Meridian 1

Meridian Integrated Voice Services

Description, installation, administration, and maintenance

Document Number: 553-3001-103
Document Release: Standard 1.00
Date: May 2000

Revision history

May 2000

Standard 1.00.

Contents

Installation and configuration **25**

About this document

This document explains how to install, configure, administer, and maintain the Meridian Integrated Voice Services (MIVS) card.

MIVS is an Intelligent Peripheral Equipment (IPE) card that provides the hospitality services of Automatic Wake Up (AWU) and Do Not Disturb (DND). The MIVS allows a guest to order their own wake up call and set a DND order through a user-friendly, easy-to-understand voice prompting sequence.

Product description

This chapter describes the Meridian Integrated Voice Services (MIVS). This chapter contains sections on the following topics:

- **Product overview**, which describes the operation and features of the MIVS product

- **MIVS card functional description**, which describes how the MIVS card functions within the Meridian 1

- **MIVS card physical description**, which describes the faceplate and backplane characteristics of the MIVS card

Product overview

MIVS lets a guest in a hotel, hospital, or other facility order Automatic Wake Up (AWU) and Do Not Disturb (DND) services from their room telephone. MIVS lets staff order AWU and DND services for guests. To order AWU and DND, guests and staff dial in to a Telephone User Interface (TUI). TUI offers a user-friendly, interactive menu system.

Overview of guest and staff operation

To order AWU or DND service, a guest dials either the AWU or the DND access DN, whichever is appropriate. The MIVS TUI prompts the guest to enter the appropriate information through the telephone keypad. If the request is successful, the MIVS TUI provides a confirmation message. The guest dials the same DN at any time to modify or cancel his request.

Note: Guests cannot customize TUI greetings.

The staff can order AWU or DND service at the guest's request. The staff dials the staff access DN and enters a password through the telephone keypad. The MIVS TUI gives the staff member the option of ordering either AWU or DND for a guest. The MIVS also gives the staff the option of customizing the TUI greetings guests hear. After the staff orders AWU or DND, MIVS prompts the staff to enter the guest's telephone number. The staff then orders the service in the same way a guest does. Also, the staff can dial into the TUI to modify or cancel the requested service.

Administration overview

The administrator determines the DNs for AWU, DND, and staff access by programming Automatic Call Distribution (ACD) queues in the X11 software. The administrator must also enter these access DNs, as well as a few other parameters, through a Browser User Interface (BUI). The administrator access the BUI from a Web browser on any PC that has a connection to the customer LAN. After the initial setup, the MIVS product requires very little, if any, ongoing administration. Ongoing administration activities include fine-tuning certain parameters, upgrading the MIVS software, and changing the number of ports (simultaneous callers) that MIVS supports.

System overview

MIVS offers 2-, 4-, and 8-port options. The size you choose depends on the number of rooms (or guests) your MIVS must serve. Each port serves one caller at a time; therefore, an 8-port MIVS can serve eight simultaneous callers.

Note: Nortel Networks recommends the 2-port option for facilities with up to 200 rooms, the 4-port option for up to 500 rooms, and the 8-port option for up to 1,000 rooms.

Figure 1 shows the position of MIVS in the Meridian 1.

Figure 1
MIVS system overview
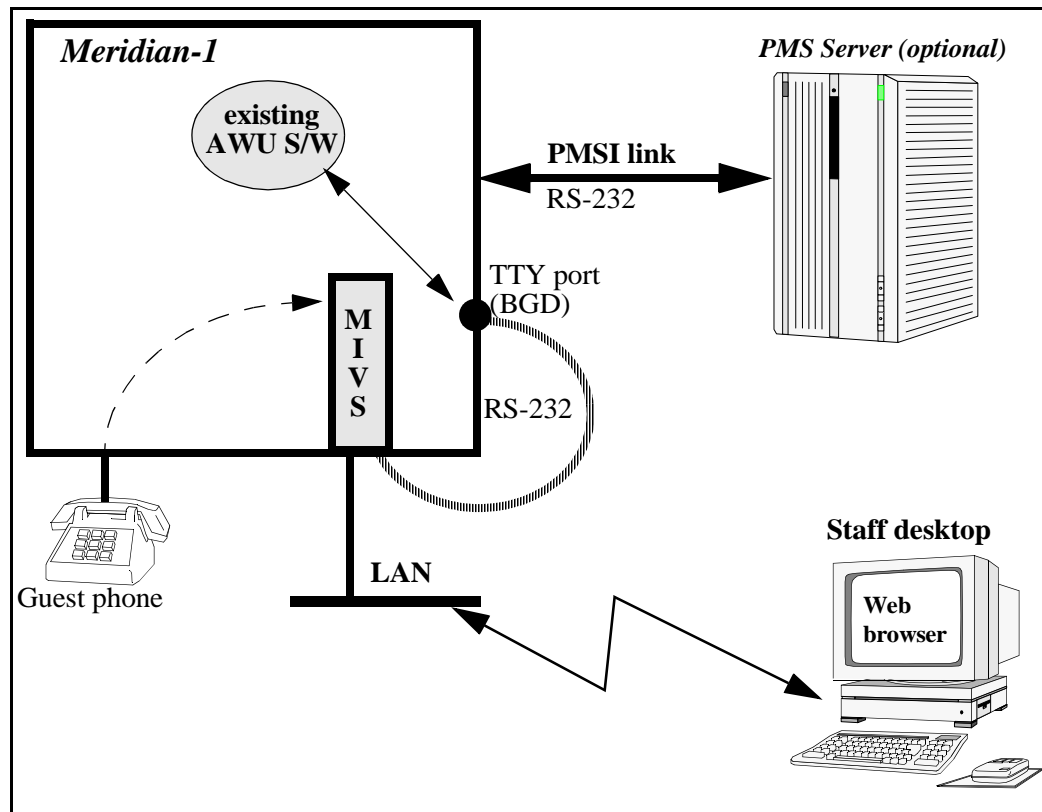
The MIVS card resides in an Intelligenet Peripheral Equipment (IPE) shelf or an Option 11C/11E cabinet. The MIVS card connects to the background (BGD) terminal through an RS-232 interface. The card sends AWU and DND requests to the Meridian 1 AWU and DND software through the BGD terminal. MIVS does not affect AWU and DND functionality, except that you cannot use AWU Flexible Feature Codes (FFCs) with MIVS.

The MIVS can also be used on the IPE expansion cabinet NTAK70XX.

MIVS does not affect the setup of the Property Management System (PMS) server. The PMS server provides room status updates to the Meridian 1, including the guest's language preference. The MIVS retrieves this information from the Meridian 1 when a caller dials into the MIVS.

Additional MIVS features

MIVS includes the following additional features:

- Occupies one slot in the IPE shelf or Option 11 cabinet

- Software transparent (the voice units emulate an M2616 digital set)

- Transmission Control Protocol/Internet Protocol (TCP/IP) connectivity is over Ethernet 10Base-T

- Multi-language voice prompts (MIVS retrieves the language preference from the Meridian 1 through the BGD terminal)

- Keycode and dongle protection of the following resources:

  — MIVS firmware release

  — Number of ports

  — Languages set

- Supports both A-Law and μ-Law

- Time and date (in the firmware) synchronize with the Meridian 1

- Uses files on Personal Computer Memory Card International Association (PCMCIA) disk for:

  — Firmware loads

  — Voice files

  — System configuration data

- BUI on embedded Web server for certain administration tasks

- Customization of the greetings through the TUI

MIVS card functional description

The MIVS card contains 2-, 4-, or 8-port options to handle two, four, or eight simultaneous callers. Each access DN is an agentless ACD queue that uses the Night Call Forward (NCFW) feature to transfer the caller to the main ACD card queue. The ports are the agents of the main ACD queue. Figure 2 provides a graphical representation of this process. You can also configure an additional agentless ACD queue to which MIVS directs guests following AWU and DND requests. For added value, this is configured as a service menu.

