethernet adapter to the I/O panel and your LAN. Refer to "Installing the Ethernet Adapter" on page 71 for instructions.

4 Log into Overlay 32 from you system terminal. Disable the original MICB pack with the DISC command.

5 Remove the original MICB card from the module.

If your original MICB used the NT5D51AB card, replace the NT5D62BA PCMCIA disk in the lower drive (drive A:) with the NT5D62BB (NT1438BC in Europe) PCMCIA disk from your upgrade kit.

If your original MICB used the NT5D51AA card, insert the NT5D62BB (NT1438BC in Europe) PCMCIA disk from your upgrade kit into the lower drive (drive A:) of your new NT5D51AC card. Also, transfer the security device from the old card to the new card.

6 Insert the MICB card with the new NT5D62BB (NT1438BC in Europe) PCMCIA disk into the slot you used for your original MICB.

7 Enable the MICB Release 2.0 card with the ENLC command from Overlay 32.

Procedure 2—enter the keycode information in the CLI

8 Return to the terminal that displays the CLI. At the "Modify, Save, Cancel:" prompt, enter **m** to **Modify**.

9 At the "max conf_ports (0):" prompt, enter the number of ports that corresponds to your MICB Release 2.0 keycode (e.g., 32).

10 At the "Card Feature (BASIC, (1-ADVANCED)):" prompt, press **Return** for BASIC functionality.

Note: The ADVANCED option is in place for future call accounting capability. This capability is not available at the time of the printing of this document.

11 At the "Modify, Save, Cancel:" prompt, enter **s** to **Save** your modifications.

12 At the keycode prompts, enter "key-code1", "key-code2", and "key-code3" (eight characters each) for MICB Release 2.0 functionality. The keycode is part of your upgrade kit.

Procedure 3—configure the system attributes in the CLI

13 Once the system successfully registers the MICB Release 2.0 keycode, log into the CLI as **admin**.

14 At the "SAdmin, SMint, PAdmin, PMaint, RGen, LOgout, ?:" prompt, enter **sa** to access **System Administration**.

15 At the "SYstem, REcorder, ?:" prompt, enter **sy** to access **System Attributes**.

16 Modify/update/reenter the system attributes of the MICB Release 2.0 card, including the IP address, gateway, and subnet mask. Refer to "System Attributes Editor" on page 100 for details.

17 At the "Modify, Save, Cancel:" prompt, enter **s** to **Save** the system attributes.

18 At the "Restart MICB?" prompt, enter **Yes**.

Note: You are now ready to access the Browser User Interface (BUI) to configure card attributes, users, and conferences. To access the BUI, you must have Netscape Communicator 4.5+ or Internet Explorer 4.01+ with service pack 1.

Procedure 4—configure the card attributes in the BUI

19 Open your web browser on your PC, enter the following in URL field: **<IP address>/micb.htm**, and press **Return**.

Note: If you intend to access this upgraded MICB through an external server, enter **<server IP address>/micb/micb.html** in the URL field.

20 At the MICB Release 2.0 login page, enter **admin** for the login and **000000** (six zeros) for the password. This brings you to the MICB Administration Utility. (See “Abnormal BUI operation” on page 154.)

21 Click on the **Cards** tab of the MICB Administration Utility to configure card attributes.

22 Click on an open field in the “Card Name” column and enter a name for the card, up to 20 characters.

Note: If you entered a card name in the System Attributes of the CLI, *and* you are using the embedded server option, the name of the card will already be in the “Card Name” column.

23 Click on the “Card ID” field next to the card name and enter the appropriate card ID.

24 Click on the **Display Details** button at the bottom-left of the screen. This displays (at the right side of the screen) the details of the selected card.

Note: If you use the embedded server option, certain details of the card already appear at the right, such as hardware and software information and the card’s IP address.

25 In the card details section, enter the appropriate details for the selected card, including the card type, the TUI DN, and the conference DN pairs.

Note: If you use the external server option, you must first enter the card’s IP address and select the appropriate card type; then click **Apply**. This establishes the external server’s connection to the card. You can then proceed to configure the rest of the card attributes.

26 Be sure to configure any necessary **Group Calls** and **Weekdays** settings.

27 Program any permanent bridges from the original MICB in the **Permanent Conferences** settings.

28 Click **Apply** to save all of the card attributes.

29 At the top-left of the MICB Administration Utility, click on the **Properties** button to open the “System Properties” dialog box (Figure 23 on page 138). Enter the ‘Mail server IP address’ and click **OK** to establish email notification to users.

Note: For email notification to work, the mail server IP address *must* be ‘unrestricted’ and able to send email to everyone on the network.

Procedure 5—configure the users in the BUI

30 Click on the **Users** tab to access the Users page of the MICB administration utility (Figure 19 on page 130).

31 Define users according to “Users administration” on page 130.

Note: Here you can define as users those who had operator (**oper**) access on the original MICB. This will allow them to continue scheduling their own conferences.

32 Click **Apply** after you define each user to save all of the user attributes.

33 Define yourself as a user of type “Superuser” so that you can enter the conference information that you took note of in Step 1.

34 Click **Exit** to exit the MICB administration utility.

Procedure 6—configure the conferences in the BUI

35 Log into the MICB BUI again, this time using your “Superuser” login ID and password.

36 Reenter the scheduled conference that were on the original MICB. Refer to “MICB user BUI description” on page 139 for instructions.

This completes the upgrade of the original MICB to MICB Release 2.0. You can now continue with normal operation and administration of the MICB Release 2.0, which the rest of this document describes.

The Command Line Interface

Introduction

The MICB Command Line Interface (CLI) enables an administrator to perform various system administrative functions. You can access the CLI through a VT-100 type terminal or a PC running a terminal emulation program, both of which connect directly to the RS-232 port on the MICB card. You can also access the CLI over the Ethernet through a hub that connects to the RJ-45 port on the MICB card. The following system administration functions are accessible through the CLI:

- Configuring system parameters
- Displaying log files contents
- Entering the keycode
- Displaying conference statistics
- Performing system maintenance
- Performing MICB functional and software upgrades

Before you can use a terminal to access the CLI, you must configure the interface parameters as described in “Installation and configuration” on page 57.

Login screen

The logon screen appears when you press the **Enter** key after you connect a terminal to the MICB RS-232 port or telnet to the MICB card. This is the initial screen, which displays the general status of the MICB card and conferences in progress. This includes:

- Start time and duration of the first twenty active and future conferences

- DNs for the conference and the chairperson (**DN** lists the numbers conferees dial to enter conferences; **ch_DN** lists the chairperson DNs.)
- Number of ports occupied and, in parentheses, the maximum number of ports reserved for that conference
- Status of each conference (*bridge* is permanent, *expanded* is using more ports than have been reserved, *active* is conference in progress, and *next* is conference scheduled to start shortly)
- Locked, indicating whether a conference is accessible by a conferee that has not yet joined the conference
- Chairperson name and title for each conference

Note: When you first install the MICB, the initial screen (Table 13) can display dummy conference scheduling that remains from factory testing or lab testing. Ensure that you use the Browser User Interface (see "The Browser User Interface" on page 121) to delete all dummy information that appears in the initial screen before you schedule conferences.

Table 13
Initial screen showing the current MICB configuration status

Meridian Integrated Conference Bridge

Card name: first_card **10005666**

Start	Duration	DN	ch_ DN	# Ports	Status	Locked	Chair-person	Title
00:00	forever	3080	3081	0(6)	bridge	yes	-	bridge 3080
09:15	2:45	3020	3021	7(5)	expand	no	Bob	Y Report
10:30	1:30	3010	3011	4(6)	active	yes	Barry	X Gate 2
11:10	2:00	3000	3001	0(3)	active	no	Dale	ZGate 3
13:15	2:00	3030	3031	0(8)	next	-	Jim	ZSales

Total ports in use: 11(20) Last refreshed: March 15, 1999 11:30

Login:

Logging in

The administrator logs in by entering the password at the 'Login:' prompt. The default password is **admin**, which the administrator can change after logging in. The administrator uses the CLI to perform the following functions:

- **System administration**, such as editing system attributes and recording brandline greetings
- **System maintenance**, such as performing system tests, running reports, archiving and restoring the database, and restarting the card
- **Protected administration**, such as editing and resetting passwords, upgrading software, and modifying software functionality
- **Port maintenance**, such as displaying the status of ports and disconnecting ports
- **Report generation**, such as running the meetings log

The administrator can change the default password. If you cannot remember the password, reset the password as the following example shows:

Login: **rst**
Enter key-code1 (8 characters): **12345678**
Enter key-code2 (8 characters): **81234567**
Enter key-code3 (8 characters): **78123456**
Passwords have been reset.

Login: **admin**

The administrator can then assign a new password by accessing the *Protected Administration* menu.

General administration procedures

General administration procedures are rules you must follow when modifying default or existing parameters that define the MICB system and conference operation. These apply when using:

- General administration commands
- Object modify procedure

- Collection modify procedure
- Custom recording procedure

General administration commands

When you must modify system administration parameters, you use one or more of the following commands:

- **M**odify - Enter **M** to indicate that you wish to modify one or more parameters.
- **S**ave - Enter **S** to save modified parameters.
- **C**ancel - Enter **C** to cancel the modification and allow the parameter to retain its previous value.

After the session is complete, the screen displays again the *Modify, Save, or Cancel*: command line for additional modification of parameters, if required.

To navigate from menus to other menus or to display help, use the following terminal keys:

- ***** - Returns you to the previous menu
- **/** - Returns you to the top menu level
- **?** - Help, which assists you with commands in the current menu

Object modify procedure

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 specifies the name and the current value of the attribute as follows:

attribute_a (current_value_a): **new_value_a**

attribute_b (current_value_b): .

For each prompt, the user may respond in three ways:

- **<cr>** - accepts the current value by pressing the Enter key
- **value** - changes the attribute by entering a new value
- **.** - terminates the session by entering "**.**" (dot)

In some cases the system displays the current value and a list of available values to select. Example:

attribute_c (current_c, (1-aaaa, 2-bbbb, 3-cccc)): 2
(where the value of attribute_c has been changed to bbbb)

After the session is complete the system lists the new set of values and prompts you to *Modify, Save, or Cancel* the modification(s).

Collection modify procedure

This procedure modifies, deletes, or adds an entry to a collection of items of the same type, such as for example, port capacity.

You can move through the list of items by entering **<cr>** to skip the item, enter a **command** to modify the item, or enter **.** (dot) to exit the list. The **command** can be:

- **m** - to modify the item in the list using object modify procedure
- **d** - to delete a selected item in the list
- **i** - to insert a list of items above the currently selected item
- **a** - to append a list of items below the currently selected item

For insert and append commands, the system prompts you to add a new item. Terminate this sequence by entering the **.** (dot). When the system executes the command(s), the program gives you the option to *Modify, Save, or Cancel* the changes. You *must* enter **S**ave to keep the new changes.

When you reach the end of the list, the system displays or prints the new list and prompts you again to *Modify* or *Exit* the list.

Custom (brandline) greeting

Name the custom greeting file BRANDLIN.WAV when you create it over the telephone set. You must record a separate custom greeting for each language.

A custom greeting is used during the conference to provide a customized greeting, in one of the available languages, that specifically identifies the conference or the company holding the conference. This greeting is an alternative to the standard “Welcome to the conference call.” greeting.

Customer greeting files provide:

- customer recording of a brandline (custom) greeting in a specific language
- user selection of one of the two greeting options:
  - brandline (custom) greeting
  - standard greeting

Use the telephone set method to record a custom greeting such as, for example, “Welcome to the Nortel Networks conference bridge”. The custom greeting is identified as BRANDLIN.WAV to distinguish it from other recorded files. For telephone set message recording, refer to “Audio Recorder” on page 102.

The Main Menu

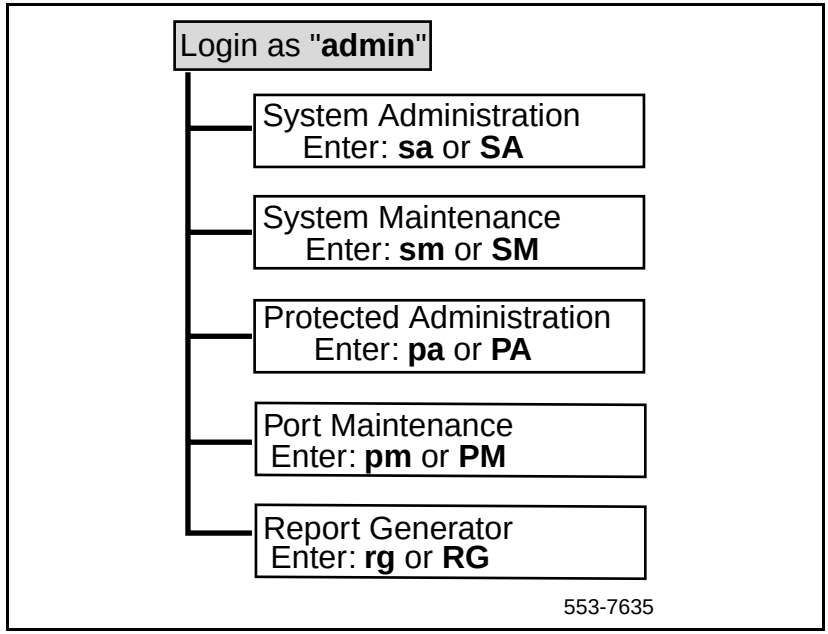
The Main Menu is the first menu to appear after the administrator logs in. The Main Menu lists administration and maintenance menus and appears as follows in the CLI:

SAdmin, SMint, PAdmin, PMaint, RGen, LOgout, ?:

To access on of the menus, enter the first two letters of the menu and press the **Enter** key. For example, to access the System Administrator menu, enter **sa**. Enter **lo** to logout.

Figure 11 illustrates the Main Menu and its submenus. After you login as an administrator, you can access the various submenus; however, you must follow general administration procedures.

Figure 11
Main Menu



Help display

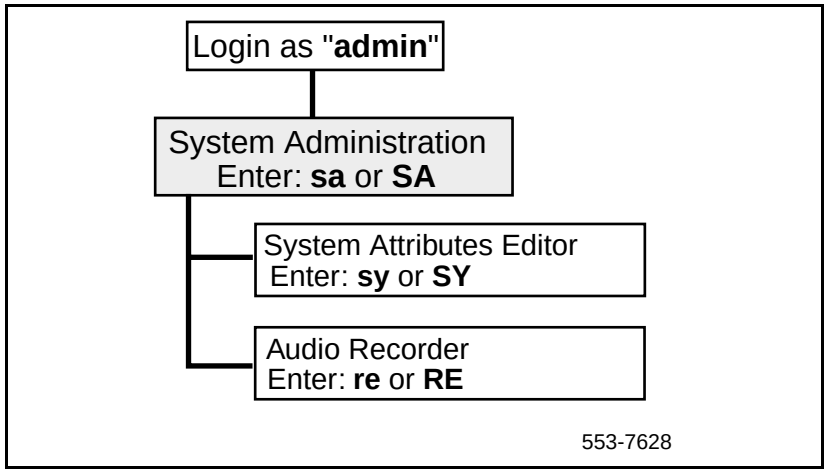
When you choose the help command (**?**), the system lists the commands that relate to the Main Menu, as follows:

Short command	Full command	Explanation
sa	SAdmin	System Administration directory
sm	SMaint	System Maintenance directory
pa	PAdmin	Protected Administration directory
pm	PMaint	Port Maintenance directory
rg	RGen	Report Generation directory
lo	LOgout	Logout

System Administration menu

To access the System Administration menus from the Main Menu, enter **sa** or **SA** or the full command (**SAdmin**). Figure 12 illustrates the System Administration screen and all the menus accessible from this screen.

Figure 12
System Administration menu



System Attributes Editor

Use this menu to modify system attributes. These are:

- **card name** - a character string with maximum length of 10 characters. The name appears at the top of the Login screen, if you specify one.
- **idle time-out** - the time the terminal is idle before it automatically logs out and displays the Login screen with general system status. The default time-out is 20 minutes and the range is from 20 to 60 minutes.
- **refresh period** - the Login screen refresh (update) time when the terminal is not in use. The default is 5 minutes and the range is from 0 to 60 minutes. Enter 0 if you wish to disable system status display.
- **report aging** - the number of days the system maintains old reservation records, associated meeting log reports, and maintenance reports. The default is 32 days and the range is from 0 to 32 days. If you select 0, the system deletes the day's files at the end of the day.

- **short occupancy** - a threshold used to detect short usage of a conference port. If the connection is less than the threshold, it can indicate a bad connection or an incorrect DN dialed. When this condition is detected, the system increments a counter and when counters are checked, those with peg-counts are displayed as potential problems. The default is 10 seconds and the range is 0-30 seconds. To disable the short occupancy count, set the threshold to 0.
- **application traffic report** - default is 0 to disable the report. Range 1-24 enables you to select the number of reports that the system issues every hour-on-the-hour.
- **disconnect a lone participant** - defines the amount of time a participant can be alone in the conference. When the time elapses, the MICB disconnects the participant. The default is 0 minutes and the range is 0-720 minutes. Select 0 to disable this feature.

Ethernet defining attributes:

- **subnet mask** - has XXX.XXX.XXX.XXX format, where every XXX is in the range 0-255. Subnet mask in binary presentation of 32 bits has at least the first 8 digits as “1” and the last digit as “0”.
- **gateway address** - has XXX.XXX.XXX.XXX format, where every token is in the range 0-255.
- **IP address** - the Ethernet protocol address, and has the same format as the gateway address.