Figure 2
Dial access to MIVS services
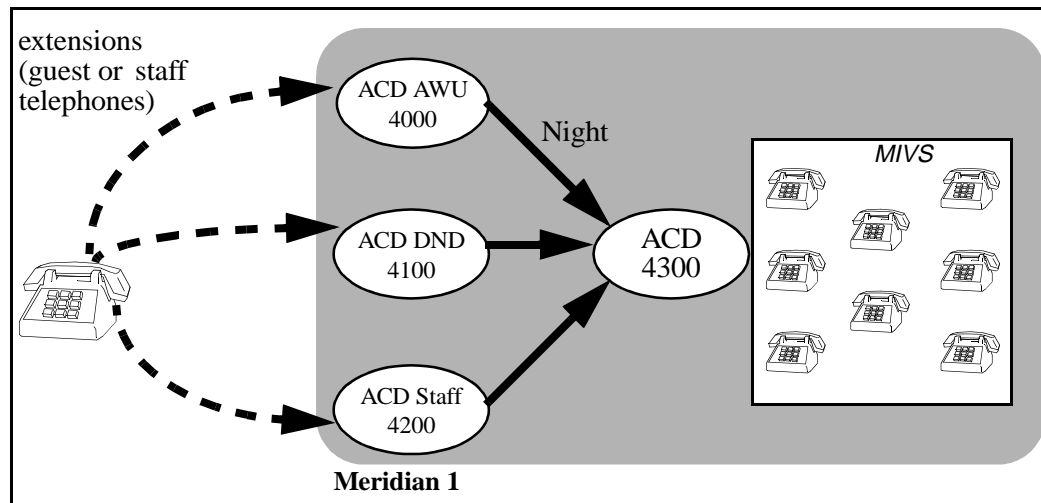
Note: The DNs in the above illustration represent examples only.

When a guest calls one of those services, the call is redirected to the MIVS ports. MIVS retains calling information as the call moves from queue to queue. When a call enters a MIVS port, information is available about the calling DN (which guest ordered) and the called DN (which service). The MIVS provides information to the guest regarding the current status of wake

up requests. However, this information is retrieved by the MIVS via the BGD port, and the process can take up to a few seconds, during which the guest must wait. Therefore, the guest hears a few seconds of ringback tone until the information is retrieved and the guest receives the prompts for the requested service.

After dialing the appropriate DN and being directed to the ACD queue, the guest receives the requested service.

Each service is configured as an ACD DN. In addition, the staff is assigned an ACD DN. Calls coming to one of the services are transferred to the ACD serving the MIVS cards, from where they are *walked-through* the prompting sequence.

Background Terminal Facility

MIVS connects to the Meridian 1 through a BGD SDI port. MIVS does not actually make the AWU and DND reservations for the guests; it simply transfers the requests to the Meridian 1 through the Background Terminal Facility. The Meridian 1 makes the reservations through its existing AWU and DND software. The Meridian 1 then returns confirmations of the services to the guests through the BGD terminal and the MIVS.

The Meridian 1 stores all of the AWU, DND, and other relevant information for the guests. When a guest or staff dials into the MIVS to request AWU or DND service, the MIVS retrieves this information from the Meridian 1 through the BGD terminal.

For more information about the BGD terminal, refer to *Background Terminal Facility description* (553-2311-316) in the Hospitality binder.

Security

MIVS uses a keycode to protect against unlawful feature usage. MIVS uses industry-standard PCMCIA cards as the software medium. The keycode restricts all upgrades of either port capacity or application software to a given MIVS card. Nortel Networks accurately tracks the keycodes to allow for satisfactory handling of field repairs and incremental upgrades. You must disable the card for all upgrades, backups, or restores.

Security is necessary for the following upgrades:

- Port capacity upgrades

- Feature enhancements

- New applications

Security is not necessary 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 upgrade. The keycode is entered through the CLI under the **Functionality Upgrade** menu. The keycode is 24 characters long and is entered in three sets of eight digits each called keycode1, keycode 2, and keycode 3.

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

MIVS capacity expansion

You can configure each MIVS card to provide two, four or eight ports. To activate a different number of ports than are currently active, you must do the following:

1   Disable the MIVS in LD 32.

2   Enter the CLI.

3   Select the **Functionality Upgrade** menu.

4   Select **Modify** to change the maximum number of ports available.

5   Select **Save** to save the changes.

6   Enable the MIVS in LD 32.

After you save the changes, you must enter the correct keycode that allows the changes to take effect. The keycode is 24 characters long, and you enter it in three sets of eight digits each (keycode1, keycode2, and keycode3). Refer to "Functionality Upgrade" on page 86 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 on the MIVS faceplate. Refer to "Software Upgrade" on page 87 for details.

MIVS card physical description

The MIVS card emulates an Extended Digital Line Card (XDLC) and communicates with the Meridian 1 through a BGD port. You can install the MIVS card into any slot on an IPE shelf or Option 11 cabinet that has the 50-pin input/output (I/O) cable. Figure 3 shows the MIVS card.

Faceplate description

The MIVS faceplate has the following characteristics:

Card LED

The MIVS faceplate provides a red card LED to indicate the status of the card. The card LED also indicates the card's self-test results during power up or insertion into an operating system. This LED indicates the following:

- The LED is ON when the MIVS card is disabled.

- The LED is OFF when the MIVS card is enabled and ready for use.

- The LED blinks three times and stays ON (until is software enabled) when the MIVS card has successfully completed the self-test.

Figure 3
MIVS card

Lock Latch

Status LED

PCMCIA Activity LED

PCMCIA slot B

PCMCIA Ejector

PCMCIA Activity LED

PCMCIA Slot A

PCMCIA Ejector

Lock Latch

PCMCIA
SOCKET
(for upgrades)

PCMCIA Hard
Drive Card

553-7624
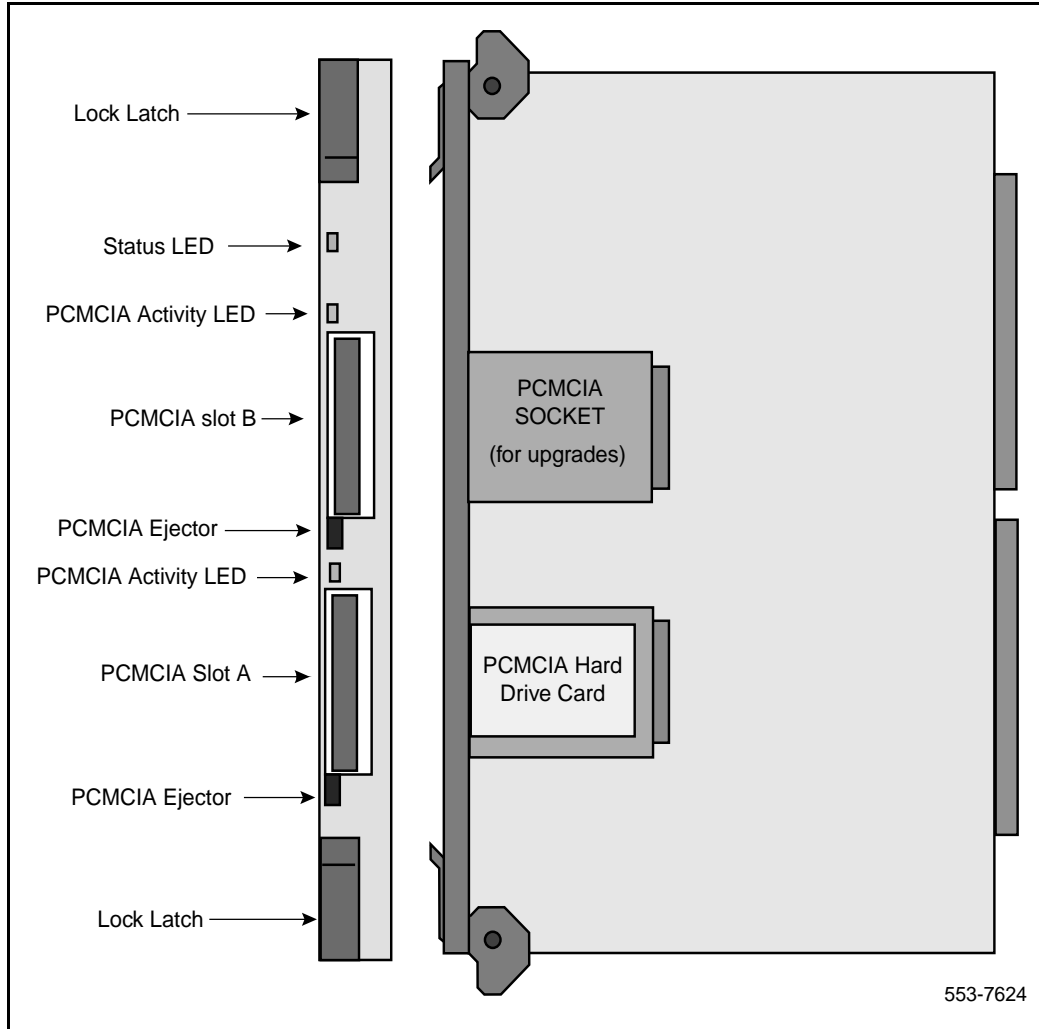
Type II/III PCMCIA slots

The MIVS faceplate provides two Type II/III PCMCIA card slots that hold the PCMCIA cards. The lower slot (drive A:) houses the PCMCIA hard drive card that stores voice prompts and firmware code. Use the upper slot (drive B:) to upgrade the firmware and make backups, when necessary. The PCMCIA hard drive card must remain in drive A: for continuous MIVS operation. Drive B: is normally empty.

PCMCIA activity indicator LEDs

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

- The LED is ON when the PCMCIA card is disabled.

- The LED is OFF when the PCMCIA card is enabled and ready for use.

- The LED blinks when the PCMCIA card is in use.

Backplane connections through the Ethernet adapter

An Ethernet interface on the MIVS is available at the I/O panel by installing the Ethernet adapter (see Figure 4). This adapter provides an Ethernet RJ-45 connector and a DB-9 connector. The RJ-45 connector provides multiple terminal access to the MIVS card (either the CLI or the BUI) through your LAN. The DB-9 connector provides serial connections to a maintenance terminal and a BGD terminal. There are two versions of the Ethernet adapter: one for Option 11C/11E and the other for IPE modules (see Table 6, "MIVS hardware list," on page 21). Also, see "Access to the Browser User Interface (BUI)" on page 23.

Note: If there is no LAN at the site, connect the PC to the Ethernet Adapter using a standard RJ-45 cross-over cable. Refer to Figure 5 on page 43 and Table 18 on page 45.

Figure 4
Ethernet adapter
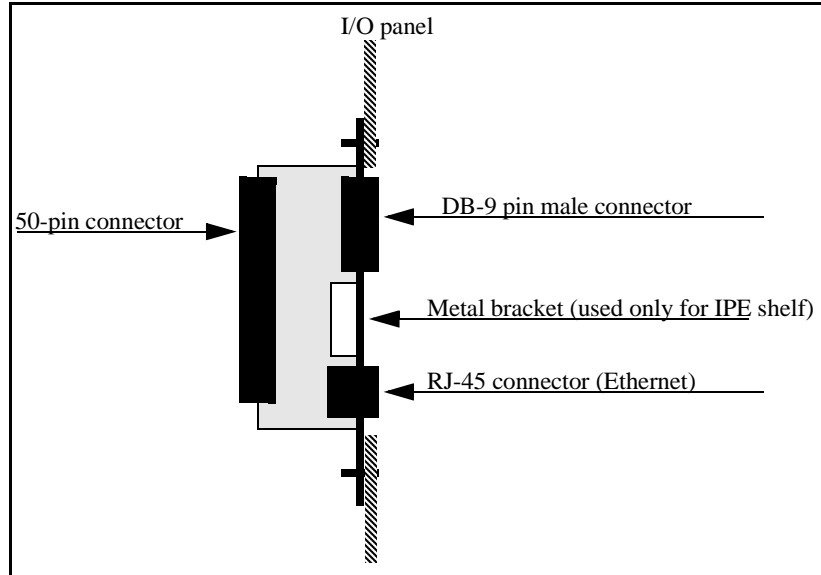
Engineering guidelines

The Meridian 1 general system engineering guidelines are described in *Meridian 1 system engineering* (553-3001-151). The following information deals specifically with engineering guidelines for the MIVS planning and implementation.

MIVS real-time impact

The MIVS real-time impact on the Meridian 1 compares to a Digital Line Card (DLC). For more information about real-time impact, refer to *Meridian 1 capacity engineering* (553-3001-149).

X11 system software engineering

The Meridian 1 must run on X11 Release 19 or later software. Each MIVS port (up to eight) emulates a digital set assigned to an ACD agent. All ports on an MIVS card belong to an ACD queue, which the ACD DN assigned to that specific MIVS card controls. MIVS routes guests and staff that dial the access DNs to the ACD queue.

Software package requirements

MIVS requires the standard X11 release software. Your system also requires the following software packages for correct MIVS operation:

- ACD basic package (45)

- ACD advanced features (41)

- Digital set (88)

- End-to-End signaling (EES) (10)

- Recorded Announcement (RAN) (7)

- Do Not Disturb (DND) (9)

- Control Class of Service (CCOS) (81)

- Background (BGD) Terminal (99)

- Room Status (RMS) (100)

- Automatic Wake Up (AWU) (102)

- Property Management System Interface (PMSI) (103), required only if customer uses PMS

- Multi-Language Wake Up (MLWU) (206), if multiple-language operation is necessary

System resource and network requirements

You must consider the use of system ACD resources. If applicable, you must review Incremental Software Management (ISM) for your specific Meridian 1 option. Each MIVS card requires the following system resources:

- Four or five ACD DNs and their associated queue and data block

- Access DNs:

  — Three agentless ACD queues for AWU, DND, and staff access

  — An optional agentless ACD for a special services (for example, Meridian Mail) menu

  — One ACD queue with up to eight agents

- A digital set block, TN, and DN for each port, up to eight. (The DN is used for outdialing and does not need to be available for Direct Inward Dialing [DID].)

- PMSI (only if using a Property Management System [PMS])

- Serial Data Interface/TeleTYpe (SDI/TTY) port for the BGD terminal

You must subtract these resources from the overall system resources. You cannot use these resources for any other application as long as they are for MIVS use.

Note: If you use agent IDs on your system, remember that MIVS *must* use successive agent IDs (for example, 3000–3007 for eight agent IDs). Ensure that a suitable block of agent IDs is available before you assign them.

MIVS requires an Internet Protocol (IP) address for administration and configuration purposes.

Incremental Software Management (ISM)

ISM calculations must consider the following:

- MIVS adds four or five ACD queues per card.

- MIVS adds up to eight ACD agents per card, corresponding to the number of MIVS ports on each card.

- MIVS can use a Meridian Mail agent for the optional special services menu.

Meridian 1 hardware engineering

MIVS comes in port-size options of 2, 4, and 8 ports. Each card requires one slot in an IPE shelf or an Option 11 cabinet. Table 1 lists the recommend port-size options for the various sizes facilities that MIVS must serve.

Table 1
Recommended port-size option for various facility sizes

Size of facility	Recommended number of ports
Up to 200 rooms	2
201–500 rooms	4
501–1000 rooms	8

System compatibility

The following systems support MIVS operation:

- Meridian 1 Options 11/11C, 11E, 21E, 51, 51C, 61, 61C, 71, 81, and 81C

- SL-1 systems NT and XT upgraded to support IPE cards

- MIVS can be installed in software releases X11 Release 19 and up, and X81 phase 7c and up

Table 2 lists the Meridian 1 modules and the card slots suitable for MIVS installation.

Table 2
MIVS installation into card slots in different IPE modules

Meridian 1 modules	MIVS card slots
NT8D11BC/ED CE/PE modules	All available IPE card slots.
NT8D37AA/BA/DC/EC[a] IPE modules	Slots 0, 4, 8, and 12
NT8D11AC/DC CE/PE modules	Slot 0

a. The NT8D37 BAA/BA/DC/EC IPE module is connected using 12 cables, so that the cabling of this shelf requires the use of only slots 0, 4, 8, and 12.
When slot 0, 4, 8, or 12 is used, you cannot use the port in the next slot. Any card that is in the next slot, that is, slot 1, 5, 9, or 13, cannot use the first half of its' slots.

The maximum number of MIVS cards per system is one.

MIVS requires access to a customer LAN. The MIVS card connects to the LAN through the Ethernet adapter at the I/O panel. The administrator configures access DNs and other parameters through a Web server.

Environmental requirements

The environmental requirements for the MIVS must meet or exceed the overall Meridian 1 system requirements. Table 3 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 that Table 3 specifies.

Table 3
Environmental requirements

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

Power requirements

The IPE module power supply (AC or DC) provides power to the MIVS. See Table 4 for a display of the MIVS power requirements. See also *Meridian 1 power engineering* (553-3001-152).

Table 4
MIVS power requirements

Voltage	Source	Current
+5 V	Backplane	3.0 A
+15 V	Backplane	0.1 A
Total maximum power		16.5 W

The maximum IPE module power budget is 30 watts per slot. To allow for thermal effects, it is best to budget no more than 20 watts per slot. The MIVS card does not exceed the power allocated for each card slot in the IPE module. Because of interaction with the PMS system, you can install only one MIVS per large or small system.

> *Note:* Power requirements limit the number of MIxx cards, including the MIVS, in an Option 11 cabinet to six. There is no restriction of this kind for IPE shelves.

Table 5 lists the transmit and receive analog signal levels as measured at the transmitter output and receiver input in the MIVS card.

Table 5
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, see *Summary of transmission parameters* (553-2201-182).		

MIVS hardware engineering

Table 6 lists the hardware components necessary for MIVS operation in the Meridian 1 and SL-1 systems.