Example:

login: **admin**
Previous admin login: Feb 11, 1997 10:00
SAdmin, SMint, PAdmin, PMaint, RGen, LOgout, ?: **sa**
SYstem, REcorder, ?: **sy**
System Attributes:
card name:
idle time-out minutes: 20
refresh period minutes: 1
report aging days: 60
short occupancy seconds: 10
application traffic report hours: 0
disconnect a lone participant: 30

subnet mask: 255.255.248.0
gateway address: 141.226.199.254
IP address: 141.226.199.50
Modify, **S**ave, **C**ancel: **m**
card name (): **first_card**
idle timeout minutes (20): **25**
refresh period minutes (1):
report aging days (60):
short occupancy seconds (10):
application traffic report hours (0): 1
disconnect a lone participant (30):
subnet mask (255.255.248.0):
gateway address (141.226.199.254):
IP address (141.226.199.50):

New System Attributes:
card name (): first_card
idle timeout minutes: 25
refresh period minutes: 1
report aging days: 60
short occupancy seconds: 10
application traffic report hours: 1
disconnect a lone participant: 30
subnet mask: 255.255.248.0
gateway address: 141.226.199.254
IP address:141.226.199.50
Modify, Save, Cancel: **Save**

System Attributes have been updated.
SYstem, REcorder, ?: /
SAdmin, SMaint, PAdmin, PMaint, RGen, LOgout, ?: **lo**

This concludes the System Attributes Editor session, returns you to the Main Menu, and logs you out.

Audio Recorder

Audio Recorder enables you to create new brandline custom greetings for each language. The brandline custom audio files serve as customized greetings for conferences.

When you select the Audio Recorder option, you see a list of brandline custom audio files, which you can modify (by entering **m**) or delete (by entering **d**). You can also insert new brandline files (by entering **i**). You cannot modify the default audio files that the factory supplies.

To create a new brandline audio file, follow these steps:

1 Log in as **admin**.

2 Enter **sa** for System Administration.

3 Enter **re** to enter the Audio Recorder.

4 Choose a language. (<cr> selects the default language.)

5 Enter **i** to record a new greeting.

6 Enter a file name, all CAPS and up to 8 characters.

7 Follow the dialing instructions given on the MICB administration screen.

8 Record the greeting and hang up.

9 Enter **s** to save the audio file.

Example:

This is an example of a recording session:

SYstem, REcorder, ?: **re**
language (american_english, (1-french, 2-brasilian_portuguese, 3-LA_Spanish, 4- UK_English)): <cr>
File Name
1 a:mlaw\user\ENGLISH\BRANDLIN.WAV: **m 1**
Dial 2099 to begin recording session.
Follow voice instructions.
Typing “exit” will end the recording session.
After the recording is completed and the phone is on-hook
Upon completion of recording, select one of the following:
Save, **M**odify, **C**ancel: **s**
SYstem, REcorder, ?:

The new message can play only after you save it. It plays when a conference participant dials either the main or the chairperson DN.

Help display

When you choose the help command (**?**), the system displays commands related to System Administration, as follows:

SYstem, REcorder, ?: **?**

Short command	Full command	Explanation
sy	SYstem	System Attribute Editor. Edit: card name, idle time out, idle refresh, conf log aging, short occupancy, traffic report frequency, IP address.
re	REcorder	Audio Recorder. Record custom messages for use in Audio Scripts.

SYstem, REcorder, ?:

System Maintenance menu

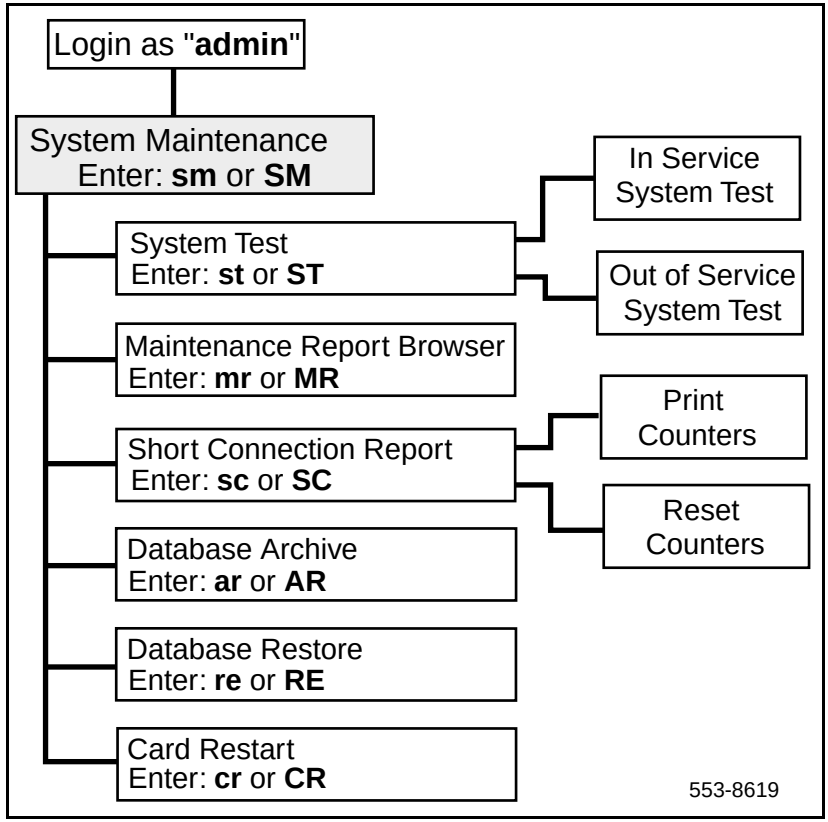
To access the System Maintenance menus from the Main Menu, enter **sm** or **SM** or the full command (**SMaint**). Figure 13 shows the System Maintenance menu structure. The System Test and Short Connection Report menus have two sub-menus.

System Tests

Use this menu to perform system component tests. You can perform in-service tests that do not disrupt service and out-of-service tests that do disrupt service for the duration of the test. Select:

- **i** - to perform in-service tests
- **o** - to perform out-of-service tests

Figure 13
System Maintenance menu



Example

In the following example, perform the service impacting (out-of-service) tests.

STest, MReport, SCon, ARchivdb, REstordb, CRestart, ?: **st**
Inserv, Outserv, ?: **o**
Perform service impacting test? (Yes, (No)): **Yes**
Performing service impacting test...Test passed.
Inserv, Outserv, ?: *****
STest, MReport, SCon, ARchivdb, REstordb, CRestart, ?:

When you select help (**?**), you see the following:

Short command	Full command	Explanation
i	Inserv	Perform in-service system test.
o	Outserv	Perform out-of-service system test.

Maintenance Report Browser

This menu enables you to display and browse maintenance reports according to date. Use these reports to analyze system problems based on error messages compiled on that specified date.

All reports have a time stamp and contain information regarding the cause of the problem. After the system displays the data, the system returns to the *year-month-day* prompt using the last selected date as default.

To exit the report, enter "**.**" (dot); to interrupt the report display, enter "***<cr>**" (star and return).

The maintenance reports have the following format:

<serial number>: <MON_REPORT_ID> <channel #> <time> <Applic_Manager_cycle> <Message Body>

Example:

Display the maintenance report for March 15, 1996.

STest, MReport, SCon, ARchivdb, REstordb, CRestart, ?: **mr**
year(1998): **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, ?:

The selected date must be in the past, not future. The old files that exceed the report aging number of days are discarded. If 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 appears indicating no messages.

Short Connection Report

The Short Connection Report menu enables you to present or reset the short connection peg-count.

Short port occupancy can indicate fault condition on the particular port or dialing of an incorrect DN. The short occupancy range is set in the System Administration menu from 1 to 30 seconds (default is 10 seconds). If 0 is selected, the short occupancy count is disabled.

You have an option to print (**p**) or reset (**r**) the counter. When printing the counters peg-count, all ports with a count are presented in the following format:

port # today's_count total_count

today's count - count of short connections that occur today
total count - cumulative count of all short connections since the MICB was last reset or the short connection counters were reset

If all counters are zero, the header is printed followed by the message:
all counters are zero

When you execute the reset, all counters are set to zero.

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, ?:

When you select help (**?**), you get the following:

Short command	Full command	Explanation
p	Print	Present peg-counts of short port occupancy.
r	Reset	Reset peg-counts of short port occupancy.

Database Archive

Database Archive enables you to backup the customer database. The system copies a set of database files from the active PCMCIA card in the lower slot (drive A:) to the backup PCMCIA card in the upper PCMCIA socket (drive B:). Names of files to be backed up are specified in the DB Description file. These files include configuration and reservation databases, as well as user made voice files.

It is especially useful to backup the customer database when you upgrade the PCMCIA card. The backup removes the need to re-enter the conference data. For backup, use the same type of PCMCIA card that sits in the lower slot (drive A:). If the PCMCIA memory is too small to accept all the archived database information, an error message appears indicating that there is not enough memory.

Example:

STest, MReport, SCon, ARchivdb, REstordb, CRestart, ?: **ar**
Backup Database? (Yes, (No)) **y**
Please wait, performing backup... completed.
STest, MReport, SCon, ARchivdb, REstordb, CRestart, ?:

Note: You cannot use a Database Archive and a Database Restore to upgrade an original MICB to MICB Release 2.0.

Database Restore

Database Restore enables you to restore the customer database to the system PCMCIA card in the lower slot (drive A:). The system copies a set of files from the backup PCMCIA card in the upper slot (drive B:) to the active PCMCIA card in the lower slot (drive A:). Names of files to be restored are specified in the DB Description file.

Example:

STest, MReport, SCon, ARchivdb, REstordb, CRestart, ?: **re**
Restore Database? (Yes, (No)) **y**
Please wait, performing restore... completed.
STest, MReport, SCon, ARchivdb, REstordb, CRestart, ?:

Note: You cannot use a Database Archive and a Database Restore to upgrade an original MICB to MICB Release 2.0.

Card Restart

This command restarts the MICB card, which initiates a software reload.

STest, MReport, SCon, ARchivdb, REstordb, CRestart, ?: **cr**
Restart MICB card? (Yes, (No)) **yes**

This action returns the MICB card to the initial screen and you must login again.

Help display

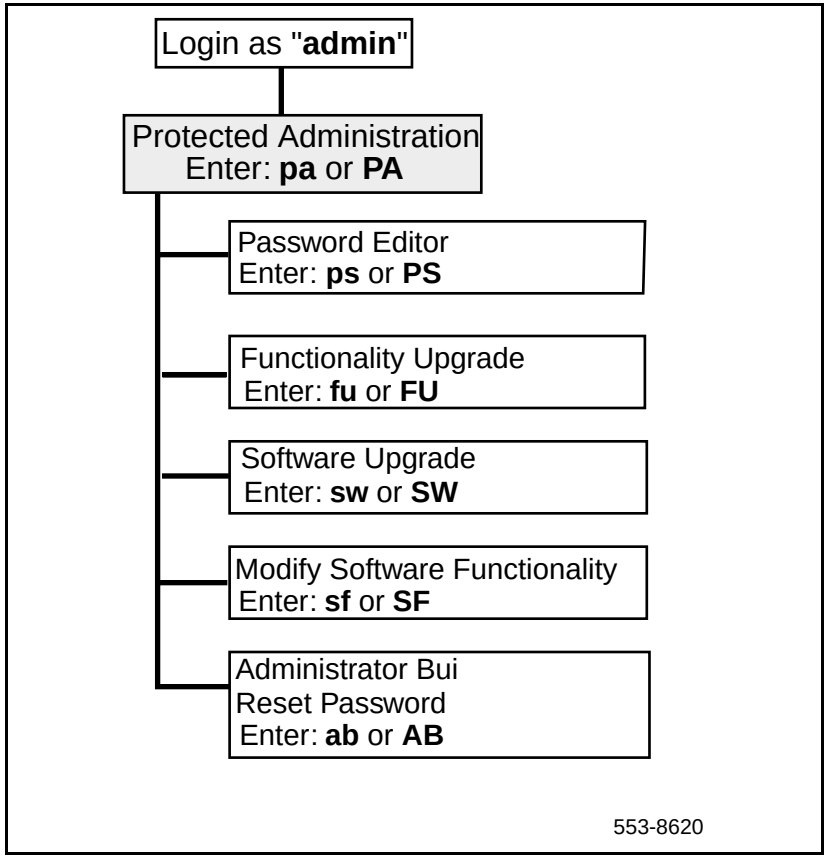
The help menu displays the commands and their explanation at the System Maintenance level.

Short command	Full command	Explanation
st	STest	System Test directory.
mr	MReport	Browse Maintenance Reports, according to date, in order to analyze system problems.
sc	SCon	Short Connection Report directory.
ar	ARchivdb	Back-up customer's database.
re	REstordb	Restore customer's database.
cr	CRestart	Reset MICB card.

Protected Administration menu

To access the Protected Administration menu from the Main Menu, enter **pa** or **PA** or the full command (**PAdmin**). Figure 14 shows the Protected Administration menu, which provides password administration and port and software upgrade keycode administration.

Figure 14
Protected Administration menu



Password Editor

To change password, log in using the default password **admin** and access the Password Editor menu from the Protected Administration menu.

You can change the default or any other password to a new password. The maximum password length is 10 characters.

Example:

This example shows how to modify the administrator password:

```
PSweditor, FUpgrade, SWupgrade, SwFunctionality, ABreset, ?: ps
Current Passwords:
admin: admin
Modify, Save, Cancel: m
admin (admin): hokeypokey
New passwords:
admin: hokeypokey
Modify, Save, Cancel: Save
Passwords have been updated.
PSweditor, FUpgrade, SWupgrade, SwFunctionality, ABreset, ?:
```

Functionality Upgrade

Functionality Upgrade enables you to change the card feature (BASIC or ADVANCED) and the number of available ports/channels on the MICB Release 2.0 card. To activate a change to the card feature and the number of ports/channels, you must enter the new keycode, which the system compares to the one in the MICB memory. Following the keycode authentication, the currently enabled MICB ports/channels are displayed.

You are allowed three attempts to enter the correct keycode. If you fail to enter the correct keycode, the changes you made do not take effect. If the keycode has been authenticated, the changes you made are stored in the memory and take effect, allowing you to use the specified number of MICB ports.

The keycode is entered using three prompts: key-code1, key-code2, and key-code3, each requiring entry of 8 digits.

Note: The ADVANCED card feature option is in place for future call accounting capability. This capability is not available at the time of the printing of this document.

Example:

This example will expand the number of available MICB ports from 8 to 16:

PSweditor, FUpgrade, SWupgrade, SwFunctionality, ABreset, ?: **fu**
max conf_ports: 8
Card Feature: BASIC
Modify, Save, Cancel: **m**
max conf_ports (8): **16**
Card Feature (BASIC, (1-ADVANCED)):
Modify, Save, Cancel: **Save**
Enter key-code1: **12121234**
Enter key-code2: **23232345**
Enter key-code3: **32222385**
Incorrect key-code
Modify, Save, Cancel: **Save**
Enter key-code1: **121ad234**
Enter key-code2: **12128934**
Enter key-code3: **32222385**
PSweditor, FUpgrade, SWupgrade, SwFunctionality, ABreset, ?:

Software Upgrade

Software Upgrade enables you to upgrade the MPU and the DSP software on an active MICB card. The new software is stored on a PCMCIA card, which you must install in slot A: on the MICB card before executing the software upgrade command. If the PCMCIA card is not in place when you try to save the upgrade, the system issues an error message as follows:

There is no PCMCIA in socket 1
MPU upgrade failed.
There is no PCMCIA in socket 1
DSP upgrade failed.

Note: You cannot perform a Software Upgrade to upgrade an original MICB to MICB Release 2.0. Refer to “Upgrade MICB to MICB Release 2.0” on page 88 for instructions on this particular procedure.

To upgrade the software:

1. Plug the PCMCIA Flash card into the top PCMCIA slot (drive B:) on the MICB. Ensure that the PCMCIA hard drive card is still in the lower PCMCIA slot (drive A:).
2. Login as the administrator (**admin**) and proceed as shown in the example below.

Example:

Upgrade the software:

```
PSweditor, FUpgrade, SWupgrade, SwFunctionality, ABreset, ?: sw
software Release: 03, issue: 07
Modify, Save, Cancel: m
Modify software? (Yes, (No)) yes
Modify, Save, Cancel: Save
Installation of MICB s/w in progress...
New s/w will be used following MICB restart.
Restart MICB? (Yes, (No)) Yes
```

3. After the upgrade is complete, it is safe to remove the PCMCIA card from the upper PCMCIA slot (drive B:).

Modify Software Functionality

Modify Software Functionality enables you to determine whether the MICB Release 2.0 card uses an embedded (EMBEDDED) or an external (EXTSRV) web-server. The external server option does not work unless you have connected the MICB card to an external server.

The following is an example of modifying the card software functionality:

```
PSweditor, FUpgrade, SWupgrade, SwFunctionality, ABreset, ?: sf
software functionality: EXTSRV
Modify, Save, Cancel: m
software functionality (EXTSRV, (1-EMBEDDED, 2-MUSIC)): 1
Modify, Save, Cancel: Save
New s/w functionality will be available following MICB restart.
Restart MICB? (Yes, (No)): Yes
```

Note: When you change the software functionality, the MICB deletes some of the customer files such as BUI users, conference DN pairs, and scheduled conferences.