Table 6
MIVS hardware list

Component	Description
NT5G15 MIVS card	An IPE card that provides AWU and DND reservation services for up to eight simultaneous callers. (The NT5G15 MIVS card, Security Device, Ethernet adapter, and PCMCIA hard drive card make up the NT5G04 package in N.A.)
PCMCIA hard drive card (NT5G33 in N.A.)	This PCMCIA card contains the MIVS software and configuration. It must reside in the lower PCMCIA drive of the MIVS card for MIVS to operate.
MIVS NT5D52AC Ethernet adapter (for IPE module installation)	This adapter attaches to the IPE module to provide connections from the MIVS card to the LAN and terminals.
MIVS NT5D52BC Ethernet adapter (for Option 11C/11E installation)	This adapter attaches to the Option 11C/11E tip/ring connector to provide connections from the MIVS card to the LAN and terminals.
NTBK48AA cable	This cable attaches to the DB-9 connector of the Ethernet adapter to provide a connection to the maintenance and BGD terminals.
RS-232 cable (customer provided)	This cable provides an extension from the NTBK48AA cable to the maintenance or BGD terminal.
RJ-45 cable (customer provided)	This cable attaches to the RJ-45 connector of the Ethernet adapter to provide a connection to the customer LAN.
RJ-45 cross-over cable (customer provided)	This cable attaches to the RJ-45 connector of the Ethernet adapter to provide a connection to the customer PC, where there is no LAN at the site.
NT5G96 20 MB PCMCIA Flash card	Use this card for software upgrades and backups.

BGD terminal

MIVS uses a BGD terminal to make AWU and DND requests to the Meridian 1 for the guest. The Meridian 1 handles these requests through its existing AWU and DND software. For more information about the BGD terminal, see *Background Terminal Facility description* (553-2311-316) in the Hospitality binder.

Access to the Command Line Interface (CLI)

The administrator uses the CLI to configure initial MIVS card parameters. The administrator also uses the CLI to perform certain maintenance and upgrade procedures. The administrator accesses the CLI through a maintenance (VT100 or a PC that emulates VT100) terminal. Set the maintenance terminal to the following parameters:

- Transmission rate: 9600 bps

- Data bits: 8

- Stop bits: 1

- Parity: no

- Flow control: none

    Note 1: Never use X-On/X-Off flow control, because flow control is hard-wired.

    Note 2: You must confgure the BDG terminal SDI port as DTE.

After you set up the MIVS card LAN parameters and connect the card to your LAN, you can Telnet to the card from any PC on your network that emulates a VT100 terminal.

Access to the Browser User Interface (BUI)

The administrator configures guest and staff access parameters through the BUI. The BUI is provided by the MIVS PCMCIA disk. Access to the BUI is through intranet only and requires a LAN and a Web browser on a PC.

LAN characteristics

Ethernet implementation over the MIVS has the following LAN characteristics:

- The MIVS Ethernet connection is separate from the external LAN traffic by a firewall.

- The Ethernet adapter options for MIVS are:

    — NT5D52AC for the IPE module

    — NT5D52BC for the Option 11C/11E cabinet (main or expansion)

- The LAN administrator assigns the IP address for the MIVS using the CLI interface during intial setup.

Web server characteristics

The web server houses the BUI and already resides on the MIVS card. Setting up 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.

Web browser characteristics

The BUI requires one of the following web browsers on a PC:

- Netscape Navigator 4.5 (or later)

- Microsoft Internet Explorer 4.01 (or later) with Service Pack 1 (SP-1)

To access the BUI, the user simply opens the browser and in the URL field, enter the address of the MIVS Web server.

The PC that contains the Web browser has the following requirements:

- 32 MB RAM (minimum)

- Windows 95 (or later)

- 200 MHz or faster processor (Pentium II recommended)

Access to the Telephone User Interface (TUI)

Guests and staff use the telephone user interface to order AWU, DND, and staff services. To access the TUI, a caller can use any Dual-Tone Multi-Frequency (DTMF) telephone in your telephone system. The TUI provides a simple DTMF menu-driven system for ordering AWU, DND, and staff services.

For TUI access, the administrator must designate access DNs in both the BUI and the X11 system software.

Installation and configuration

This chapter describes the installation and configuration of the MIVS card. This chapter describes the following installation and configuration topics:

- "X11 system software configuration" on page 30

- "MIVS installation preparation" on page 39

- "Connect the Ethernet adapter to the LAN" on page 44, "Connect the maintenance terminal" on page 47, "Connect the BGD terminal" on page 51, and

- "MIVS configuration" on page 52

Overview of system configuration and MIVS installation

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

Quick X11 system software configuration

To configure the X11 system software for an MIVS card, do the following:

1 Define a BGD terminal port in Overlay 17.

2 Define DND call treatment for your Meridian 1 in Overlay 15.

3 Define an ACD data block. This defines the ACD DN that you assign to the MIVS card (in Step 5).

   Note: If you use ACD agent IDs, remember to reserve a range of agent ID numbers for the MIVS ports.

4 Define the three access DNs (the AWU DN, DND DN, and Staff DN) in Overlay 23. These are three ACD queues with no agents. Set the Night Call Forward (NCFW) DN for each access DN to the ACD DN of the MIVS card.

5 Define each MIVS port as an M2616 digital set in Overlay 11. Define the MIVS ports as ACD agents in the ACD data block. Define the digital set keys as follows:

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

   — Key 1: Single Call Non-Ringing (SCN) with a dedicated DN

   — Key 2: Not Ready (NRD)

   — Key 3: Make Set Busy (MSB)

   — Key 4: Call Transfer (TRN)

   — Key 5: Three-Party Conference (AO3)

   — Key 10: Display

6 Define the service DN in Overlay 23. This step is optional, but necessary if you want to automatically transfer the guests to either Meridian Mail services or an attendant after they order AWU or DND service. Set the NCFW prompt to the Meridian Mail DN and ensure that the queue is in *night service*.

7 You can configure Incoming Call Indicator (ICI) keys.

Quick MIVS installation and configuration

To install the hardware for MIVS, do the following:

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

2   Identify the card slot in the IPE module, Option 11C, or 11E cabinet where you intend to install the MIVS card.

3   Install the NT5D52AC Ethernet adapter onto the IPE module I/O panel or the NT5D52BC into the Option 11C/11E tip/ring connector cutout. See "Install the Ethernet adapter" on page 41.

4   Install the MIVS card in the designated card slot. For available card slot locations, see Table 2, "MIVS installation into card slots in different IPE modules," on page 18.

5   Connect a VT100 terminal (or a PC emulating a VT100 terminal) to the MIVS card through the Ethernet adapter and NTBK48AA cable. See "Connect the maintenance terminal" on page 47 and select the appropriate connection option based on your requirements. See also "Configure the maintenance terminal" on page 54.

6   At the VT100 terminal, enter the keycodes for the MIVS cards. See "Functionality Upgrade" on page 86 for keycode entry. See also "Enter the keycode information" on page 54.

VT100 connection is only required for initial configuration. After you enter the keycode and network address information, you can access MIVS using Telnet or a similar application.

7   Still at the VT100 terminal, log into the CLI (login name = **user**) and set the IP address, subnet mask, and gateway address for the MIVS card. After this, restart the MIVS card. See "Set the LAN parameters in the CLI" on page 55.

8   Connect the MIVS card to the LAN through the RJ-45 connector on the Ethernet adapter.

9   Connect MIVS RS-232 port to the Meridian 1 BGD.

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

11   At the system terminal, load Overlay 32 to enable the MIVS card (**ENLC l s c**, where **l** is the loop, **s** is the shelf, and **c** is the card).

For Option 11 systems, the enable command is ENLC s c, where s is the shelf and c is the card.

12   From the Web browser on your PC, enter **http://<card IP address>/mivs_bui.htm** to access the MIVS BUI, where **<card IP address>** is the IP address of the MIVS card, which you configured (in Step 7).

13   Log into the BUI (user name = **admin** and password = **000000**) and enter the appropriate information. See "Configure the MIVS administration parameters in the BUI" on page 56.

Program ICI keys for MIVS

In some cases, the MIVS transfers the guest to operator assistance (attendant console). It is **optional** to define ICI to identify the call type (MIVS call). See Tables 7 and 8.

Table 7
LD 15 ICI definition

Prompt	Response	Description
REQ	CHG	Change data.
TYPE	CDB ATT	Customer Data Block. ATT for Release 21 gate opener
CUST	0–99	Customer number
OPT	ICI IC2	Incoming call indicator
ICI	0–19 LDx	(x=0–3, for listed directory number)
Note: The MIVS administrator can define ICI as LDN.		

Define LDN for ICI as described in Table 8.