Administrator BUI Reset Password

Administrator BUI Reset Password enables you to reset the passwords of all administrators that use the browser user interface (BUI). The default administrator password for the BUI is **000000**.

Note: This command is valid only for **embedded** software functionality.

To reset the BUI password to the default value for all administrators, follow this example:

```
PSweditor, FUpgrade, SWupgrade, SwFunctionality, ABreset, ?: ab
Reset BUI Administrator Password? (Yes, (No)): Yes
Password has been reset.
PSweditor, FUpgrade, SWupgrade, SwFunctionality, ABreset, ?:
```

Help display

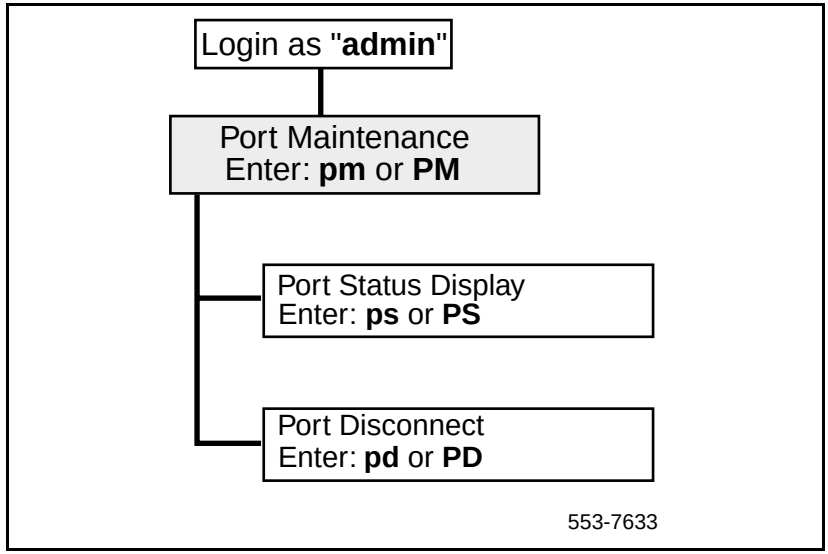
The following information appears when the help (?) command is chosen at the Protected Administration level.

Short command	Full command	Explanation
ps	PSweditor	Password Editor
fu	FUpgrade	Functionality Upgrade: allow or restrict capabilities secured by the key code.
sw	SWupgrade	Software Upgrade. Upgrade MPU and/or DSP software.
sf	SwFunctionality	Modify Software Functionality. Upgrade MPU and/or DSP software.
ab	ABreset	Administrator BUI Reset Password.

Port Maintenance menu

To access the Port Maintenance menu from the Main Menu, enter **pm** or **PM** or the full command (**PMaint**). Figure 15 shows the Port Maintenance menu and its commands. The commands display the status of the MICB ports and disconnect a specific MICB port.

Figure 15
Port Maintenance menu



Port Status Display

This commands displays the status of all MICB ports regardless of their allocation. The possible status for any port is: Idle, Dialing_out, Ringing, Talking, or Disable.

Example:

PStatus, PDisconnect, ?: **ps**

Port_ID	Port_Status	Port_ID	Port_Status
0	DISABLE	16	IDLE
1	DISABLE	17	IDLE
2	IDLE	18	DIALING_OUT
3	TALKING	19	DIALING_OUT
4	TALKING	20	RINGING
5	TALKING	21	RINGING
6	IDLE	22	IDLE
7	RINGING (Note)	23	DIALING_OUT (Note)
8	TALKING	24	TALKING
9	TALKING	25	IDLE
10	TALKING	26	TALKING
11	TALKING	27	TALKING
12	IDLE	28	IDLE
13	RINGING	29	DIALING_OUT
14	TALKING	30	IDLE
15	IDLE	31	RINGING

Note: Dialing out and ringing are very short events.

PStatus, PDisconnect, ?:

Port Disconnect

Port Disconnect enables you to disconnect a specific MICB port from a conference.

Example:

PStatus, PDisconnect, ?: **pd 13**
Disconnect port 13? (Yes, (No)) **yes**
Port 13 has been disconnected.
PStatus, PDisconnect, ?:

Help display

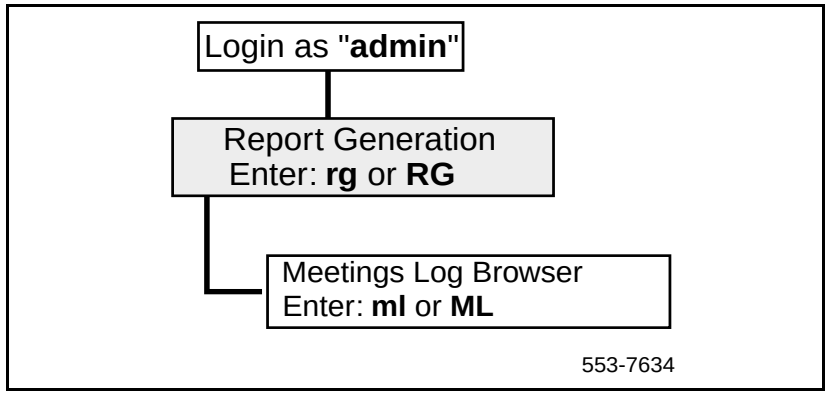
The following help information appears when the help (?) command is chosen at the Port Maintenance level.

Short command	Full command	Explanation
ps	PStatus	Display Status of all Ports.
pd	PDisconnect	Disconnect specified port.

Report Generation menu

To access the Report Generation menu from the Main Menu, enter **rg** or **RG** or the full command (**RGen**). Figure 16 shows the Report Generation menu used to present the log of conference events for a particular date.

Figure 16
Report Generation menu



Meetings Log Browser

This command displays a log of conference events for a specified date. After the MICB displays the data, the system returns to the *year-month-day* prompt using the last selected date as default. To exit the log, enter "**.**" (dot) at the prompt. If you want to exit the log before the entire log appears, enter "***<cr>**" (star and return).

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

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

Example:

MLog, ?: **ml**
year (1999): **1998**
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*//

year (1998): **.**
MLog, ?:

The date you select to display the conference log must be in the past, not future.

The system deletes old log files after the predefined report aging time is exceeded. If there are no log files for the specified date, the system indicates this.

Help display

The following information appears when you choose the help (**?**) command at the Report Generation level.

Short command	Full command	Explanation
ml	MLog	Meeting Log Browser. Present log of conference events for a particular date.

The Browser User Interface

The Meridian Integrated Conference Bridge (MICB) provides a Browser User Interface (BUI) for the definition and maintenance of MICB cards and users. You also use the BUI for the scheduling and maintenance of MICB conferences (both regular and permanent).

You must define the following minimum card attributes: card name, IP address, card type, agent ID information (if applicable), and conference DN pairs. You can also define a card ID, a TUI DN, group call lists, permanent conferences, and “Weekdays” definitions for a card.

For a user, you define such attributes as the user name, the user ID, the user type, the telephone ID, and the user’s email address.

You schedule a conference by setting the start time, the duration, the number of required ports, and other attributes. This document describes the web-based BUI for updating the MICB conference schedule.

System requirements

You access the MICB web server over an Ethernet connection through your local intranet. To access the MICB server, you need a computer with one of the following internet browsers:

- Microsoft Internet Explorer, version 4.01 or higher, with Service Pack 1
- Netscape Communicator, version 4.5 or higher

The MICB web server can exist in one of two forms:

- As an external server - The MICB web server runs on an external workstation. This option requires the following:

- A 200 MHz Pentium PC with at least 64 MB of RAM, a 1+ GB hard drive, and a CD-ROM drive
- Windows NT 4.0 Server (or later)
- Microsoft Internet Information Server 3.0 (or later)
- Microsoft NT Service Pack 3.0 (or later)
- MICB Web Server software (on a CD-ROM)
- As an embedded server - 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 MICB card's IP address.

The external server provides one point of administration for several MICB cards. All users navigate their browser to the server's IP address. However, each regular user (not the administrator) is associated with a specific card, and this card is contacted immediately when the user logs on.

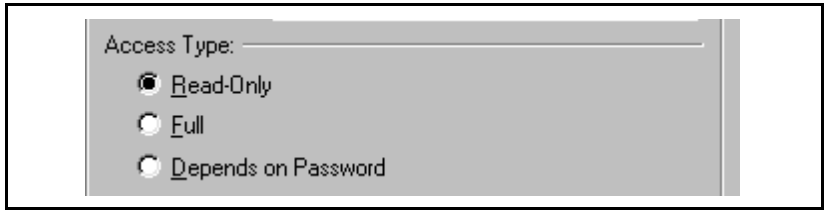
The embedded server option supports up to a total of 100 registered users and ten simultaneous users. The external server option supports up to 1000 registered users and 50 simultaneous users.

Web server conventions

Three action buttons appear at the bottom of various windows within this browser user interface (BUI):

- **Apply**—saves the current settings in the window
- **OK**—saves the current settings in the window and returns the user to the previous window
- **Cancel**—returns the user to the previous window without saving the current settings (i.e., **Cancel** discards any modifications you made to the settings.)

Radio buttons indicate a choice of only *one* out of many options. For example:



Square ‘check-boxes’ indicate independent yes/no options, where the user can select *any number* of the options. For example:

A ‘combo box’ provides a list from which the user can choose a single option. To open a combo box, click on the down arrow at the right of the currently selected option. The combo box, when open, looks similar to this:

The Login window

The first window you see when you point your web browser to the MICB BUI is the login window. To point your browser to the MICB BUI, enter **<IP address>\micb.htm** in the URL field and press **Return**. **<IP address>** is the IP address of the MICB card or the external server. See Figure 17.

Figure 17
Web server Login window

At the LOGIN prompt, enter your login ID. The administrator determines each user's login ID. At the PASSWORD prompt, enter the password. The password is six digits and is the same one you use to access the Telephone User Interface (TUI). The first time you log in as a user or super-user, you use a default password that the administrator determines. After you log in, you can change the password by clicking on the key icon in the Conference Manager window.

When you log in to the MICB BUI, the login ID connects you to the server as a particular user type. The administrator determines what user type each user is. The three user types and their functionality are:

- **User**—A user can reserve conferences under his or her account as well as modify and delete his or her own conferences. A user can also view all scheduled conferences.

- **Super-user**—In addition to the normal user functionality, a super-user can reserve conferences under other users' accounts. A super-user can modify and delete the conferences of other users.
- **Administrator**—The administrator manages MICB system parameters, including user IDs, group-call tables, permanent bridges, and other MICB features.

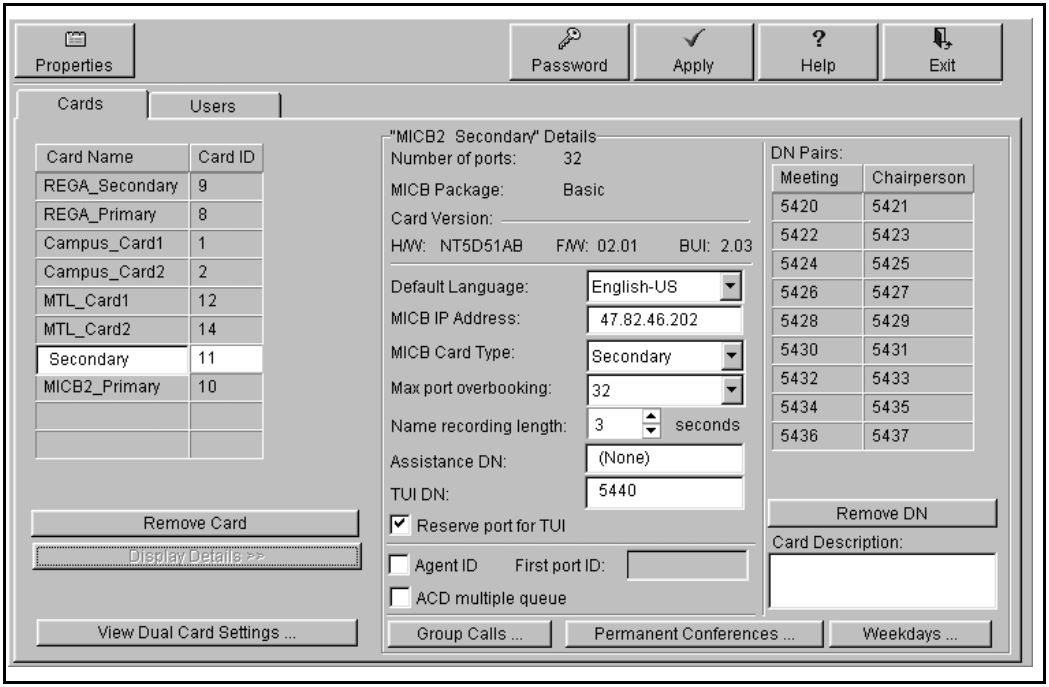
Users and super-users use the same BUI, while the administrator BUI is different. The user/super-user BUI handles conferences. The administrator BUI is only for system management and does not schedule conferences. The administrator can create permanent bridges, while the user and super-user cannot. In the external server configuration, each user/super-user is associated with one MICB card only and has no access to other cards. The administrator manages all MICB cards that the web server controls.

Note: The administrator must first define all card attributes and user attributes before user and super-users can access the BUI to schedule conferences.

MICB administration utility

To enter the MICB administrator BUI, enter the administrator login ID and password at the login window (see "The Login window" on page 124). Figure 18 shows the MICB Administration Utility window, which is the main administration window.

Figure 18
MICB Administration Utility, Cards page



Across the top of the main administration window are five buttons:

- **Properties** button opens the Properties window (see "Properties button" on page 137)
- **Password** button opens the Change Password dialog box, which allows the administrator to change the administrator password (see "The Change Password dialog box" on page 153)
- **Apply** button saves the current data

- **Help** button opens the online help
- **Exit** button terminates the BUI session and logs you out

The main administration window contains two pages: the Cards administration page and the Users administration page. Click on the tab for the page you want to view.

Cards administration

Manage MICB card parameters from the Cards page of the MICB Administration Utility (see Figure 18). In the external server configuration, one BUI server can manage up to ten MICB cards. In the embedded server configuration, the BUI shows only one card.

The table on the left lists the names of the all of the cards that the BUI server manages. Each name is up to 20 characters in length. The right-hand column of the table lists the card ID of each card. The card ID is a decimal number up to four digits long and represents the card in billing reports and CDR charge-account records.

You can add a card by typing into an empty row. You can select a card by clicking on it; the selected card is highlighted.

The **Remove Card** button deletes the currently selected card.

The **Display Details** button displays the details of the selected card in the right-hand portion of the Cards page. To display the details of a card at the right of the frame, you must select the card from the ‘Card Name’ list, then click on **Display Details**.

The **Dual Card settings...** button opens an auxiliary window for the configuration of a dual-card set. See “Dual-card settings” on page 132.

Card details

The parameters of the selected card appear on the right-hand side of the Cards page. The left column of the details section lists the number of ports, the MICB package, and the version of the selected card, including the hardware vintage, the firmware version, and the BUI version. You can configure the following attributes of the selected card:

Default Language: The default language of the conferences.
Default: English - US

MICB IP address: The card's IP address. With the embedded server option, the card's IP address appears automatically and you cannot change it. With the external server option, you must first enter the card's IP address and click **Apply** to establish a connection to the card; you can then define the remaining card attributes. In both options, the CLI, not the BUI, defines the card's IP address.

MICB Card type: The card type, which is either 'Regular' (for a stand-alone card), 'Primary' (for a dual-card set), or 'Secondary' (for a dual-card set).
Default: Regular

Max port overbooking: The maximum number of ports available for reserving conferences, including overbooking. The range is 100-125% of the number of ports the card is equipped with (e.g., 32-40 for a 32 port card).
Default: the actual number of ports on the card

Name recording length: The amount of time given to conferees to record their names when entering conferences, from 2-10 seconds.
Default: 2 seconds

Assistance DN: The DN to which the MICB card forwards help requests, up to seven digits in length.

TUI DN: The DN to dial for Telephone User Interface (TUI) operations, up to seven digits in length.

Reserve port for TUI: Check this box to reserve one of the ports solely for TUI operations. The reserved port is not available for conferences.

The next framed area is for ACD setup, which must match the Meridian 1 system configuration. Configure the following attributes:

Agent ID: Indicates whether ACD is configured with the Agent ID option.

First port ID: If the Agent ID box is checked, then enter here the first agent ID for MICB ports, up to four digits in length. The other ports use the *succeeding* agent IDs. For example, if the first agent ID is 3000 and the MICB card has 24 ports, then the card uses IDs 3000-3023.

Note: Ensure that all agent IDs that you intend to use (3000-3023 in this example) are available before you assign them.

ACD multiple queue: Indicates whether ACD is configured with the multiple-queue option.

The DN pairs table lists the paired conferee and chairperson DNs. You can define up to ten DN pairs per card.

Note: The dual-card DN pair counts toward the limit of DN pairs allowed on *both* the primary *and* the secondary cards. Therefore, you can define only nine DN pairs on each the primary and secondary cards in a dual-card configuration. You define the main and chairperson DNs for dual-card conferences in the Dual Card Settings dialog box.

You can select a DN by clicking on it; the selected DN is highlighted. You can edit a DN by typing directly in the table. You can add a DN pair by typing into an empty row. A DN can be up to seven digits in length.

The **Remove DN** button deletes the currently selected DN pair. You must click **Apply** for the change to take effect.

The Card description field allows you to enter a description of the card, up to 30 characters in length.