Table 8
LD 15—LDN for ICI definition

Prompt	Response	Description
REQ	CHG	Change data.
TYPE	CDB LDN	Customer Data Block. LDN for Release 21 gate opener
CUST	0–99	Customer number
OPT	NLDN XLDN	
DLDN	YES NO	
LDN0	xxxx	xxxx – listed Directory Number 0
LDA0	1–63 ALL	Attendant console associated with LDN 0)
LDN1	xxxx	(xxxx - listed Directory Number 1)
LDA1	1–63 ALL	(Attendant console associated with LDN 1)
...		
LDN5	xxxx	(xxxx - listed Directory Number 0)
LDA5	1–63 ALL	Attendant console associated with LDN 5
ICI	xx LD0	xx key number for ICI for LDN 0–5
	xx LD1	
	...	
	xx LD5	

X11 system software configuration

Before you install any of the MIVS hardware, you can configure the X11 system software for MIVS through the system TTY terminal.

Note: For MIVS, your Meridian 1 must run X11 Release 19 or later software. Also, your Meridian 1 must have the software packages that "Software package requirements" on page 15 lists.

Define the BGD terminal port

The MIVS card does not store AWU information. When a guest requests AWU service, the MIVS card forwards the request to the existing AWU software on the Meridian 1. To enable the transfer of AWU requests from the MIVS card to the Meridian 1, you must set up a BGD terminal. The setup involves the definition of a BGD terminal port in the X11 system software.

Note: This means that there must be a free serial port available on the system.

To define the BGD terminal port, load Overlay 17 from the system terminal and enter the appropriate responses to the prompts as shown in either Table 9 (Options 21-81C) or Table 10 (Option 11).

Table 9
Define a BGD terminal port through Overlay 17 (Options 21–81C)

Prompt	Response	Description
REQ	CHG	
TYPE	CFN	
ADAN	NEW/CHG TTY xx	xx is the device number, from 0–15
CTYP	aaaa	Card type (DCHI, MSPS, SDI, SDI2, or XSDI)
GRP	x	Network group number, from 0–4 (Option 81)
DNUM	xx	Device number, from 0–15 (the same as the ADAN device number)
DES	a...x	Designator for AML port
USER	BGD	For background terminal
CUST	xx	Customer number, from 0–99

Table 10
Define a BGD terminal port through Overlay 17 (Option 11)

Prompt	Response	Description
REQ	CHG	
TYPE	ADAN	
ADAN	NEW/CHG TTY xx	xx is the device number, from 0–15
TTY_TYPE	SDI	
CAB	x	SDI cabinet number
CDNO	xx	SDI card number
PORT	xx	Device number, from 0–15 (the same as the ADAN device number)
DES	a...x	Designator for AML port
FLOW	NO	No flow control
BPS	9600	Rate of data transfer, in bits per second
BITL	8	Bit length of 8
STOP	1	1 stop bit
PARY	NONE	No parity
ENL	NO	
USER	BGD	For background terminal
CUST	xx	Customer number, from 0–99
Note: See "Configure the BGD terminal" on page 53.		

Define DND call treatment for the Meridian 1

You must define a treatment for calls to a DN that has DND active. You can have the Meridian 1 return a busy tone (BST) to the caller, or you can transfer the caller to either an attendant (ATT) or a designated recorded announcement (RAN) route. To define DND call treatment for your Meridian 1, load Overlay 15 from the system terminal, and enter the appropriate responses to the prompts that Table 11 shows.

Table 11
Define DND call treatment for the Meridian 1 through Overlay 15

Prompt	Response	Description
REQ	CHG	
TYPE	CDB/FTR	FTR for Release 21 gate opener
CUST	xx	Customer number, from 0–99
DNDL	YES, (NO)	Definition of the DND lamp for analog sets, for DND indication
...		
TYPE	INT	Release 21 gate opener
DNDT	(BST), ATT, RAN	Treatment for calls to DNs with DND active: busy tone, attendant, or recorded announcement
RRT	xxx	RAN route for DND treatment, from 0–511

Define the ACD data block

To configure the ACD data block, load Overlay 23 from the system terminal and enter the appropriate responses to the prompts that Table 12 shows. This defines the main ACD DN of the MIVS card.

Table 12
Define the ACD data block through Overlay 23

Prompt	Response	Description
REQ	NEW	New control data block
TYPE	ACD	ACD data block
CUST	xx	Customer number, from 0–99
ACDN	<ACD DN>	Main ACD DN of the MIVS card
MAXP	8	Maximum number of ACD agent positions

Note 1: Leave the NCFW prompt blank when you define the ACD DN assigned to the MIVS card.

Note 2: You must reserve a range of agent ID numbers for the MIVS ports. Refer to the information contained in Note 2 on page 50.

Define the access DNs

You must define three ACD queues with no agents: the AWU access DN, the DND access DN, and the staff access DN. Each ACD queue (access DN) must NCFW to the main ACD DN of the MIVS card. To define the access DNs, load Overlay 23 from the system terminal, and enter the appropriate responses to the prompts that Table 13 shows.

Table 13
Define the access DNs through Overlay 23

Prompt	Response	Description
REQ	NEW	New control data block
TYPE	ACD	ACD data block
CUST	xx	Customer number, from 0–99
ACDN	<DN#>	The access DN (either for AWU, DND, or staff)
MAXP	1	Maximum number of ACD agent positions
NCFW	<ACD DN>	The main ACD DN of the MIVS card you defined in Table 12.

Note: Repeat commands in this table for each of the three access DNs.

Define MIVS ports as digital sets

Each MIVS port represents an ACD agent with the digital set M2616. Table 14 shows how to use the Multi-line Telephone Administration program, Overlay 11, to configure these features.

Note: MIVS does not support autoconfiguration for Option 11. You must define the MIVS ports manually.

Table 14
Configure MIVS ports as digital sets through Overlay 11

Prompt	Response	Description
REQ	NEW	Add a new data port
TYPE	2616	Digital telephone set M2616
TN	l s c u	Terminal number of the MIVS port
DES	a...x	ODAS telephone designator
CUST	xx	Customer number, from 0–99
KEY	0 ACD <ACD DN> <CLI> <pos ID>	ACD DN plus CLI plus position ID (CLI = 0, usually)[1]
KEY	1 SCN <any DN>	Line key
KEY	2 NRD	Not Ready key
KEY	3 MSB	Make Set Busy key
KEY	4 TRN	Call Transfer key
KEY	5 AO3	Three-party conference
KEY	10 DSP	Display
Note 1: CLI required for Release 22 and later.		

Note: The number of virtual ACD agents of the ACD queue is equal to the number of MIVS ports. For example, if you enable four ports, you must define four ACD agents. If the TN for the MIVS card is 28 0 6, for example, then the TNs for the four agents are 28 0 6 0 through 28 0 6 3. Port sequencing always begins at Port 0.

Define the service DN (optional)

You can define a service DN that transfers guests automatically to either Meridian Mail services or to an attendant, after they order AWU or DND service. To define this service DN, load Overlay 23 from the system terminal and enter the appropriate responses to the prompts that Table 15 shows.

Table 15
Define the service DN through Overlay 23

Prompt	Response	Description
REQ	NEW	New control data block
TYPE	ACD	ACD data block
CUST	xx	Customer number, from 0–99
ACDN	<DN#>	The service DN for the MIVS card
MAXP	1	Maximum number of ACD agent positions
NCFW	<DN#>	The DN for Meridian Mail or an attendant. You must first define the Meridian Mail **Service** menu.

Sample dial plan for MIVS

Table 16 shows a sample dial plan for an MIVS card.

Table 16
Sample dial plan for a MIVS card

Description of DNs	Sample DNs	See Note
ACD DN	7000	Table 12
AWU access DN	7001 (NCFW=7000 in LD 23)	Table 13
DND access DN	7002 (NCFW=7000)	Table 13
Staff access DN	7003 (NCFW=7000)	Table 13
Special service DN	7004 (NCFW=MM or attendant DN)	Table 15
Note: For the third-column references, see "Sample dial plan for MIVS" on page 38.		

MIVS installation preparation

The preparation consists of unpacking and inspecting the components, taking inventory, and locating the card slot where you will install the MIVS card.

Unpack and inspect the components

Unpack and inspect the equipment for damage. When you unpack, follow the general precautions that computer and telephone equipment manufacturers recommend:

1   From the installation site, remove items that generate static charge.

2   Use antistatic spray if the site has carpet.

3   Check that you have the RJ-45 and RS-232 customer supplied cables. Refer to Table 6 on page 21.

4   Ground yourself before you handle any equipment.

5   Remove equipment carefully from its packaging.

6   Visually inspect the equipment for obvious faults or damage. Report any damaged component to your sales representative and the carrier who delivered the equipment.

Take inventory

1   After you have unpacked and visually inspected the equipment, verify that all the equipment is at the site before the installation begins.

2   Check the equipment you received against the shipping documents.

3   Note any shortages and report them to your sales representative. PMS requirements limit the number of MIVS cards per system to one.

Identify the card slot

Table 17 lists the Meridian 1 modules and the card slots suitable for MIVS installation.

Table 17
MIVS installation into card slots in different IPE modules

Meridian 1 modules	MIVS card slots
NT8D11BC/ED CE/PE modules	All available IPE card slots.
NT8D37AA/BA/DC/EC[a] IPE modules	Slots 0, 4, 8, and 12
NT8D11AC/DC CE/PE modules	Slot 0

a. The NT8D37 BAA/BA/DC/EC IPE module is connected using 12 cables, so that the cabling of this shelf requires the use of only slots 0, 4, 8, and 12.
When slot 0, 4, 8, or 12 is used, you cannot use the port in the next slot.
Any card that is in the next slot, that is, slot 1, 5, 9, or 13, cannot use the first half of its' slots.

Note: Power requirements limit the number of MIxx cards, including the MIVS, in an Option 11 cabinet to six. There is no restriction of this kind for IPE shelves.

MIVS equipment installation

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

- verify that the preinstallation preparation has been completed (this includes verifying that all the equipment has been received undamaged)

- plan your MIVS equipment, port configuration, and external equipment connection configuration (see "Engineering guidelines" on page 15).

Install the Ethernet adapter

On 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 you will install the MIVS.

2   Plug the 50-pin connector on the NT5D52BC Ethernet adapter into the 50-pin tip/ring connector on the Option 11C/11E cabinet.

3   Secure the Ethernet adapter to the cabinet.

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 of 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 selected for MIVS card installation.

5   Install the NT5D52AC Ethernet adapter into the selected I/O panel connector cut-out using the saved retaining screws. See Figure 6 on page 46.

6   Fasten the I/O panel to the module using the retaining screws that you removed earlier. Replace the module's cover plate.

Install the MIVS card

1   Identify the IPE card slot selected for the MIVS card. Refer to Table 17, "MIVS installation into card slots in different IPE modules," on page 40.

2   Make sure that the PCMCIA hard drive card is in the lower PCMCIA slot on the faceplate, and that it is firmly seated.

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

4   Insert the MIVS card into the card guides and gently push the card until the card makes contact with the backplane connector.

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

6   Observe the Red LED at the top of the faceplate (the card LED). This LED blinks three times after the self-test successfully finishes. The LED then stays ON until you software enable the MIVS card.

MIVS cabling

You connect the MIVS card to the maintenance terminal, the BGD terminal, and your LAN through the Ethernet adapter. Before you make these connections, however, attach the NTBK48AA cable to the DB-9 connector of the Ethernet adapter (see Figure 5).

Note: The TTY port labeled P1 needs to be permanently connected to an SDI port programmed as a background terminal (BGD). The P2 port is unused in this MIVS version.

Figure 5
The Ethernet adapter and the NTBK48AA cable
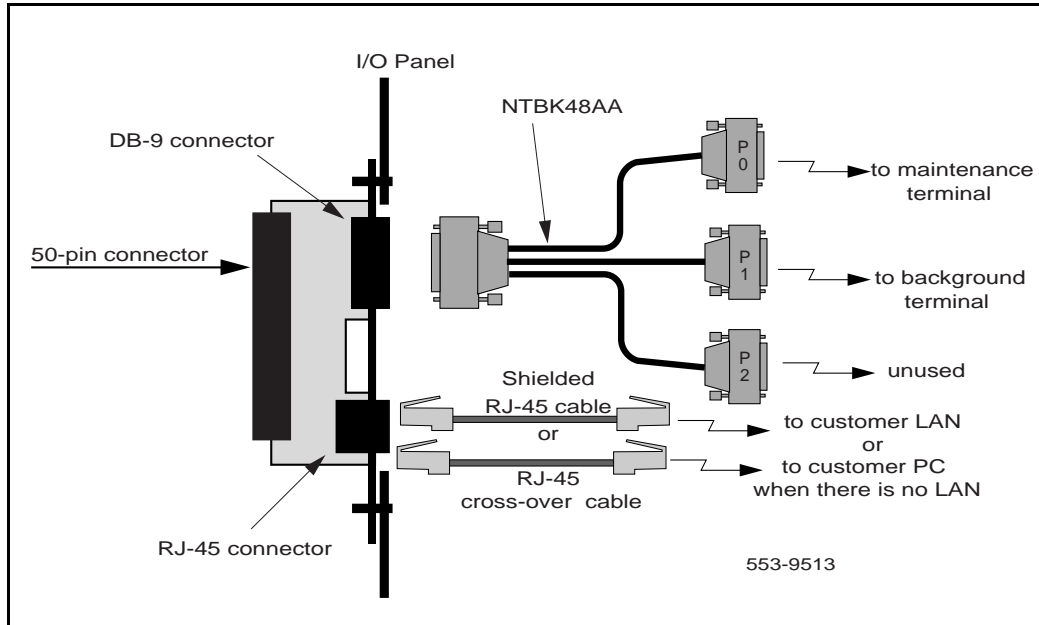
Connect the Ethernet adapter to the LAN

You must connect the MIVS card to your LAN, through the Ethernet adapter, to have access to the BUI. With a connection to your LAN, you can also telnet to the CLI from a terminal on your intranet. To connect the MIVS card to your LAN, follow these steps:

1   Check the installation of the Ethernet adapter on the I/O panel according to "Install the Ethernet adapter" on page 41.

2   Plug the modular cable RJ-45 plug into the RJ-45 jack on the Ethernet adapter. See Figure 6 on page 46

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

4   Make the other necessary Ethernet connections using standard Ethernet connection rules.

Connect the Ethernet adapter to a customer PC when no LAN exists

To connect the MIVS card to a customer PC when no LAN exists, follow these steps:

1   Check the installation of the Ethernet adapter on the I/O panel according to "Install the Ethernet adapter" on page 41.

2   Plug the modular cross-connect cable RJ-45 plug into the RJ-45 jack on the Ethernet adapter. See Figure 6 on page 46.

The LED on the Ethernet Adapter should be lit for a proper connection. If it is not lit, re-connect the cable.

Refer to Table 18, "RJ-45 cross-over (Ethernet) cable pinouts," on page 45 for the RJ-45 cross-over cable pinouts.

3   Plug the RJ-45 plug at the other end of the modular cross-connect cable RJ-45 cable into the PC.

Figure 6 on page 46 illustrates the I/O connector bracket connection to the MIVS card, the maintenance terminal, the LAN and PC connections.

Table 18
RJ-45 cross-over (Ethernet) cable pinouts

Pin Number	Signal	Pin Number	Signal
1	TX+	3	RX+
2	TX -	6	RX -
3	RX+	1	TX+
4	---	4	---
5	---	5	---
6	RX -	2	TX+
7	---	7	---
8	---	8	---

Figure 6
Maintenance terminal and LAN or PC connection through the Ethernet adapter

NOTE: ①,②,③ Indicate three ways of connecting the terminal.
For item 3, the alternate connection
(shown by the dashed line) is to the customer PC
when there is no LAN.

553-9515
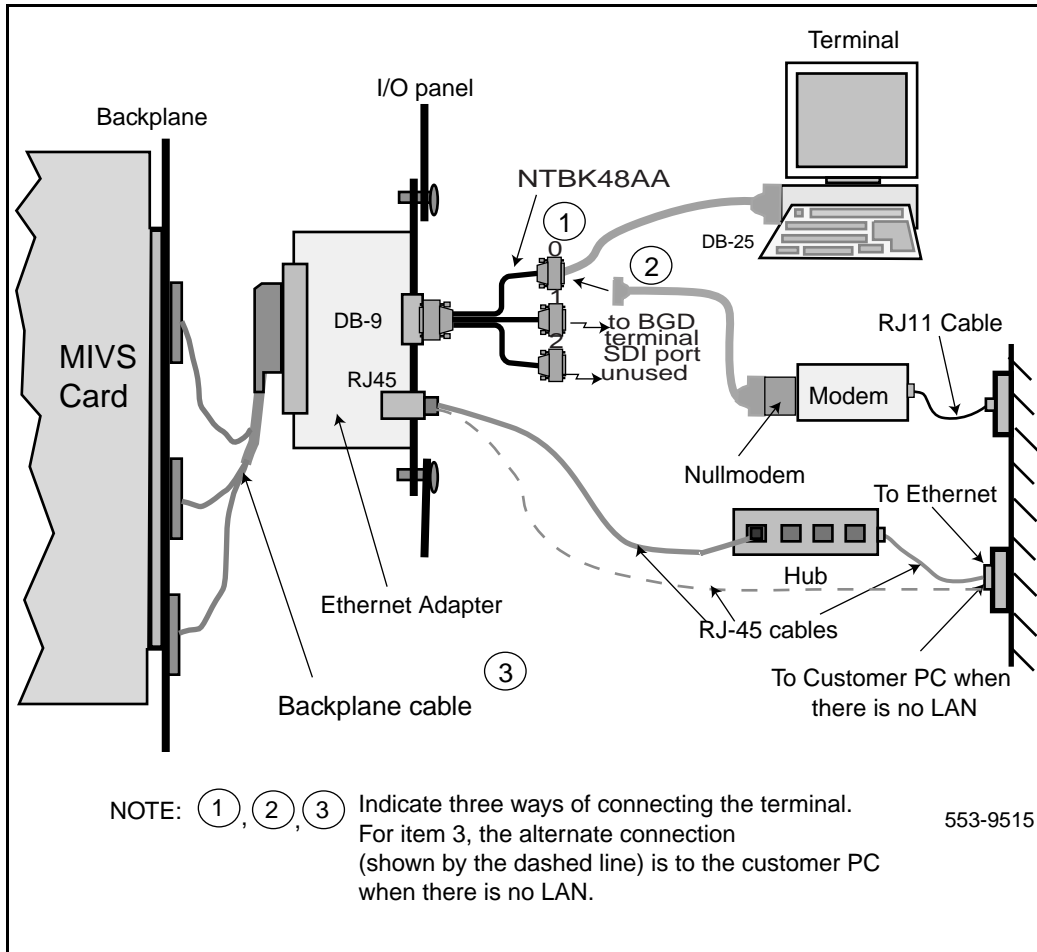
Connect the maintenance terminal