The **Group Calls...** button opens an auxiliary window for the configuration of group calls for this card. See “Group-call configuration” on page 133.

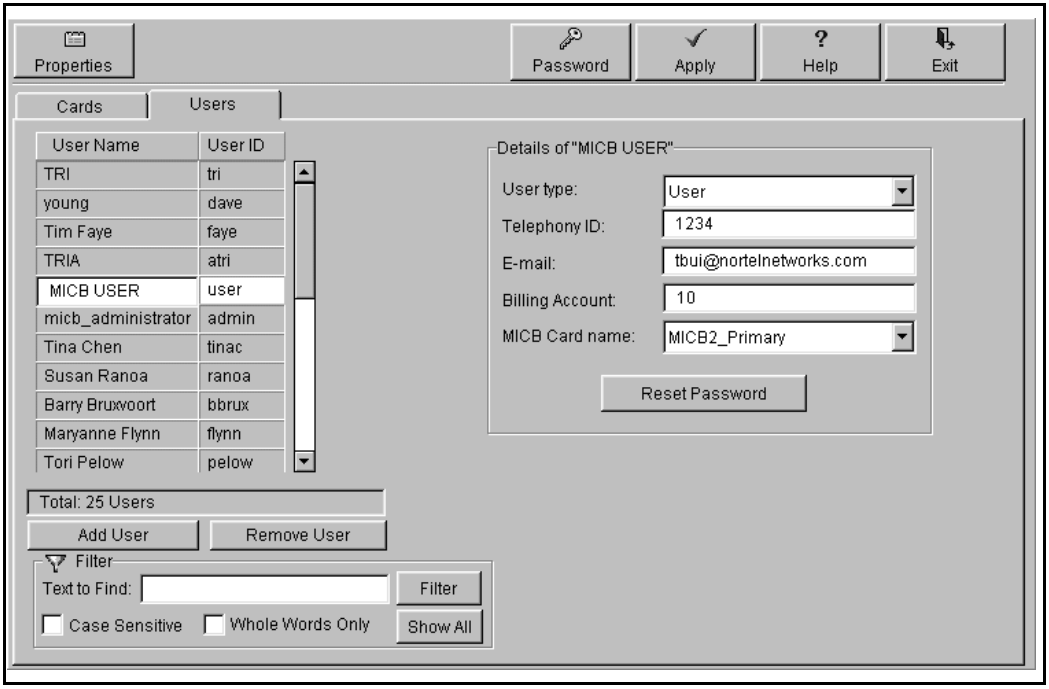
The **Permanent Conferences...** button opens an auxiliary window for the configuration of permanent conferences for this card. See “Permanent-conference configuration” on page 135.

The **Weekdays...** button opens a dialog box for defining the range of working days. Default: from Monday to Friday.

Users administration

Manage MICB user parameters from the Users page of the MICB Administration Utility (see Figure 19). In the external server configuration, the external web server stores all user data. In the embedded server configuration, each MICB card stores its own user data.

Figure 19
MICB Administration Utility, Users page



The table on the left side of the Users page lists all of the users, listing for each user the user name (up to 20 characters) and the login ID (up to 10 characters). You can sort the list by either user name *or* user ID by clicking on the title of the appropriate column. For example, to sort the list alphabetically by user ID, click on the **User ID** column head. You can select a particular user by clicking on it; the selected user is highlighted, and the user details appear on the right.

Note: The "User ID" functions as the login ID for the user.

The **Add User** button below the table opens a new line below the currently selected user. You can enter a new user in this new line.

The **Remove User** button deletes the currently selected user.

You can define up to 1000 users in the external server configuration or up to 100 users in the embedded server configuration. A user can be assigned to only one MICB card.

The 'Filter' area at the bottom of the Users page allows you to display a select subset of users. When you click the **Filter** button, only users matching the 'Text to Find:' field appear in the users list. The **Show All** button cancels the filter and re-displays the entire list of users.

User details

The parameters of the selected user appear on the right-hand side of the Users page. You can configure the following attributes for each user:

User type: The type of user, either user, super-user, or administrator.

Note: Initially, there is one user of type 'administrator' with password '000000' and billing account number of 1. This is for the first login after installation.

Telephony ID: The user ID for user login to the TUI, up to six digits in length.

e-mail: The e-mail address of the user, for receiving reservation confirmation by e-mail, up to 36 characters in length.

Billing account: The account number of the user, up to nine digits, for billing purposes. This number appears in the billing reports and in Meridian 1 CDR records for conferences owned by the user.

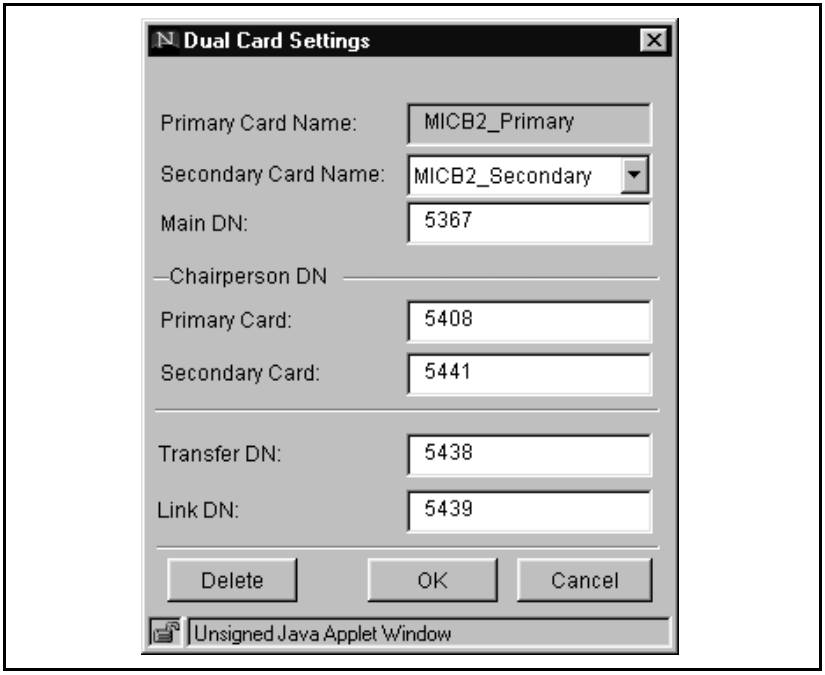
MICB Card name: The name of the card the user is assigned to. Only the external server configuration supports this field.

Click the **Reset Password** button to reset the selected user's password to the initial password. See "Properties button" on page 137 for information on the initial password.

Dual-card settings

Configure the two cards that are to serve as a pair for dual-card conferences as primary and secondary cards. To enter the dual-card setup, click on the **Dual Card settings...** button in the main administration window of the *primary* card. The Dual Card Settings dialog box then appears, as Figure 20 shows.

Figure 20
Dual Card Settings dialog box



Note: Before you can configure the dual-card settings, you must first configure the card attributes of both the primary and the secondary card. You set the dual-card settings from the primary card.

The Primary Card Name is the name of the card currently selected in the main administration window; you cannot change the Primary Card Name in this window. However, you can configure the following attributes:

Secondary Card Name: Select the Secondary Card Name from the list of *already* configured cards.

Main DN: The DN that conferees dial to access a dual-card conference. Enter the DN that you defined as an NACD DN according to Table 11, "Configuring the main DN for dual-card conferences using Overlay 23," on page 68.

Primary chairperson DN: The DN that the primary chairperson dials to perform chairperson functions on the primary card.

Secondary chairperson DN: The DN that the secondary chairperson dials to perform chairperson functions on the secondary card.

Transfer DN: The DN that the primary card uses to transfer calls to the secondary card.

Link DN: The DN that the two cards use to create a voice path between them.

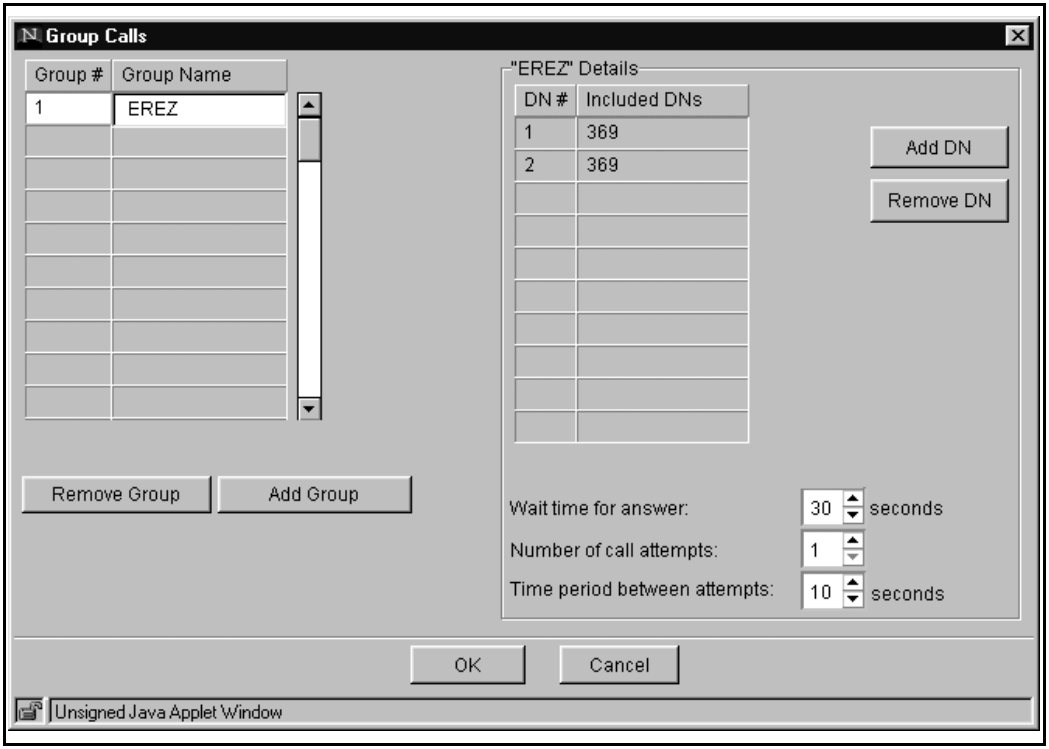
All parameters from the Dual Card Settings dialog box, except for the chairperson DNs, are sent to both cards. The chairperson DNs are sent to their respective cards.

Group-call configuration

For each MICB card, you can define groups for the group-call feature. To enter the group-call setup, click on the **Group Calls...** button on the cards page of the main administration window. The Group Calls dialog box then appears, as Figure 21 shows.

The table on the left side of the Group Calls dialog box lists all of the groups defined for the selected card. You can define up to 64 group-call lists per card.The group number is the number that the chairperson dials when executing the group-call command. The group name is up to 20 characters of free text that describes the group. The BUI sorts the group-call lists by group number.

Figure 21
Group Calls administration page



You can select a group by clicking on a particular row of the table. The group is then highlighted and the group's details appear at the right.

The **Add Group** button below the table opens a new line below the currently selected group. You can enter a new group in this new line.

The **Remove Group** button deletes the currently selected group.

Group details

The group details on the right side of the Group Calls dialog box lists the DNs assigned to the selected group. The order of the DNs indicates the priority of calling; for example, when a conference has seven ports available, the MICB dials only the first seven DNs on the list. A group call list can contain up to 61 DNs.

The **Add DN** button to the right of the table opens a new line below the currently selected DN. You can enter a new DN, up to 20 digits, in this new line. The MICB sets the DN number in the left-hand column automatically.

The **Remove DN** button deletes the currently selected DN.

You can also configure the following attributes for each group:

Wait time for answer: The number of seconds to wait for a called party to answer when dialling the selected group. The range is 15-90 seconds.
Default: 30 seconds

Number of call attempts: The number of times to dial each number in the group call list. The MICB card can re-dial a number in the case of failure. A value of 1 means only one attempt with no retries. The range is 1-3 attempts.
Default: 1 attempt

Time period between attempts: In case of dialing failure, the number of seconds the MICB card waits before re-dialing the number. The range is 5-30 seconds.
Default: 10 seconds

Permanent-conference configuration

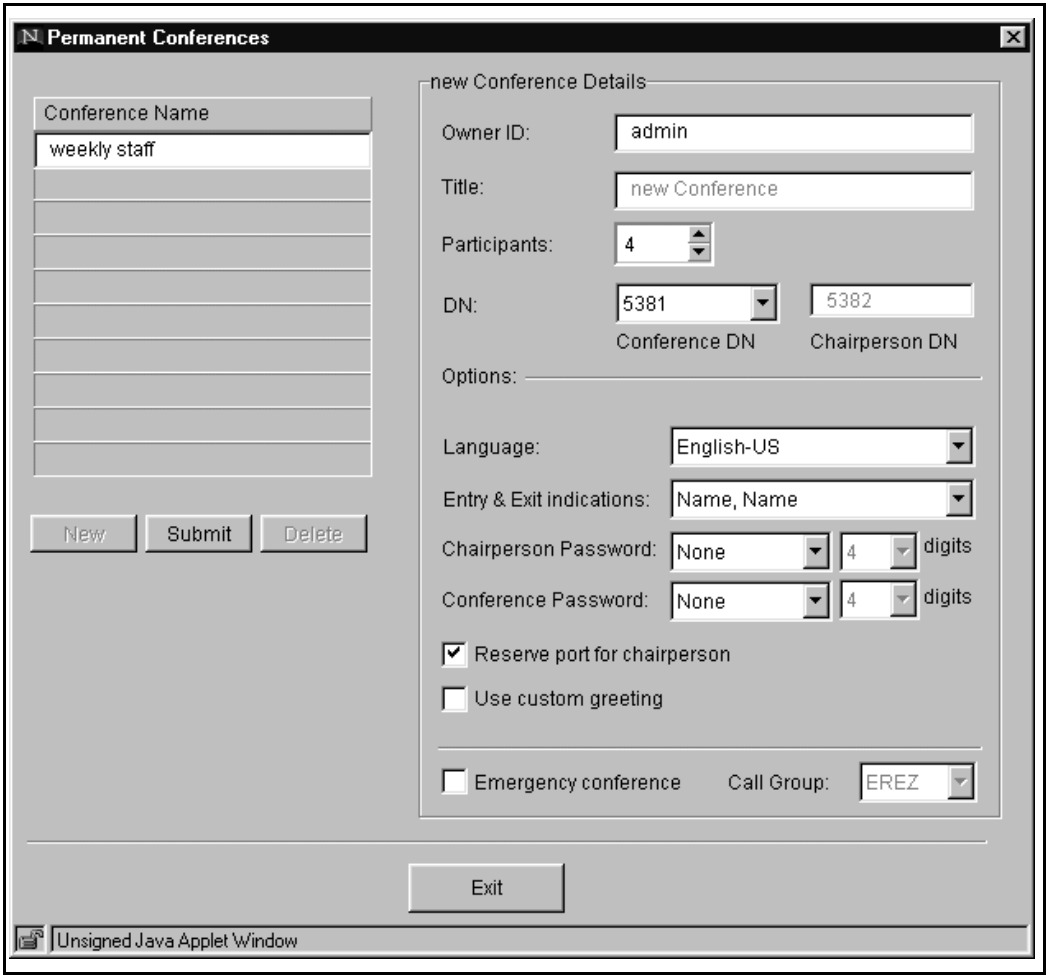
For each MICB card, you can define permanent conferences, or bridges. To enter the permanent-conference setup, click on the **Permanent Conferences...** button on the cards page of the main administration window. The Permanent Conferences dialog box then appears, as Figure 22 shows.

Note: MICB Release 2.0 does not support dual-card permanent conferences. However, you can define permanent conferences on either of the cards in a dual-card configuration, as long as the number of participants does not exceed the number available on that particular card (maximum of 32).

The table on the left side of the Permanent Conferences dialog box lists all of the permanent conferences defined for the selected card. The conference name is up to 20 characters of free text that describes the conference.

You can select a conference by clicking on a particular row of the table. The conference is then highlighted and the conference's details appear at the right.

Figure 22
Permanent Conferences dialog box



The **New** button below the table opens a new line below the currently selected permanent conference. You can enter a new conference in this new line.

The **Submit** button sets the currently defined permanent conference.

The **Delete** button deletes the currently selected permanent conference.

Conference details

For a selected conference, you can configure the following details shown on the right side of the Permanent Conference dialog box:

Owner ID:	The user ID of the owner of the permanent conference.
Title:	The title of the permanent conference.
Participants:	The number of ports to reserve for the permanent conference, up to the number of ports configured on the MICB card.
DN:	The DN that conferees must dial to enter the permanent conference.

Configure the *Language*, *Entry & Exit Indications*, *Chairperson Password*, *Conference Password*, *Reserve port for chairperson*, and *Use custom greeting* attributes the same way as those explained for the MICB Conference Reserver window (see "MICB user BUI description" on page 139).

Check the *Emergency conference* box at the bottom of the dialog box to activate the Emergency Conference feature. An emergency conference has an associated group-call list, which you select in the adjacent combo-box. When somebody dials the DN for an emergency conference, the MICB immediately dials every DN on the selected group calls list.

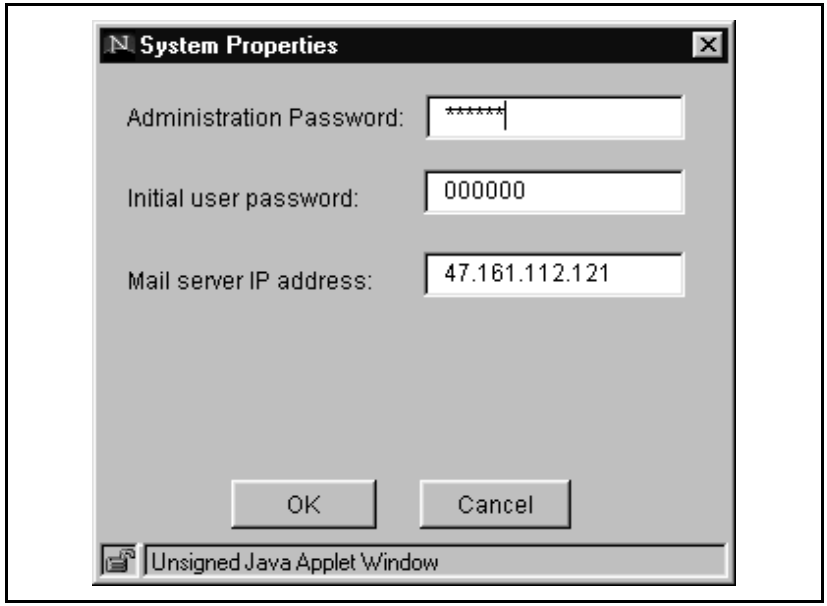
After you add or modify a permanent conference, press the **Submit** button to save the conference attributes before proceeding to the next conference. After you press the **Submit** button, an acknowledgment window appears, which specifies whether the Submit operation was successful.

If you abandon pending modifications (i.e., not pressing the **Submit** button) by selecting another permanent conference or by pressing the **New** or **Exit** buttons, a dialog box appears asking you whether to discard the pending modifications or set them.

Properties button

Click on the **Properties** button at the top of the main administration window to open the System Properties dialog box shown in Figure 23. This dialog box manages general settings that are not card-specific.

Figure 23
System Properties dialog box



You can configure the following characteristics in the System Properties dialog box:

Administrator password: The login password of the administrator that is currently logged in. When you first install the MICB card, this password is 000000.

Initial user password: The initial user password when the administrator adds a new user or resets a user's password. This password is initially 000000.

Mail server IP address: The server for sending emails of conference reservations. To enable the email notification feature, you must enter the appropriate IP address in this field. Do this before you allow users to login and schedule conferences.

Note: For email notification to work, the mail server IP address *must* be 'unrestricted' and able to send email to everyone on the network.

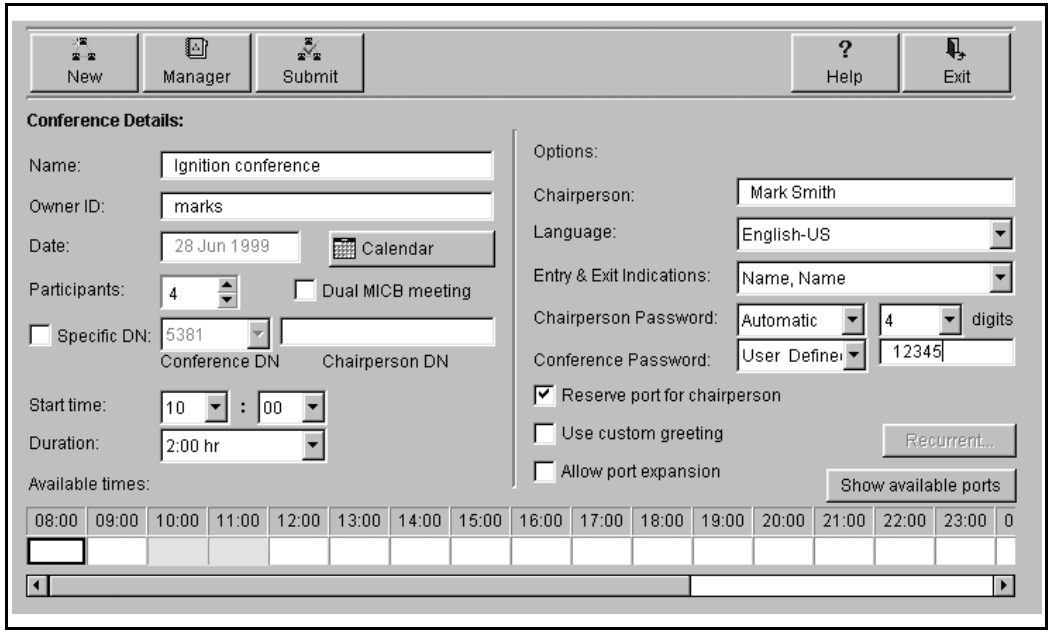
MICB user BUI description

This section describes each BUI user window.

MICB Conference Reserver

The MICB Conference Reserver window is the main window of the MICB user/super-user BUI. See Figure 24. This window is where you reserve a new conference, which is the most common task. Thiwindow appears immediately after a user or super-user logs in. The window is visible during the entire user/super-user session.

Figure 24
MICB Conference Reserver window



Across the top of the Conference Reserver window are five buttons:

- **New** button clears all entries in the Conference Reserver window so that you can define a new conference.
- **Manager** button opens the Conference Manager window. (See “Conference Manager” on page 148.)

- **Submit** button submits the conference details to the MICB to reserve a conference. You receive a confirmation message.
- **Help** button opens online help.
- **Exit** button logs you out of the BUI.

The left half of the window contains fields where you enter basic information to set up the conference. The right half of the Reserver window contains fields where you set options and features. Click on the **Submit** button to save the conference.

Descriptions of each of the conference attributes that appear on the Conference Reserver window follow:

Name: A maximum of 20 characters that describes the conference. The user can leave this field blank.

Owner ID: The login User ID of the person who created the conference. A conference is billed to the owner's account. Only the owner can modify or delete a conference. For regular users, this field is read-only, and the adjacent button is absent. Super-users can edit data in this field, so the conference is reserved on behalf of the specified Owner ID. The specified user becomes the owner of the conference when the conference is set.

Date: The date of the conference. The adjacent 'Calendar' button opens an auxiliary window that displays one month at a time. See "The auxiliary Calendar window" on page 152. Scroll to a particular month and click on the appropriate day to select the date of the conference.
Default: current date

Participants: The number of participants, including the chairperson, in the conference. The number of conference participants depends on the provisioning of the MICB card.
Default: 4

Dual MICB meeting Check this box to schedule a dual-card conference (up to 62 participants). This checkbox is disabled if the MICB card is not a primary card. When you check this box, the MICB enters the pre-defined dual-card conference DNs in the conference DN and chairperson DN fields.

Specific DN: Check this box to select the conference DN from the combo box. The combo box shows all available conference DNs. Each conference DN has a chairperson DN associated with it.
Default: The box is not checked and MICB selects the conference DN automatically.

Start time: Select the conference start time in 15-minute increments.
Default: Current time.

Duration: Select the conference duration in increments of 15 minutes. Minimum conference duration is 15 minutes. Maximum conference duration is 12 hours.
Default: 1 hour

Chairperson: The conference chairperson of the conference. By default, it is the same as the owner's name, but the user can modify it. The chairperson name has a maximum length of 20 characters.

Language: Select the conference language. The administrator determines the default language.

Entry & Exit Indications: Indicates how the system announces participants as they enter and leave a conference. There are four options:
Name, Name—Entry by name, exit by name
Name, Tone—Entry by name, exit by tone
Tone, Tone—Entry by tone, exit by tone
Silence—Silent entry and exit (no indication)
Name announcements are preceded by a tone.
Default: **Name, Name**

Chairperson password: The password, from four to eight digits in length, that the chairperson dials to enter the conference. There are three options for defining this password:
Automatic—The MICB card generates the password automatically after the conference is set. The user determines how long the password is by the combo box to the right.
User defined—The user specifies the desired password in the box to the right.
None—No password is defined and none is needed to enter the conference.
Default: **None**

Conference password: The password that the conferees dial to enter the conference. This password has the same parameters as the chairperson password.

Reserve port for chairperson Check this box to reserve one of the conference ports for the chairperson. If this box is not checked, the chairperson can be blocked from the conference if sufficient conferees dial in to the conference before the chairperson does.
Default: Box is checked

Use custom greeting Check this box to use the 'brandline' greeting for the conference. If this box is not checked, the system uses the built-in factory default greeting.
Default: Box is not checked

Allow port expansion Check this box to allow the conference to expand beyond the number of ports reserved for it. An expanded conference uses ports that are neither in use nor reserved by any other conference.
Default: Box is not checked

The **Recurrent...** button at the bottom right of the window opens an auxiliary window that allows you to schedule a conference that recurs periodically. See "Recurrent conferences" on page 143. Dual MICB meetings cannot be recurrent. This button is disabled when the Dual MICB meeting box is checked. You must check the Specific DN box to enable this button.

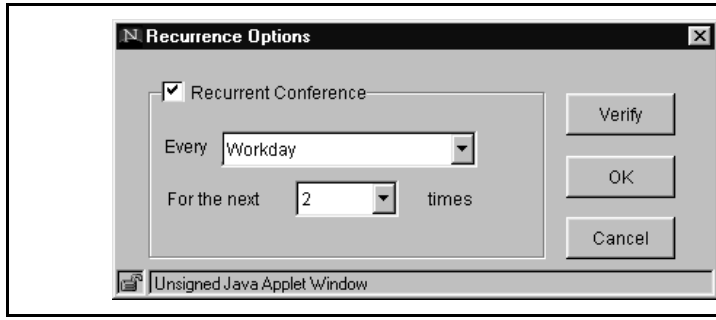
The scale at the bottom of the window shows the available periods for the selected day. When the **Date** and **Participants** parameters are set, the time periods that can accommodate these parameters appear in white. (The system takes the Dual MICB meeting option into account.) Unavailable times have a gray background. If the user indicates a DN, the scale removes times when the DN is not available. When the user selects a conference start time and length, the meeting appears on the scale in yellow.

The **Show available ports** button - Press once to indicate on the scale the number of ports available in each hour. Press the button again to remove the port-availability information.

Recurrent conferences

Click on the **Recurrent...** button in the MICB Conference Reserver window to open an auxiliary window that allows you to schedule a conference that recurs periodically. See Figure 25.

Figure 25
Recurrent Conference dialog box



You can configure the following attributes in the Recurrent Conference dialog box:

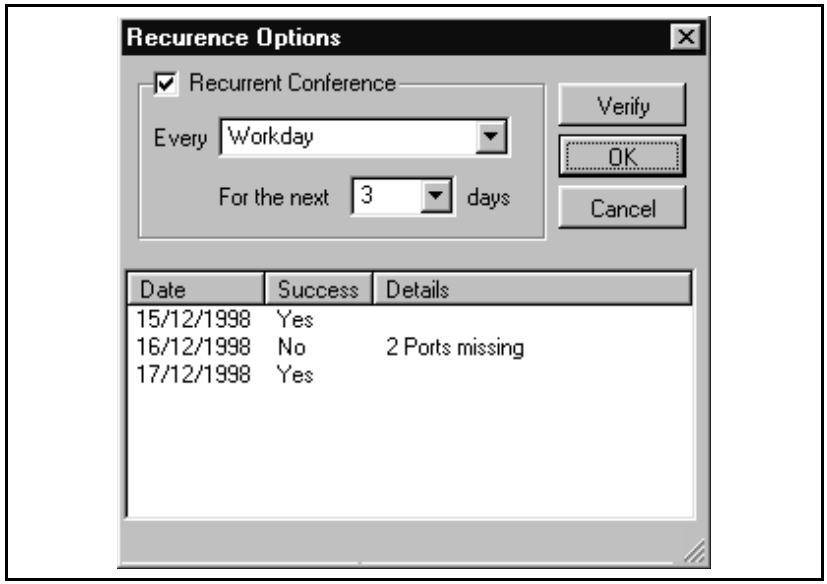
Recurrent Conference box Activates or deactivates the 'recurrent' feature. The box is checked the first time you open this dialog box.

'Every' combo box Determines the frequency of the recurrent conference. The options are: Workday, Day, Week, Two weeks, and Month. The administrator defines 'Workday' (e.g., Monday-Friday). 'Day' refers to every day of the week, including non-work days.

'For the next' combo box Determines how many times, from 2 to 15 times, the conference occurs. The number of occurrences can extend up to one year.
Default: 2 times

Click the **Verify** button to check the requested dates in the MICB card. The result appears as a list as shown in Figure 26.

Figure 26
Recurrent meeting 'Verify' results



Note: The system does not reserve the recurrent conference at this point; it only verifies whether all requested occurrences are available.

The user can accept the results by pressing **OK**, cancel the recurrent conference operation by pressing **Cancel**, or modify the parameters and try again. When the user modifies the parameters, the results list disappears and the dialog box returns to its initial form as in Figure 25.

When the user presses **OK**, the system stores the parameters and closes the dialog box. However, the system does not actually reserve the recurrent conference until the user presses the **Submit** button in the MICB Conference Reserver window. See "Setting a conference" on page 145. If there are simultaneous users on the MICB BUI, it is possible that the reservation result is different from the 'Verify' result. This can happen because the system reserves ports in the order that the users request them by pressing the **Submit** button.

Setting a conference

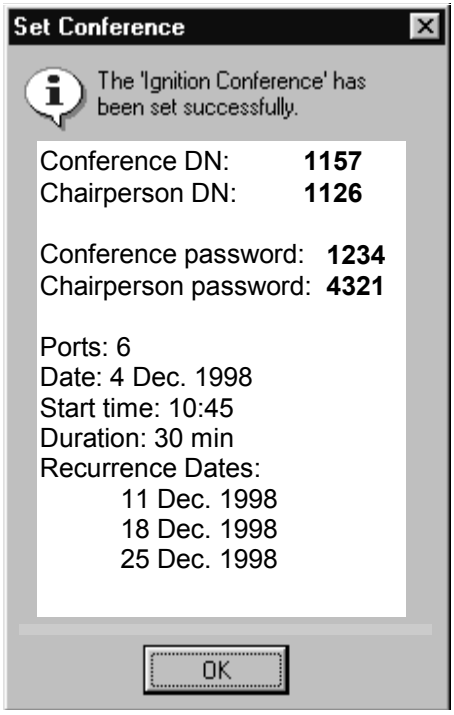
Once you have entered all of the parameters for a particular conference, press the **Submit** button in the MICB Conference Reserver window to reserve the conference on the MICB card. If the reservation is successful, an acknowledgment box appears (see Figure 27).

The window is the same for a single or recurrent conference. The window shows the main conference parameters: DNs, passwords, number of ports, date, time, and duration. If you set a recurrent conference, you can also view all successful recurrence dates in this window. You can view all other parameters of the conference in the MICB Conference Reserver window, which is still in view.

Note: It is especially important to note the contents of the Conference reservation acknowledgment window if you had the MICB card set the DNs and/or passwords automatically.

You can copy the text in the white portion of the Conference reservation acknowledgment window and paste it elsewhere. The operation for copying and pasting the text is the same as for most word processors.

Figure 27
Conference reservation acknowledgment window



Reservation failure

If the MICB card cannot reserve a requested single conference, the Single conference ‘Set’ failure message appears (see Figure 28).

The failure message gives the reason for the reservation failure. If the reason for failure is insufficient ports, you have the option to set the conference anyway with a smaller number of ports by pressing **Set Anyway**. Otherwise, you can press **Cancel** and reconfigure the conference. If the reason for failure is that a DN is not available, you must reconfigure the conference.

For a recurrent conference, pressing **Submit** reserves the conference for all of the requested dates that are available. If the list of dates actually set differs from the list shown in the ‘Verify’ result, the Recurrent conference ‘Set’ failure message window appears (see Figure 29).

Figure 28
Single conference 'Set' failure message

Figure 29
Recurrent conference 'Set' failure message

Email confirmation

When conference setup is successful, MICB automatically sends the conference owner an email with the details. Table 14 gives an example of the email format.

Table 14
Email confirmation

Your tele-conference meeting has been booked by MICB as follows:	
Owner ID:	Barryb
Conference DN:	1157
Chairperson DN:	1126
Conference password:	1234
Chairperson password:	4321
Date:	4 Dec. 1998
Start time:	10:45
Duration:	30 min
Ports:	6
Recurrence dates:	11 Dec. 1998
	18 Dec. 1998
	25 Dec. 1998
Options:	
Chairperson name:	Barry Bigglesworth
Language:	American_English
Entry & exit indications:	Name, Name
Reserve port for chairperson:	yes
Use custom greeting:	no
Allow port expansion:	no

Conference Manager

Click on the Manager button at the top of the Conference Reserver window (shown in Figure 30). The Conference Manager window displays all the meetings scheduled for a selected day on that one MICB card. The Conference Manager window has an auxiliary Calendar window to select dates. The Conference Manager and Calendar windows appear side by side.