You can connect the MIVS maintenance terminal locally using a direct cable connection or remotely using a modem connection. The maintenance terminal provides access to the CLI on the MIVS card. You can connect the terminal to the MIVS as a:

- Local connection through Port 0 of the NTBK48AA cable using a terminal cable

- Remote connection through Port 0 of the NTBK48AA cable using a cable and a modem for remote access

- Remote, multi-terminal access through the Ethernet adapter's RJ-45 jack and a RJ-45 modular cable to a LAN hub

Set up the modem connection to the Ethernet adapter

To connect a modem (including a null modem) to the NT5D52AA Ethernet adapter, you require an RJ11 cable and a 9-pin to DB25 cable. Refer to Figure 6 on page 46. Refer to Table 19 on page 48 for a description of the NT5D52AA Ethernet adapter pins.

Use the following procedure:

1 Connect the cable between Port 0 of the NTBK48AA cable from the Ethernet adapter, and the modem. Use a null modem if required.

2 Connect the modem to a phone plug.

3 Connect RJ11 cable from the modem to the Ethernet port.

Table 19
NT5D52AA Ethernet adapter pins

	Pin Number	Signal Description
9-pin serial connector	2	RS232 Tx (Transmit)
	3	RS232 Rx (Receive)
	5	GND (Ground)
RJ45 Ethernet connector	1	LAN_Tx+
	2	LAN_Tx -
	3	LAN_Rx+
	6	LAN_Rx -

Local terminal connection through the NTBK48AA cable

To connect a local maintenance terminal through the NTBK48AA cable, connect Port 0 of the NTBK48AA cable to the terminal using a direct cable (see Figure 6 on page 46 for the connection illustration).

1   Position the terminal on a desk near the system.

2   Check the installation of the Ethernet adapter on the I/O panel (see "Install the Ethernet adapter" on page 41).

3   Check the installation of the NTBK48AA cable to the DB-9 male connector on the Ethernet adapter.

4   Plug the terminal cable 25-pin female connector into the 25-pin male connector (labeled **Port 0**) of the NTBK48AA cable.

5   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 null modem is necessary). If the connection requires a gender changer, you can obtain one at your local electronics store. (See "Configure the maintenance terminal" on page 54 for further information.)

Remote maintenance terminal connection using a modem

You can connect a remote maintenance terminal by connecting the NTBK48AA cable to a modem (see Figure 6 on page 46 for the connection illustration).

1   Check the installation of the Ethernet adapter on the I/O panel (see "Install the Ethernet adapter" on page 41).

2   Check the installation of the NTBK48AA cable to the DB-9 male connector on the Ethernet adapter.

3   Plug the terminal cable 25-pin female connector into the 25-pin male connector (labeled **Port 0**) of the NTBK48AA cable.

4   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 null modem adapter.

5   Plug the DB-25 male connector of the null modem adapter into the DB-25 female connector on the modem.

6   Plug the modular modem cable RJ-11 plug into the RJ-11 jack on the modem.

7   Plug the other end of the modular modem cable RJ-11 plug into the RJ-11 jack on the wall, for PSTN access.

Remote multi-terminal connection through the LAN

You can access the MIVS card from multiple terminals through telnet over the LAN. See Figure 6 on page 46 and refer to "Connect the Ethernet adapter to the LAN" on page 44 for instructions.

Note: You cannot access the MIVS card in this way until you first configure the LAN parameters for the MIVS card. See "Set the LAN parameters in the CLI" on page 55. Initial setup of the MIVS card, including setting the LAN parameters, requires a serial terminal connection to the MIVS card.

Figure 7 provides an example of an MIVS Telnet login screen session.

Figure 7
MIVS Telnet session login screen example

```
Dongle:

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

login: user

previous user login: June 12, 2000 16:44

SAdmin/, SMaint/, PAdmin/, PMaint/, AAdmin/, ADebug/, MIVS/, LOgout,?: MIVS

SAdmin/, SMaint/, PAdmin/, PMaint/, LOgout, ?: sa

SYstem, ?: sy

System Attributes:
card name: Alpha
agent id: not defined (see Note 1 below)
subnet mask: 255.255.240.0
gateway address: 47.82.32.1
I.P. address: 47.82.46.92
Modify, Save, Cancel:
```

> *Note 1:* "not defined" is the value for the "agent id" field, if the "Agent ID Not Defined" prompt (AID) is set to NO (the default) in LD 23.

> *Note 2:* For the "agent id" field, an entry is required if the site has configured an ACD ID in overlay LD 23. To get this value, print an ACD management report as follows:

Prompt	Response	Description
REQ	PRT	Print ACD data.
TYPE	SCB	Schedule Control data block.
AID	YES	Agent ID mode.
- IDLB	(1)-9999	Agent ID Lower Boundary
- IDUB	*IDLB*-(9999)	Agent ID Upper Boundary
...		

Note 3: Ensure that the Agent IDs used for MIVS:

— fall between the lower and upper boundaries, as printed in the IDLB and IDUB fields illustrated above.

— are not used by other ACD agents.

— are consecutive, for example, 0-7.

Note 4: The number entered for the Agent ID, if needed, must be the Agent ID assigned to port 0 of the MIVS card.

Connect the BGD terminal

MIVS uses the BGD terminal to make requests to the Meridian 1 for AWU and DND services. To connect the BGD terminal to the MIVS card and the Meridian 1, do the following:

1   Position the terminal on a desk near the system.

2   Check the installation of the Ethernet adapter on the I/O panel (see "Install the Ethernet adapter" on page 41).

3   Check the installation of the NTBK48AA cable to the DB-9 male connector on the Ethernet adapter.

4   Plug the terminal cable 25-pin female connector into the 25-pin male connector (labeled **Port 1**) of the NTBK48AA cable (see Figure 5 on page 43). Port 1 connects to the SDI that is configured as the BGD terminal.

   Note: You need a null modem to make the connection, if you have a DTE connection (see Table 20 on page 52 for the connector pinout).

5   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 null modem is necessary). If the connection requires a gender changer, you can obtain one at your local electronics store. (See "Enter the keycode information" on page 54 for further information.)

Table 20
Connector pinout for the NT8K48AA

Adapter Pin No.	Pin Name	Pin Number	Port Number
3	RX RS-232 (CRT)	2	0
2	TX RS-232 (CRT)	3	0
5	GND RS-232 (CRT)	7	0
7	RX SCC3 (BGT)	2	1
6	TX SCC3 (BGT)	3	1
5	GND SCC3 (BGT)	7	1
9	RX SCC4 (optional)	2	2
8	TX SCC4 (optional	3	2
5	GND SCC4 (optional)		

MIVS configuration

Before you can begin MIVS operation, you must perform the following configuration procedures:

- Configure the BGD terminal

- Configure the maintenance terminal for CLI access

- Enter the keycode information

- Set the LAN parameters in the CLI

- Configure the MIVS operating parameters in the BUI

Configure the BGD terminal

To configure the BGD terminal for MIVS operation, do the following:

1   Ensure that you configured the BGD terminal in the X11 system software, as described in "Define the BGD terminal port" on page 30.

2   Define the interface parameters of the BGD I/O card as follows:

- Transmission speed: 9600 bps
- Data bits: 8
- Stop bit: 1
- Parity: No
- Flow control: No

Note: You must configure the BDG terminal SDI port as DTE.

3   Set the BGD terminal parameters. Refer to Table 21.

Note: The SET OPTION CONFIRM is set to OFF by default. It is changed to ON because the MIVS uses the information sent back from the BGD SDI port.