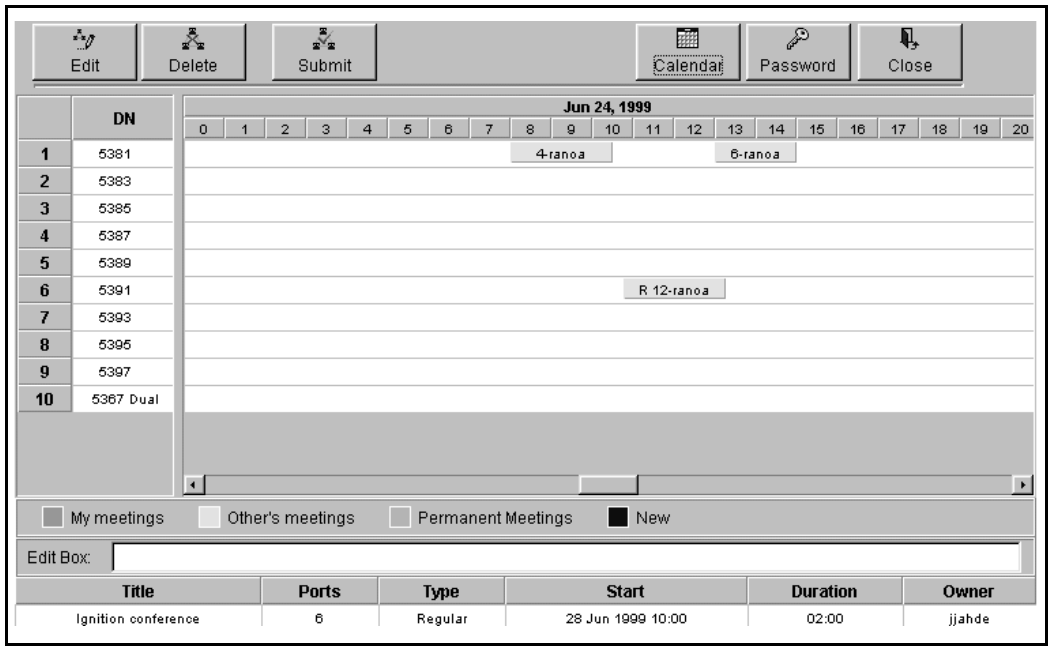
User privileges

A user can schedule meetings only for himself or herself.

Super-user privileges

A super-user can schedule meetings for all users.

Figure 30
Conference Manager window



Conference manager description

Across the top of the Conference Manager window are six buttons:

- **Edit** button brings you to the Conference Reserver window to edit the details of a conference that you highlighted in the Conference Manager window.
- **Delete** button deletes a conference that you selected, if you have permission.
- **Submit** button submits the details of a conference that you are first defining or modifying for the MICB to save.

- **Calendar** button opens the auxiliary Calendar window so that you can select which day's conferences you want to view. (See "The auxiliary Calendar window" on page 152.)
- **Password** button opens the Change Password dialog box so that you can change your user password.
- **Close** button closes the Conference Manager window and returns you to the Conference Reserver window. You will lose all changes to conferences unless you first clicked on the **Submit** button.

The main part of the Conference Manager window shows the conferences scheduled for the selected day. The horizontal scale indicates the time. The vertical scale indicates the conference DNs. A colored, horizontal bar represents each conference. Immediately below the body of the window is a key to the colored bars:

- **Orange** indicates conferences that the current user owns.
- **Yellow** indicates conferences that others own.
- **Lavender** indicates a permanent bridge.
- **Dark blue** indicates a conference that the user is defining or modifying but has not yet submitted.

The letter '**R**' on a conference bar indicates a recurrent conference.

The vertical, dotted line in the body of the window indicates the separation between days. The window shows two days—the day selected and the day following.

To edit or delete a conference, click on a conference and press the **Edit** or **Delete** buttons at the top of the Conference Manager.

The bottom row of the Conference Manager window displays the main details of the selected conference. When a user clicks on a field in this row, its contents appear in the 'Edit Box' above. The user can edit the selected field's contents. After you edit the contents of the selected field, press **Return** and click on the **Submit** button to set the changes.

Note: Users can only edit or delete their own conferences.

User operation

Users can define a new conference by dragging the mouse from left to right in the row of the desired DN. The new conference you are defining appears in the lower table; you can enter the conference title and the number of ports, or conferees, there. You can adjust the duration of the conference by adjusting the size of the conference bar or by updating the 'Duration' column in the lower table.

If you have the dual-MICB card option, you can define a dual-card conference by dragging the mouse from left to right in the bottom DN row titled 'Dual'. You can only create or modify a dual-card conference in the primary MICB card. A dual-card conference appears in the Conference Manager of the secondary card as well, but you cannot change any of its attributes there. A dual-card conference appears in the lower table, just like other conferences.

You can view details of a selected conference in the MICB Conference Reserver window, which is the main window. See "MICB user BUI description" on page 139. To return to the main window, click on the **Edit** button at the top of the Conference Manager window. The main window contains the parameters of the conference that you selected in the Conference Manager window. In the main window, a user can modify the parameters of the selected conference if he or she owns the conference. A super-user can modify the parameters of any of the conferences.

> ***Note:*** If a user is viewing the parameters of any conference, the passwords do not appear.

Click on the **Delete** button to delete the selected conference. This opens a dialog box for confirmation. If the selected conference is a recurrent conference, the dialog box gives you two delete options:

- The selected instance only
- All instances of the recurrent conference

Click on the **Submit** button to reserve, or save the modifications of, the selected conference. If the reservation is successful, an acknowledgment box appears (see Figure 27 on page 146).

Click on the **Calendar** button to display or hide the auxiliary Calendar window.

Click on the **Password** button to open a dialog box for modifying the user's (or super-user's) password. The password can be up to six characters in length.

Click on the **Close** button to return to the MICB Conference Reserver window without the attributes of a selected conference.

The auxiliary Calendar window

Figure 31 shows the Calendar window, which appears when you click on the **Calendar** button in either the Conference Reserver window or the Conference Manager window. The window opens to the current day.

Figure 31
Calendar window

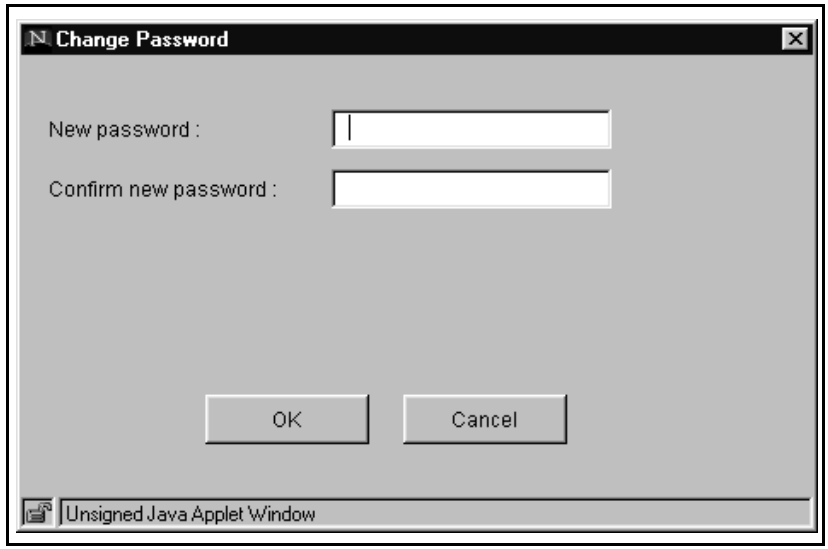
The year and month appear at the top of the window. The down arrows to the right of the year and month open combo boxes that allow you to select the desired year and month. The MICB card allows reservations up to one year in advance. Once you have selected the desired year and month, select the desired day by clicking on that day. A black box frames the selected day.

Click the **Today** button to return the calendar to the current day. Click the **Apply** button to set the conference date in the Conference Reserver window or to update the Conference Manager window to the selected date. Click the **OK** button to set the conference date in the Conference Reserver window, or to update the Conference Manager window to the selected date, *and* close the calendar. Click the **Cancel** button to close the calendar window and keep the current date.

The Change Password dialog box

From the Conference Manager window, you can change your login password by clicking on the **Password** button. When you click on the **Password** button, the Change Password dialog box opens, which Figure 32 shows.

Figure 32
Change Password dialog box

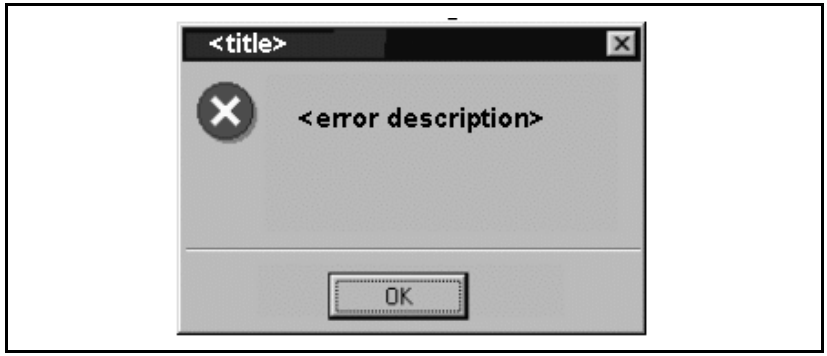


To change your user or super-user password, type in the new password you want to have. The new password can be up to six numbers. (Letters are not allowed.) Type the new password a second time to confirm it. Click **OK** to change your password and close this dialog box; MICB gives you a confirmation message that it has changed your password. Alternatively, you can click **Cancel** to close this dialog box without changing your password.

Abnormal BUI operation

Critical errors occur when the BUI can't execute the user's request or when unexpected conditions prevent BUI service. The reason for the critical BUI error can be failure of the equipment or incorrect configuration. Figure 33 shows the format of the critical error message.

Figure 33
Critical error message format



Operational errors are a result of incorrect user input or a temporary blocking of resources. In the case of incorrect user input, operation can continue immediately by re-entering the input correctly. In the case of temporary blocking of resources, the user must wait for resources to become available. Figure 34 shows the format of the operational error message.

Figure 34
Operational error message format

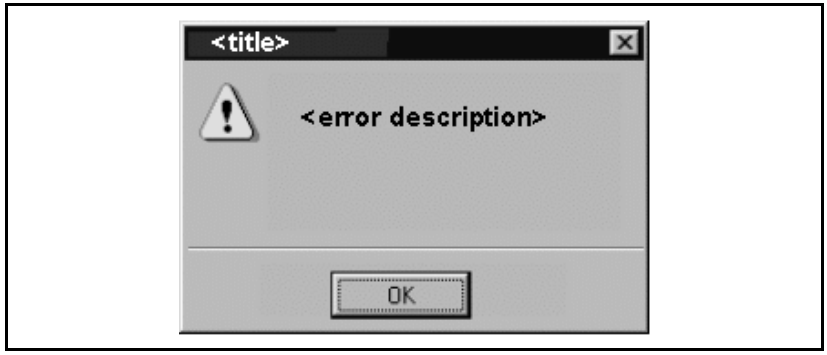


Table 15 lists some of the possible error messages.

Table 15
BUI error messages

Error title	Error description	Notes
Critical errors		
MICB	Lost communication with MICB. Re-access MICB with your browser.	This message appears when the BUI JAVA program loses communication with the MICB card (when the embedded server is used) or the server (when the external server is used).
Operational errors		
MICB Login	Incorrect password or user ID. Re-try login.	This message appears when the user tries to login with the incorrect user ID or password.
MICB Browser User Interface	User Interface server is full. Try again later.	This message appears when a user tries to access the BUI server at a time when the maximum number for a BUI session has been reached.
MICB Browser User Interface	User Interface blocked by maintenance activity. Try again later.	This message appears when the BUI is blocked because the administrator is using the CLI. It can occur in the middle of a BUI session, or when the user tries to access the MICB card.
MICB Browser User Interface	User interface is idle for too long - session disconnected!	This message appears when the BUI session is terminated due to a no-input timeout.

The Telephone User Interface

MICB provides a DTMF, menu driven, Telephone User Interface (TUI) scheduler. This interface allows a user to book a new simple conference using the key pad of the telephone. The user dials a unique DN for using the TUI, then schedules a conference by following a menu of instructions.

You must define the TUI DN in both the Meridian 1 system and the MICB card. In the Meridian 1 system, you define a new ACD DN with NCFW (see "The Command Line Interface" on page 93). In the MICB card, you define a new DN for the TUI scheduler through the Browser User Interface (BUI) (see "The Browser User Interface" on page 121). Also, you must use the BUI to define a TUI user ID for each user. A user that uses the TUI scheduler must first enters his or her TUI user ID and password. After scheduling a conference using the TUI, the user can see the conference on the BUI and only the user can modify or delete this conference.

The MICB card allocates only one port for the TUI. You define this port through the BUI. There are two options for configuring this port:

- available only for TUI use
- available for general use (both TUI use and conference use)

When you configure the port for TUI use only, only 31 ports are available for conference use. When you configure the port for general use, then it is available either for TUI purposes or for conference use.

Scheduling a conference

A user can use the TUI only to define a new simple conference with default attributes. The user inserts the conference parameters (through the key pad of the telephone) at the prompts of a guided voice menu. Also, the MICB plays actual voice error messages when the user makes a mistake.

Note: A user that calls the TUI has up to seven minutes to schedule a conference. After seven minutes, the MICB sends a voice message to the user indicating that the allotted time is over. The MICB then disconnects the call.

To schedule a simple conference through the TUI, perform the following procedure:

1. Dial the TUI DN.
2. Enter your TUI user ID.
3. Enter your TUI password (up to 6 digits).
4. Enter the date (optional) and time of the conference; the default date is the current date.
5. Enter the duration.
6. Enter the number of ports.
7. Enter the Conferee DN (optional); if not entered, the MICB card generates it. (The MICB card determines the Chairperson DN automatically.)
8. Enter the main and chairperson password lengths (optional).
9. Select the conference language (optional).

After the user enters all conference parameters, the MICB requests the user to confirm the reservation. The MICB sends a confirmation email to the TUI user.

The default attributes that the user does not set, but are set automatically by the MICB are:

1. Entry and exit by name
2. No custom greeting
3. No conference expansion
4. No name for the name of the conference
5. No name for the name of the chairperson

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

TUI voice files

The TUI voice files are audio files that are associated with scheduling a conference through the TUI. You cannot change these files and Nortel Networks includes them here for informational purposes only.

Table 16lists the TUI voice files that you hear when scheduling a simple conference.

Table 16
TUI voice files, simple conference reservation group

No.	Contents
1	*Welcome to the telephone menu driven scheduler*
2	*Please enter your user id up to 10 digits followed by star*
3	*Please enter your password up to 6 digits followed by star*
4	*To set a conference for today press '1', to set a conference for a specific day press '2'*
5	*Please enter the date.* *Two digits for the day, two digits for the month and four digits for the year followed by star*
6	*Please enter the time.* *Two digits from 0 to 23 hours and two digits in units of 15 minutes followed by star*
7	*Please enter the duration up to 12 hours.* *Two digits for the hours and two digits in units of 15 minutes followed by star*
8	*There are*
9	*Available ports*
10	*Please enter the number of ports up to the number of available ports, followed by star*
11	*To continue entering the conference definitions press 1, for automatic entering press '2'*

Table 16
TUI voice files, simple conference reservation group

No.	Contents
12	*To choose a DN press'1'*
13	*For automatic choice press'2'*
14	*To choose*
15	*Press*
16	*To choose a main password length*
17	*Press a digit between '4' and '8' followed by star. Otherwise press '0' followed by star*
18	*To choose a chairperson password length*
19	*To choose a language press '1'*
20	*The conference definitions are*
21	*Date is*
22	*Time is*
23	*Duration is*
24	*Number of ports is*
25	*Main DN is*
26	*Main password length is*
27	*Chairperson password length is*
28	*To approve press '1',to change press '2', to repeat conference definitions press '3', to input conference definitions again press '4'*
29	*The conference is defined as follows*
30	*Chairperson DN is*
31	*Main password is*
32	*Chairperson password is*

Table 16
TUI voice files, simple conference reservation group

No.	Contents
33	*I repeat*
34	*Your conference has been set successfully*
35	*Goodbye*
36	*Hours*
37	*Minutes*
38	*Date and time must be between now and a year from now*
39	*Duration is out of range*
40	*There are no DNs available for the requested time*
41	*There are no ports available for the requested time*
42	*DN is already in use*
43	*Conference DN does not exist*
44	*Incorrect input*
45	*You have failed to enter a correct input*
46	*The time to set a conference has expired*
47	*The telephone menu driven scheduler can not be access at this time*
48	*Please hang-up and call your Meridian Integrated Conference Bridge administrator*
49	*User id is*
50	*Password is*
51	*To approve press star*
52	*To change press other digit*
53	*And*

Table 17 lists the TUI voice files that play when selecting a language for the conference.

Table 17
TUI voice files, language selection group

No.	Contents
1	*For American English press*
2	*For Brazilian Portuguese press*
3	*For British English press*
4	*For Chinese press*
5	*For French press*
6	*For Japanese press*
7	*For Korean press*
8	*For L.A. Spanish press*
9	*For German press*
10	*For Italian press*

Table 18 lists the TUI voice files that play to confirm the language choice.

Table 18
TUI voice files, language confirmation group

No.	Contents
1	*Language is*
2	*American English*
3	*Brazilian Portuguese*
4	*British English*
5	*Chinese*
6	*French*
7	*Japanese*
8	*Korean*
9	*L.A. Spanish*
10	*German*
11	*Italian*

Table 19 lists the TUI voice files that play when modifying a conference.

Table 19
TUI voice files, conference modification group

No.	Contents
1	*To change date and time press*
2	*To change the duration press*
3	*To change the number of ports press*
4	*To change the DN press*
5	*To change the main password length press*
6	*To change the chairperson password length press*
7	*To change the language press*

Table 20 lists the TUI digit voice files.

Table 20
TUI voice files, digits group

No.	Contents
1	*One*
2	*Two*
3	*Three*
4	*Four*
5	*Five*
6	*Six*
7	*Seven*
8	*Eight*
9	*Nine*
10	*Zero*

Table 20
TUI voice files, digits group

No.	Contents
11	*Star*
12	*Number-sign*
13	Silence for 500ms
14	Silence for 1 second
15	*And*
16	*One (for a suffix)*
17	*Two (for a suffix)*
18	*Three (for a suffix)*
19	*Four (for a suffix)*
20	*Five (for a suffix)*
21	*Six (for a suffix)*
22	*Seven (for a suffix)*
23	*Eight (for a suffix)*
24	*Nine (for a suffix)*
25	*Zero (for a suffix)*
26	*Star (for a suffix)*
27	*Number-sign (for a suffix)*

Table 21 lists the TUI numbers voice files.

Table 21
TUI voice files, numbers group

No.	Contents
1	*One*
2	*Two*
3	*Three*
4	*Four*
5	*Five*
6	*Six*
7	*Seven*
8	*Eight*
9	*Nine*
10	*Ten*
11	*Eleven*
12	*Twelve*
13	*Thirteen*
14	*Fourteen*
15	*Fifteen*
16	*Sixteen*
17	*Seventeen*
18	*Eighteen*
19	*Nineteen*
20	*Twenty*
21	*Thirty*

Table 21
TUI voice files, numbers group

No.	Contents
22	*Forty*
23	*Fifty*
24	*Sixty*
25	*Seventy*
26	*Eighty*
27	*Ninety*
28	*Hundred*
29	*Thousand*
30	*Million*
31	*And*
32	*Zero*
33	*A.M.*
34	*P.M.*

Table 22 lists the TUI voice files regarding dates.

Table 22
TUI voice files, dates group

No.	Contents
1	*January*
2	*February*
3	*March*
4	*April*
5	*May*
6	*June*
7	*July*
8	*August*
9	*September*
10	*October*
11	*November*
12	*December*
13	*of January*
14	*of February*
15	*of March*
16	*of April*
17	*of May*
18	*of June*
19	*of July*
20	*of August*
21	*of September*

Table 22
TUI voice files, dates group

No.	Contents
22	*of October*
23	*of November*
24	*of December*
25	*the 1st*
26	*the 2nd*
27	*the 3rd*
28	*the 4th*
29	*the 5th*
30	*the 6th*
31	*the 7th*
32	*the 8th*
33	*the 9th*
34	*the 10th*
35	*the 11th*
36	*the 12th*
37	*the 13th*
38	*the 14th*
39	*the 15th*
40	*the 16th*
41	*the 17th*
42	*the 18th*
43	*the 19th*

Table 22
TUI voice files, dates group

No.	Contents
44	*the 20th*
45	*the 21st*
46	*the 22nd*
47	*the 23rd*
48	*the 24th*
49	*the 25th*
50	*the 26th*
51	*the 27th*
52	*the 28th*
53	*the 29th*
54	*the 30th*
55	*the 31st*
56	*1st*
57	*2nd*
58	*3rd*
59	*4th*
60	*5th*
61	*6th*
62	*7th*
63	*8th*
64	*9th*
65	*10th*

Table 22
TUI voice files, dates group

No.	Contents
66	*11st*
67	*12nd*
68	*13rd*
69	*14th*
70	*15th*
71	*16th*
72	*17th*
73	*18th*
74	*19th*
75	*20th*
76	*21th*
77	*22th*
78	*23th*
79	*24th*
80	*25th*
81	*26th*
82	*27th*
83	*28th*
84	*29th*
85	*30th*
86	*31st*

Maintenance

This chapter describes Meridian Integrated Conference Bridge (MICB) maintenance tools and procedures to guide you in identifying the MICB faults, locating defective equipment, correcting problems by fixing or replacing defective equipment, and verifying the operation of the MICB after corrections or replacements have been made.

Maintenance overview

You must approach problem identification systematically. A problem can have more than one cause. To isolate the cause, a knowledge of MICB operation is required. Once you identify the cause, you can correct the problem by replacing the defective card, connecting accidentally disconnected cables, or correcting the software security problem.

The 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).

This document focuses on the maintenance of the MICB equipment. It requires that the Meridian 1 system operate correctly before you start diagnosing the MICB problems. System installation and maintenance guide documents— *General Maintenance Information* (553-3001-500), *Fault Clearing* (553-3001-510), and *Hardware Replacement* (553-3001-520)—describe how to maintain the entire system. This chapter describes how to maintain the MICB as an integral part of the system.

Diagnostic tools

Use diagnostic tools to troubleshoot problems in the system including problems with the MICB. When diagnosing MICB problems, you might have to use more than one of these tools.

System diagnostic tools consist of:

- LED indicators
- display codes
- card self-tests
- sanity monitoring
- overlay commands
- history files

MICB status LED indicator

The MICB has a card LED indicator at the top of the faceplate. The card LED is a red LED that indicates the status of the card. If the LED is ON, the card can be faulty or disabled. When you power up the card, the card blinks three times during self-test and then it stays ON if functioning correctly, otherwise it turns ON without blinking and stays ON. The LED turns OFF when the card is software enabled.

Self-test

Each MICB card automatically performs a self-test when you insert it into an operating system module or when you power up or reset the system. You can also perform a self-test on a card using software commands or menus.

The self-test checks general MICB functions and determines whether they are operating correctly. It is very useful when you first install the cards, because the card automatically starts the self-test upon insertion and gives you an immediate indication of its operating status.

The self-test is a detailed test and analysis of the installed hardware, both to determine the integrity of the hardware and to establish the configuration of the MICB card by checking the processor, the RAM capacity, the Flash memory, the DSP, etc. See Table 23.

Table 23
MICB self-test sequence

Item tested	Description of action
Processor/Coprocessor	Read and store processor ID. Run processor self-test.
DRAM	Check the amount of DRAM installed. Perform R/W test.
PCI Chipset	Perform R/W test on selected registers.
System I/O Controller	Perform R/W test on selected registers.
PCMCIA Controller	Perform R/W test on selected registers.
DS-30X Interface	Test shared memory and perform loopback test over SD-30 LCA.
CE-MUX Interface	Test shared memory and perform loopback test over CE-MUX LCA.
PCMCIA DSP card(s)	Check the presence of DSP cards and initiate 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	Check the presence of Flash memory and the MICB check configuration information.

Sanity monitoring

Sanity monitoring is a background routine that checks the operation of system resources such as CPU activity, memory allocation, etc. This background routine attempts to restore normal system operation if the system performance has degraded to an unacceptable level. If all else fails, this routine restarts the system to try to restore it to normal 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 stays ON.

Overlay commands

Each card performs diagnostic tests as part of the daily routines, or you can activate diagnostic tests from a maintenance TTY or the SMP (when equipped). See the Nortel Networks technical publication (NTP), titled *Hardware Replacement* (553-3001-520).

The MICB card appears as an Extended Digital Line card to the system in which it is installed. You can use, therefore, all relevant system maintenance commands for an Extended Digital Line card with the MICB. Enabling and disabling of ACD digital telephone set M2616 is done in LD 32.

Table 24 lists some of the commands used to control the MICB status and functions.

Table 24
Commands to enable/disable MICB channels

LD 32 Commands	Operation performed
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 Command	**Operation performed**
UNTT	Performs self-test on the MICB.

The MICB card handles all the above commands exactly as the Extended Digital Line card does, transparently to the system.

History file

Information on any fault conditions is stored on the MICB card to provide a history file for the craftsperson. The file is in the form of a cyclical buffer, which is overwritten from the top when it runs out of space. It is configured to use memory resources efficiently.

MICB fault isolation and correction

Fault clearing procedures for the MICB are the same as for other IPE cards; refer to *Fault Clearing* (553-3001-510) for more information.

Table 25 deals specifically with MICB service problems. To diagnose these problems, the table refers you to the test procedures in this manual that can most likely resolve these problems based on the symptoms these problems exhibit.

Table 25
MICB equipment problems

Symptoms	Diagnosis	Solution
Red card LED on the MICB is permanently on.	Card is disabled or faulty.	Go to “MICB self-test steps” on page 178 to check the card status and perform self-test.
Display on the controller card shows fault codes.	Card faulty, failed self-test or problem communicating with peripheral equipment.	Go to “MICB self-test steps” on page 178 and “Reset MICB card command” on page 178 to check self-test and self-test on reset. Also refer to *X11 Administration* (553-3001-311) for a list of codes.
Error messages printed on the terminal or the Meridian 1 TTY.	Hardware or software problems with the MICB.	Note various error messages. Refer to *X11 Administration* (553-3001-311) for a list of these messages and their description. Based on the code’s description, take the appropriate action to resolve the problem.

If you cannot resolve the problem after exhausting all available diagnostic tools and test procedures, make a list of all the symptoms you observed and contact your field service representative.

MICB self-test steps

1. The card performs a self-test upon insertion.
2. The card LAN polls the card.
3. If the self-test passes, the card sends back a “powered-up occurred” message.
4. The card LAN requests the configuration data.
5. The card returns the configuration data (card type, X11 signaling type, and TN mapping type 2).
6. The card LAN enables the DS-30X signaling channel.
7. The MICB card waits until it receives the configuration data (trunk type, signaling type, balance impedance, etc.) via the DX-30X, but it then discards this data.
8. The card goes into its main program loop.

Reset MICB card command

1. The software sends a reset message to the card if no channels are busy.
2. The card sets all appropriate resources to the ‘disabled’ state and turns on the faceplate LED.
3. The MICB card resets and performs a self-test. Self-test results are stored in case the Meridian 1 performs a later query.
4. The card LAN polls the card.
5. If the self-test passes, the card sends back a “powered-up occurred” message.
6. The card LAN requests the configuration data.
7. The card returns the configuration data (card type, X11 signaling type, and TN mapping type 2) and enables the DS-30X link.
8. The card LAN enables the DS-30X signaling channel.
9. The card waits until it receives the configuration data (trunk type, signaling type, balance impedance, etc.) via the DS-30X, but it then discards this data.
10. The card goes to its main program loop.

Card replacement

The MICB is based on PCMCIA technology. This allows you to remove the MICB from the IPE shelf indefinitely without loosing the configuration data.

To replace the MICB card:

1. Disable the MICB card by loading the LD 32 overlay and executing the **DISC l s c** command, where **l**= loop, **s**= shelf or module, **c**= card in the module.
2. Remove the card from its card slot in the IPE module.
3. Remove the PCMCIA card from the faulty MICB card.
4. Transfer the PCMCIA card to the new MICB card.

   Note: This procedure moves all software, configuration, and records to the replacement MICB card.

5. Transfer the Security Device from the faulty MICB to the replacement.

   Note: The new card reuses the keycode. The keycode is still on the PCMCIA card, which you removed from the faulty MICB.

6. Enable the new card by executing the **ENLC l s c** command.
7. Configure the newly installed MICB card.
8. Package the faulty MICB card and ship it to the repair center.

   Note: When replacing the PCMCIA card, it is important to back up the data on the PCMCIA card so that you don't need to re-enter it. For instructions on backing up the data, refer to "Database Archive" on page 90.

External (PC) server maintenance

If the external server software fails on your PC, restart the MICB server program in *one* of the *three* following ways:

- Select **Start->Programs->Micb Server Application->Micb Server** from the server desktop.
- In the "C:\WINDOWS\Start Menu\Programs\MICB Server Application" window, double-click on the "MICB Server" icon.
- Restart the PC. The MICB Server program runs automatically after you restart the PC.

If this does not restore the external server to proper functionality, contact your distributor.

Note: Server failure does not affect conferences that users have already defined. It also does not affect TUI operation.

Appendix A: MMI error messages

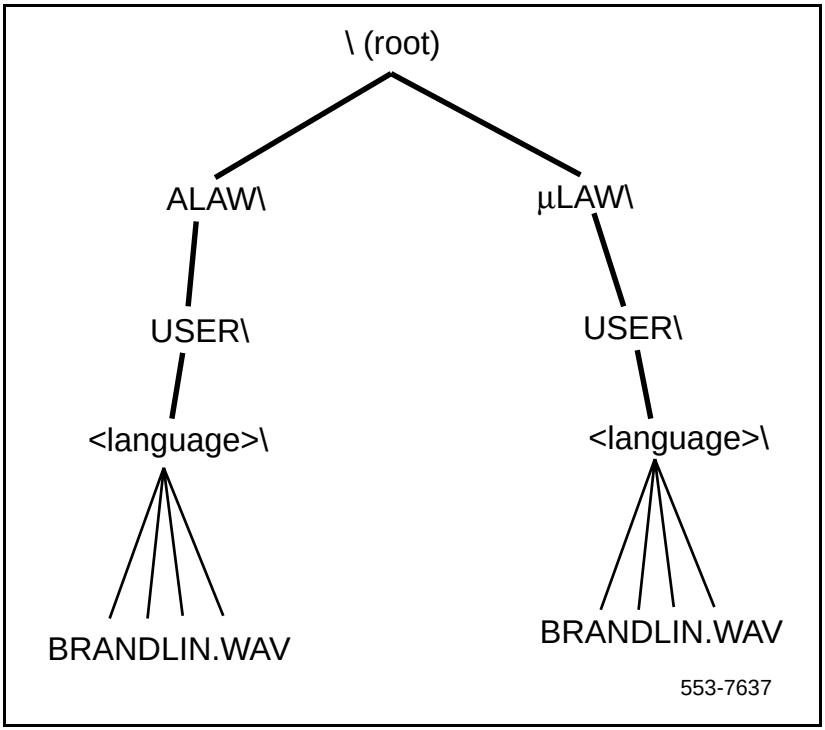
Appendix A contains the maintenance terminal pin assignments and the MMI error messages.

Brandline (custom greeting) file

A BRANDLIN.WAV file is copied to the PCMCIA disk to partition A: - the voice partition. Since voice files in the database are uncompressed, they have to be converted to the desired coding law before copying to the target PCMCIA disk. Partition A: is divided into two directories, A-law and μ-law, to which the converted voice files are copied.

You must record a separate brandline greeting for each language and copy it to the PCMCIA disk following the directory structure shown in Figure 35.

Figure 35
PCMCIA disk audio file structure



MMI Error Messages

These error messages are displayed on the maintenance terminal during conference events.

Table 26
MMI error messages (Part 1 of 2)

Error message text	Comments
Failure on accepting key code	Check the keycode.
Incorrect login	Enter the correct password.
Incorrect card ID entered	Check the card ID.
Wrong input type	Check the input type.
Input out of range	Specify the input within the rage.
Enter: yes, no, y or n.	Spell out yes or no.
Enter yes or no.	Enter the appropriate response.
Entered string too long	Check the string length.
Wrong number of input parameters	Check input parameters.
Input should be in HH:MM format.	Use the correct time format.
Invalid command for this directory	Check the directory/command.
Command not valid at this point	Check the command.
Audio recording in process, input ignored	Wait until recording is completed.
There are no reports for this date.	The specified date has no reports.
Date entered must not be in the future.	The date for conference maintenance must be present date.
Date entered is too far in the past.	Files are deleted once their age reaches “conf log aging”.
Date entered is too far in the future.	Reservations can be made only 6 months in advance.

Table 26
MMI error messages (Part 2 of 2)

Error message text	Comments
Command must be followed by a valid number.	Choose entry number according to the table presented.
Voice file specified does not exist.	When defining files per event
Voice file specified already exists.	When recording new file
Event must have at least one associated file.	Check the event and check the file table for that event.
A day in the past cannot be modified.	Check the specified date.
Error occurred while recording.	You may have to re-record.
DN provided for recording is available for 2 more minutes!	This is a warning.
Recording session terminated	End of recording is announced.
Invalid port number	Use the correct port number.

Appendix B: Product integrity

This chapter presents information about Meridian Integrated Conference Bridge (MICB) reliability, environmental specifications, and electrical regulatory standards.

Reliability

Reliability is measured by the Mean Time Between Failures (MTBF).

Mean time between failures (MTBF)

The MICB card Mean Time Between Failure (MTBF) is better than 88 years.

Environment specifications

Measurements of performance in regards to temperature and shock were made under test conditions as described in the following table.

Temperature-related conditions

Refer to Table 27 for a display of acceptable temperature and humidity ranges for the MICB.

Table 27
MICB environmental specifications

Specification	Minimum	Maximum
Normal Operation		
Recommended Relative humidity	15° C 20%	30° C 30% (non-condensing)
Absolute Relative humidity	0 ° C 5% to	40° C 90% (non-condensing)
Rate of change	Less than 1° C per 3 minutes	
Storage		
Long Term Relative Humidity	–40° C 20% –40° C to 70° C, non-condensing	70° C 55% (non-condensing
Short Term (less than 72 hr)	–40° C	70° C
Temperature Shock		
In 3 minutes In 3 minutes	-40° C to 25° C to	25° C 70° C
	-40° to 70° C, non-condensing	

Electrical regulatory standards

The following three tables list the safety and electro-magnetic compatibility regulatory standards for the MICB, listed by geographic region. Specifications for the MICB meet or exceed the standards listed in these regulations.

Safety

Table 28 provides a list of safety regulations met by the MICB, along with the type of regulation and the country/region covered by each regulation.

Table 28
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 29 lists electro-magnetic emissions regulations met by the MICB card, along with the country's standard that lists each regulation.

Table 29
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 30 lists electro-magnetic immunity regulations met by the MICB card, along with the country's standard that lists each regulation.

Table 30
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
AS/NZS 3548l	EMC (Australia/New Zealand)
NFC 98020	France EMC standard

Appendix C: Daily reports

There are two type of reports that are saved daily. The files are kept for a 32 (default) days or less (depending on the definition of “report aging days” system attribute).

The report files format are built according to the ASCII Comma-Delimited format (which supported also by EXCEL of Microsoft (as .CSV files)).

Pull the files by FTP over the TCP/IP LAN using a fixed password.

Over-booking report

Each line will save the following information:

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

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

The over-booking daily report format:

- 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>

Example:

- DATE: Aug 20 1998,,,
- hour,max ports,duration minutes,duration seconds
- 00,00,00,00
- 01,00,00,00

- 02,32,01,00
- 03,31,00,00
- 04,30,00,00
- 05,32,00,30
- 06,00,00,00
- 07,00,00,00
- 08,00,00,00
- 09,20,00,00
- 10,32,00,30
- 11,00,00,00
- 12,32,01,00
- 13,31,00,00
- 14,30,00,00
- 15,32,45,00
- 16,00,00,00
- 17,00,00,00
- 18,00,00,00
- 19,20,00,00
- 20,00,00,00
- 21,00,00,00
- 22,00,00,00
- 23,00,00,00

Billing report

Each line contains the following information:

- 1st field: time stamp in hours (00-23)
- 2nd field: time stamp in minutes (00-59)

- 3rd field: time stamp seconds (00-59))
- 4th field: event
  - 1 - Meeting Booked
  - 2 - Meeting Modified
  - 3 - Meeting Start
  - 4 - Active Meeting Modified
  - 5 - Meeting cancelled before it has started
  - 6 - Active meeting cancelled (after it has been started).
  - 7 - Meeting schedule time has ended.
  - 8 - Card Restart
- 5th field: card ID (up to 4 digit number)
- 6th field: meeting ID (up to 10 digit number)
- 7th field: billing account (up to 9 digit number)
- 8th field: meeting date
- 9th field: meeting start time in hours (00-23)
- 10th field: meeting start time in minutes (00-59)
- 11th field: meeting start time in seconds (00-59)
- 12th field: duration in hours (01-12)
- 13th field: duration in minutes (00-59)
- 14th field: ports (02-40)

Note: For a permanent bridge the meeting date, start time, and duration fields are not relevant and are therefore always equal to zero.

The first line is for the date, second line is for the field names, and all other lines are for the events.

The daily billing report format:

- 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>

Example (meeting ID is 32, user billing account is 999 and the 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 has been modify to 8 ports.

Third line - at 10:28am meeting has been started.

Forth line - at 11am active meeting has been modified to 3 hours duration.

Fifth line - at 01:28pm meeting has been ended (time has ended).

Sixth line - at 04:00pm card has been 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
- 13,28,00,07,7,32,999,,,,,,,
- 16,00,00,08,7,32,999,,,,,,,

Appendix D: Event script files

The Event Script files are audio files that are associated with conference events. An Event Script can contain a single file or a set of files that are activated in a specific sequence. You cannot change these files and Nortel Networks includes them here for informational purposes only.

Table 31 shows a list of events that occur during a conference. For each event the system plays one or more audio files to instruct the conferees and the chairperson. These audio files are listed in Table 32 and are numbered in the File column of this table.

Table 31
Voice script files (Part 1 of 3)

No.	Situation	Files
With name entry option:		
1.	Greeting to dial-in conferee with name entry	1, 2, 13
2.	Entry of conferee to meeting with prompt name	14, 3
3.	Exit of conferee from meeting with prompt name	15, 4
Without name entry option:		
4.	Greeting to dial-in conferee	1
5.	Entry of conferee to meeting	14
6.	Exit of conferee from meeting	15
General Prompts:		
7.	Announcement to single conferee	5, 6

Table 31
Voice script files (Part 2 of 3)

No.	Situation	Files
8.	Chairperson command acknowledge	16
9.	Chairperson command negative acknowledge (lack of resources)	17
10.	Chairperson command error acknowledge (illegal command)	17
11.	Dial-in to non-existent meeting	18
12.	Dial-in to locked meeting	106, 114, 26
13.	Dial-in to fully attended meeting	115, 26
14.	2nd chairperson dial-in attempt	116, 26
15.	Count conferees	27
16.	Meeting termination early warning-10 min till end	15, 7
17.	Meeting termination announcement	15, 8
18.	Record main menu	9
19.	Record invitation	13
20.	Record stopped	16
21.	Record error operation	11,9
22.	Record error operation for new file	11,10
23.	Record main menu for new file	10
24.	Nothing to play for new file	12
25.	Password request	21
26.	Repeated password request	22
27.	Incorrect password	23, 22

Table 31
Voice script files (Part 3 of 3)

No.	Situation	Files
28.	Exit from the system	24,25,26
29.	Announce to MIMS dialled-out user	71, 72
30.	Second TUI attempt	113, 114, 26
31.	Meeting lock	106
32.	Meeting unlock	107
33.	Meeting duration expanded	110
34.	Meeting duration not expanded	111
35.	Port muted	108
36.	Port unmuted	109
37.	All ports muted	117
38.	All ports unmuted	118
Help menus		
39.	Single conferee help	
40.	Participant help	
41.	Scrolling help	
42.	Dial out help	
43.	Chairperson first group help	
44.	Chairperson second group help	

Table 32 represents the system script files that play for a specific event as shown in Table 31 where, for example, event 1 activates files 1, 2, and 13.

Table 32
Event script files (Part 1 of 7)

No.	Contents
1.	*Welcome to the conference call*
2.	*Please say your name after the tone*
3.	*Is joining the meeting*
4.	*Is leaving the meeting*
5.	*You are the only person in the meeting now*
6.	Music
7.	*Your conference call will end in ten minutes*
8.	*Your conference call has ended, thank you*
9.	*Press 2 to play, 5 to record or number-sign to exit*
10.	*Press 5 to record or number-sign to exit*
11.	*You have entered an incorrect command*
12.	*There is nothing to play*
13.	tone 6 for 500 ms
14.	tones: 3,4,5,6 for: 100ms, 100ms, 100ms, 300ms respectively
15.	tones: 6,5,4,3 for: 100ms, 100ms, 100ms, 300ms respectively
16.	tone 2 for: 200ms on, 50ms off, 200ms on, off.
17.	tone 1: 5 bursts of 80ms on/ 80ms off
18.	tone 1: 250ms on/250ms off (Overflow tone) for 10 seconds
19.	tone 1: 500ms on/500ms off (busy tone) for 10 seconds
20.	tone 3: 200ms off/300ms on

Table 32
Event script files (Part 2 of 7)

No.	Contents
21.	*Password*
22.	*Please enter your password followed by number-sign*
23.	*Password incorrect*
24.	*You have failed to enter your password*
25.	*Please hang-up and call your Meridian Integrated Conference Bridge administrator*
26.	*Goodbye*
27.	*The number of conferees is:*
28.	*One*
29.	*One (for a suffix: e.g., twenty one)*
30.	*Two*
31.	*Two (for a suffix: e.g., twenty two)*
32.	*Three*
33.	*Three (for a suffix: e.g., twenty three)*
34.	*Four*
35.	*Four (for a suffix: e.g., twenty four)*
36.	*Five*
37.	*Five (for a suffix: e.g., twenty five)*
38.	*Six*
39.	*Six (for a suffix: e.g., twenty six)*
40.	*Seven*
41.	*Seven (for a suffix: e.g., twenty seven)*
42.	*Eight*

Table 32
Event script files (Part 3 of 7)

No.	Contents
43.	*Eight (for a suffix: e.g., twenty eight)*
44.	*Nine*
45.	*Nine (for a suffix: e.g., twenty nine)*
46.	*Ten*
47.	*Eleven*
48.	*Twelve*
49.	*Thirteen*
50.	*Fourteen*
51.	*Fifteen*
52.	*Sixteen*
53.	*Seventeen*
54.	*Eighteen*
55.	*Nineteen*
56.	*Twenty*
57.	*Twenty (for a prefix: e.g., twenty one)*
58.	*Twenty one*
59.	*Twenty two*
60.	*Twenty three*
61.	*Twenty four*
62.	*Twenty five*
63.	*Twenty six*
64.	*Twenty seven*

Table 32
Event script files (Part 4 of 7)

No.	Contents
65.	*Twenty eight*
66.	*Twenty nine*
67.	*Thirty*
68.	*Thirty (for a prefix: e.g., thirty two)*
69.	*Thirty one*
70.	*Thirty two*
71.	tones: 3,4,5,6 for: 100ms, 100ms, 100ms, 300ms respectively
72.	*You have a meeting please press star to enter*
73.	*User ID?*
74.	*Please enter your User ID followed by the number-sign*
75.	*If you have finished entering your User ID please press the number-sign*
76.	*Password?*
77.	*Please enter your Password followed by the number-sign*
78.	*If you have finished entering your Password please press the number-sign*
79.	*Login incorrect, please try again, User ID?*
80.	*Login incorrect, please contact your administrator for assistance, goodbye*
81.	*Room ID?*
82.	*Please enter the room ID, used the dial-pad to spell out the name of the room followed by the number-sign*
83.	*If you have finished entering the Room ID please press the number-sign*
84.	*Invalid Room ID, please try again, Room ID?*

Table 32
Event script files (Part 5 of 7)

No.	Contents
85.	*Invalid Room ID, please contact your administrator for assistance, goodbye*
86.	*You will be disconnected in ten seconds unless you complete your entry and press the number-sign*
87.	*You have entered too many digits*
88.	*Please wait*
89.	*Connecting you to your scheduled meeting*
90.	*There are no conference ports available, good bye*
91.	*Your account information can not be access at this time, please contact your administrator*
92.	*Please enter the room ID,.....*
93.	*The Room for the scheduled meeting is not ready, please call back at the start time or enter another room*
94.	*You have more than one scheduled meeting, Room ID?*
95.	*You will now join your meeting, please say your name after the tone*
96.	*The audio portion of your meeting will end in ten minutes*
97.	*The audio portion of your meeting will end in ten minutes, extend your meeting if necessary*
98.	*Your conference call has been extended*
99.	*Your conference call has ended, thank you*
100.	*Connecting you to your meeting*
101.	*Your conference port was reserved for another meeting starting in ten minutes, you can continue the meeting web only after that time*
102.	

Table 32
Event script files (Part 6 of 7)

No.	Contents
103.	
104.	
105.	tone of DTMF asterisk
106.	*Meeting is locked*
107.	*Meeting is unlocked*
108.	*Muted*
109.	*Unmuted*
110.	*Your meeting duration has been expanded*
111.	*Your meeting duration has not been expanded*
112.	*Port number is*
113.	*Telephone user interface scheduler is already in use*
114.	*Please try again in five minutes*
115.	*Meeting is fully attended*
116.	*Chairperson is already in the meeting*
117.	*All ports have been muted*
118.	*All ports have been unmuted*
119.	
120.	*To stop help menu press the star twice*
121.	*To dial-out press '*0' followed by the phone number and the number-sign*
122.	*To group call-out press '*2' followed by the group list number and the number-sign*
123.	*To redial last dialed-out number press '*#'*

Table 32
Event script files (Part 7 of 7)

No.	Contents
124.	*To self mute or unmute press '*19'*
125.	*To mute or unmute all participants press '*10'*
126.	*To return with the called party press '*2'*
127.	*To return to the meeting without the called party press '*3'*
128.	*To return to the meeting press '*3'*
129.	*To lock or unlock the meeting press '*4'*
130.	*To count conferees and play list of participants press '*6'*
131.	*To stop or continue the play of the list of participants press the number-sign*
132.	*To consult with the participant press '0'*
133.	*To mute or unmute the participant press '1'*
134.	*To play the current participant press '2'*
135.	*To play the previous participant press '4'*
136.	*To play the next participant press '6'*
137.	*To disconnect the participant press '9'*
138.	*To drop all participants press '*90'*
139.	*To drop last dial-out participant press '*91'*
140.	*To drop last dial-in participant press '*92'*
141.	*To expand conference duration by 15 minutes press '*98'*
142.	*To stop or replay music press '*99'*

Table 33 lists the beep frequencies and their levels.

Table 33
Tone specification

Index	Frequency (Hz)	Level (dBm/freq)
1	480+620	-24
2	440+660	-17
3	440	-14
4	560	-17
5	660	-17
6	880	-17
Maximum single frequency deviation is +/- 2% Maximum level deviation is +/- 5 dB		

List of Terms

ACD

Automatic Call Distribution.

ACD DN

Automatic Call Distribution Directory Number (pilot DN of an ACD queue).

ASIC

Application-Specific Integrated Circuit. A microprocessor chip designed to do specific tasks; providing graphics capability is one such task.

BIOS

Basic Input/Output System. Permanent program outlines in buffers that allow software to interact with hardware components (e.g., keyboard) in a device-independent manner.

Browser User Interface

An interface that allows the performance of OA&M functions on conferences, users, and cards through a standard web browser.

BUI

See Browser User Interface.

CE

Common Equipment.

CE-MUX

Common Equipment bus with MUltipleXed address and data.

Chairperson DN

The directory number the conference chairperson dials to enter the conference.

CLI

See Command Line Interface.

CO

Central Office.

Command Line Interface

An interface that allows the performance of OA&M functions on cards through telnet or through a standard VT100 terminal.

CCITT

The International Telegraph and Telephone Consultative Committee.

CPE

Customer Premise Equipment. Equipment that resides on a customer's premises and which the customer controls instead of the Central Office

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.

CRT

Terminal.

CSA

Canadian Standards Association.

dB

Decibel.

dBm

Decibel with reference to Milliwatt.

DID

Direct Inward Dial trunk.

DMA

Direct Memory Access.

DN

Directory Number.

DIN

A German manufacturer of electronic devices for interconnection and other purposes.

DS-30X

Parallel serial transmission from a superloop (XNET) card to a Controller Card in an IPE shelf.

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.

EEPROM

Electrically Erasable Programmable Read Only Memory device.

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”.

EPLD

Erasable Programmable Logic Device. An electronic device for performing logical operations that one can easily erase and reprogram.

ESD

Electro-Static Discharge.

ESS

Environmental Stress Screening.

EST

Environmental Stress Testing.

EXUT

Enhanced Universal Trunk card.

Field programmable

A program that is changeable after installation.

FCC

Federal Communications Commission.

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 semipermanently stored within ROM.

Flash memory

Electrically erasable memory that is non-volatile (not affected by power disruptions).

FPGA

Field Programmable Gate Array.

HI

Host Interface- DSP to MPU.

ID

Identification.

IDE

Integrated Drive Electronics. A low-cost hard disk drive interface.

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.

IVR

Interactive Voice Response. An application that allows telephone callers to interact with a host computer via pre-recorded messages and prompts.

Kernel

That part of a computer's operating system that performs basic functions like switching between tasks.

LAN

Local Area Network.

LED

Light Emitting Diode.

Loader

A device that moves a program or data from a floppy or hard disk and stores it into a computer's RAM memory.

M1

Meridian 1 switch.

Main DN

The directory number that conferees dial to enter the conference.

MAT

Meridian Administration Tool. Software enabling those performing OA&M to have a Windows™ graphical user interface (GUI) with Nortel (Nortel Networks) switches.

MINT

Message INTerrupt. This occurs when a message being transmitted receives an interrupt signal from an outside device, which must process a task of its own. Then the transmission of the original message can resume, or be resent.

MMail

Meridian Mail. Nortel's proprietary voice processing platform.

MMI

Man-Machine Interface.

MPU

Microprocessor Unit in the MICB card.

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.

MTTR

Mean Time To Repair. The average time required for corrective maintenance.

MWI

Message Waiting Indicator. A lamp or other visual display on a telephone set that informs the user that one or more messages have been left in the user's voicemail box.

NTP

Nortel Networks technical publications; customer documentation. Each NTP is identified by a unique ten-digit publication number.

OA&M

Operations, Administration, and Maintenance.

OEM

Original Equipment Manufacturers.

OTP

One-Time Programmable. Name given to a type of PCMCIA card.

PAS

Product Administration System.

PBX

Private Branch eXchange. A telephony switch that is privately owned.

PCB

Printed Circuit Board.

PCM

Pulse Code Modulation. A method for encoding an analog voice signal into a digital bit stream.

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.

RTC

Real Time Clock. System clocking influenced/determined by connection to a time process external to processing by the system.

SBC

Sub-Band Coding. Algorithm used by Meridian Mail and NGen for compressing speech data down to just over a quarter of its original size.

Scalable architecture

A way of designing a system that allows it to be resized with relative ease; the cost required to increase its size in proportion to the new size.

SCSA

Signal Computing System Architecture. A generalized open-system architecture describing the components and specifying the interfaces for a signal processing system for PC-based voice processing, call processing, and telecom switching.

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.

SL-1

Generic term given to Nortel digital switches. Meridian 1 refers specifically to the current series of Nortel PBXs.

STA

Single Terminal Access.

Telephone User Interface

An interface that allows the scheduling of simple conferences over a DTMF telephone.

TN

Terminal Number.

TUI

See Telephone User Interface.

VGA

Video Graphics Adapter. A computer adapter that provides high resolution graphics and 256 colors.

UART

Universal Asynchronous Receiver/Transmitter.

UI

User Interface.

.WAV

File format used for storing voice files created under Microsoft Windows.

Index

E

F

G

I

L

M

O

P

R

S

T

U

W

Meridian 1

Meridian Integrated Conference Bridge

Description, Installation, Administration, and Maintenance

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 Industry Canada. 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 their own expense.
SL-1 and Meridian 1 are trademarks of Nortel Networks.
Document number: 553-3001-102
Document release: Standard 4.00
Date: April 2000
Printed in Canada

NORTEL NETWORKS

How the world shares ideas.