4   Put the terminal in LOGOUT mode.

Table 21
BGD terminal parameters

Parameter	Description
SET OPTION CONFIRM ON	The default is set to OFF, so you have to change the setting to ON.
SET OPTION PORT xx SET ON	**xx** is the device number, from 0–15, that you defined at ADAN in LD 17.
SET OPTION PORT xx DISPLAY OFF	**xx** is the same device number as above, from 0–15.
SET OPTION LANGUAGE xx OFF	**x** is the language number, from 0–5. Do this for each language.

Configure the maintenance terminal

To access the CLI, you must use a VT100-type terminal. See "Connect the maintenance terminal" on page 47 for instructions on connecting the VT100 terminal to the MIVS. Specify the VT100-type terminal interface characteristics to ensure compatibility with the MIVS 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 X-On/X-Off flow control.

Enter the keycode information

When you first connect a VT100 terminal to your MIVS 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 MIVS keycode (e.g., 8).

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

4   At the keycode prompts, enter **keycode1**, **keycode2**, and **keycode3** (eight characters each) for MIVS functionality.

If the keycode entry is successful, the CLI notifies you, a login prompt appears. You can now enter the LAN parameters for your MIVS.

Set the LAN parameters in the CLI

If you cannot connect the MIVS to the customer's LAN, you need to make a direct connection between the PC and the MIVS Ethernet adapter to load the Browser User Interface (BUI) screens. You use a standard cross-over RJ45 Ethernet cable and follow the instructions below:

1   Obtain PC IP address. To find the PC Ethernet address:

    a   Go to the Control Panel.

    b   Double-click on the Network icon.

    c   Highlight the TCP/IP and Ethernet adapter enter.

    d   Select Properties. The IP address tab shows the Ethernet address and submask.

    Note: Changing the PC Ethernet address requires a reboot.

2   Define the MIVS IP address "close" (sequenced) to the PC IP address. For example, if the PC IP address is 100.99.98.97, define the MIVS IP address as 100.99.98.96, or 100.99.98.98.

3   Define the MIVS subnet mask the same as the PC subnet mask.

4   Do not define a gateway.

    Note: Check the connection using the PC/UNIX ping command (ping<IP-address>).

To enter the LAN parameters for an MIVS card that you can connect to the customer network, do the following:

1   Once the system successfully registers the MIVS keycode, log into the CLI as **root user directory**.

2   At the **root user directory** prompt, enter **mivs** to access the MIVS directory.

3   At the **SAdmin, SMaint, PAdmin, PMaint, LOgout, ?:** prompt, enter **sa** to access **System Administration**.

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

5   Enter the system attributes of the MIVS card, including the IP address, gateway, and subnet mask. See "CLI System Administration menu" on page 78 for details.

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

7   At the Restart MIVS? prompt, enter Yes.

   Note: This step may take a few minutes.

8   From a PC terminal, "ping" the MIVS card to ensure that it has a proper connection to the LAN. To ping an MIVS card, do the following:

   a   Click **Start** and select **Run**.

   b   In the **Open:** field, enter **ping <IP address>**, where <IP address> is the IP address of the MIVS card.

   c   Click **OK** and observe the DOS window that opens.

   If you receive the *Reply from <IP address>...* message, you have set up the LAN connection properly and you can proceed. If you receive the *Request timed out.* message, there is a problem with the LAN connection.

9   You must define an agent ID here if you use agent IDs. Refer to the information contained in Note 2 on page 50.

Configure the MIVS administration parameters in the BUI

The final procedure that you must perform to enable MIVS operation is the configuration of the administration parameters in the BUI. To configure the MIVS administration parameters, do the following:

   Note: MIVS only permits one person at a time to log into the BUI.

1   Open the Web browser on your PC. For minimum browser versions, see "Web browser characteristics" on page 23.

2   In the URL field of the Web browser, enter the following:
   http://<MIVS card IP address>/mivs_bui.htm

3   Press **Enter**. The **MIVS BUI login** window appears (see Figure 8).

4   In the **MIVS BUI login** window, enter the User Name (default = **admin**) and the Password (default = **000000** [six zeros]), and press **Enter**.

5   In the **MIVS BUI Administration Parameters** window (see Figure 9), enter the phone number for Automatic Wake Up service in the appropriate field (this is **7001** from Table 16 on page 38).

6   Enter the phone number for Do Not Disturb service (this is **7002** from Table 16 on page 38).

Figure 8
MIVS BUI login window

7   Enter the staff phone number (this is **7003** from Table 16 on page 38).

8   Define the TUI password for staff access to the MIVS (enter from one to nine digits).

9   Select the language for staff access (**English** is the default).

10   **Optional**: Enter the phone number for guest access to a special menu. (This is the phone number that MIVS transfers a guest to automatically after the guest orders AWU or DND service.) The default setting is **NONE** and should appear when no other DN has been defined.

11   From the pull-down menu, select the number of service failures that can occur before the MIVS transfers the guest to an attendant.

Figure 9
MIVS BUI Administration Parameters window
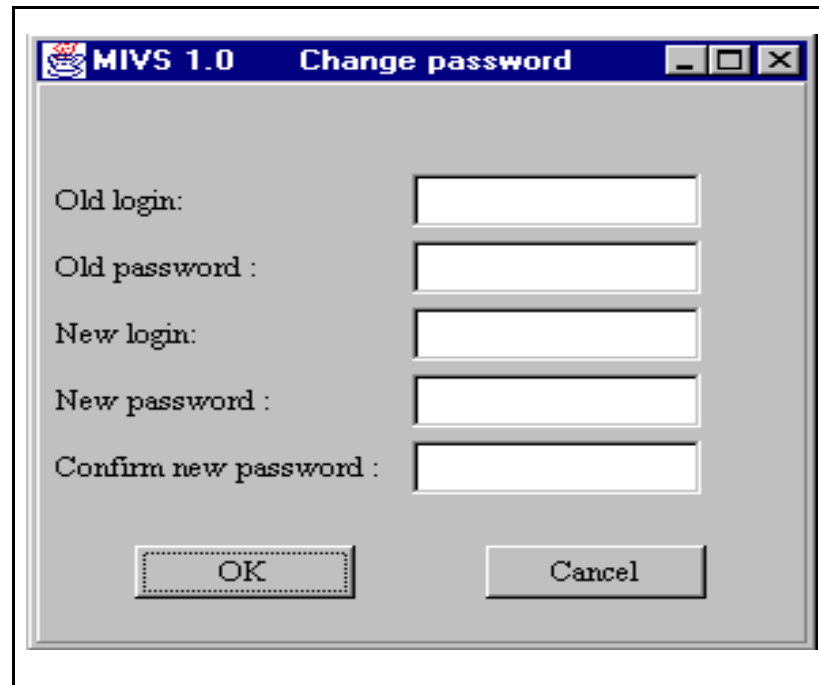
12 Enter the attendant phone number that MIVS must transfer a guest to when a guest presses **0** or experiences the predetermined number of service failures. You can enter LDN if ICI keys are defined or direct access to attendant.

13 Click **Apply** to save the administration parameters.

14 Click **Exit** to exit the BUI.

Change user name (login) and password for BUI access

The default user name (login) is **admin** and the default password is **000000** (six zeros). You can change these parameters after you enter the BUI. To change the user name and password for BUI access, do the following:

1   Click **Change name and password** at the top of the **MIVS BUI Administration Parameters** window. The **MIVS BUI Change password** window appears (see Figure 10).

Figure 10
MIVS BUI Change password window

2   Enter the **old user name** (**login**) and **old password** in the appropriate fields.

3   Enter the **new user name** (**login**) and **new password** in the appropriate fields. (The user name [login] can be up to six alphanumeric characters in length. The password can be from one to seven alphanumeric characters in length.)

4   Enter the **new password** (**login**) again to confirm it.

5   Click **OK** to close the **MIVS BUI Change password** window and save the new user name and password. (Click **Cancel** to close the **MIVS BUI Change password** window without changing the user name [login] and password.)

Note: There is no limit to how often you can change the user name (login) and password.

Language configuration

Follow the procedures in this section to configure the MIVS language settings.

1   Click **Configure Languages** from the **MIVS BUI Administration Parameters** window. The **MIVS BUI Language Configuration** window appears (see Figure 11).

2   Choose a language from the pull-down menu. The menu lists six languages. (**English** is the default.)

3   Click the radio button next to the number or character field in the same row as the language to indicate which method Meridian 1 uses to designate the language.

4   If you use a number to indicate language designation (default), choose a number from 0–5 from the pull-down menu.

5   If the administrator selects the character field, assign a character string for Meridian 1 to designate a language.

Figure 11
MIVS BUI Language Configuration window
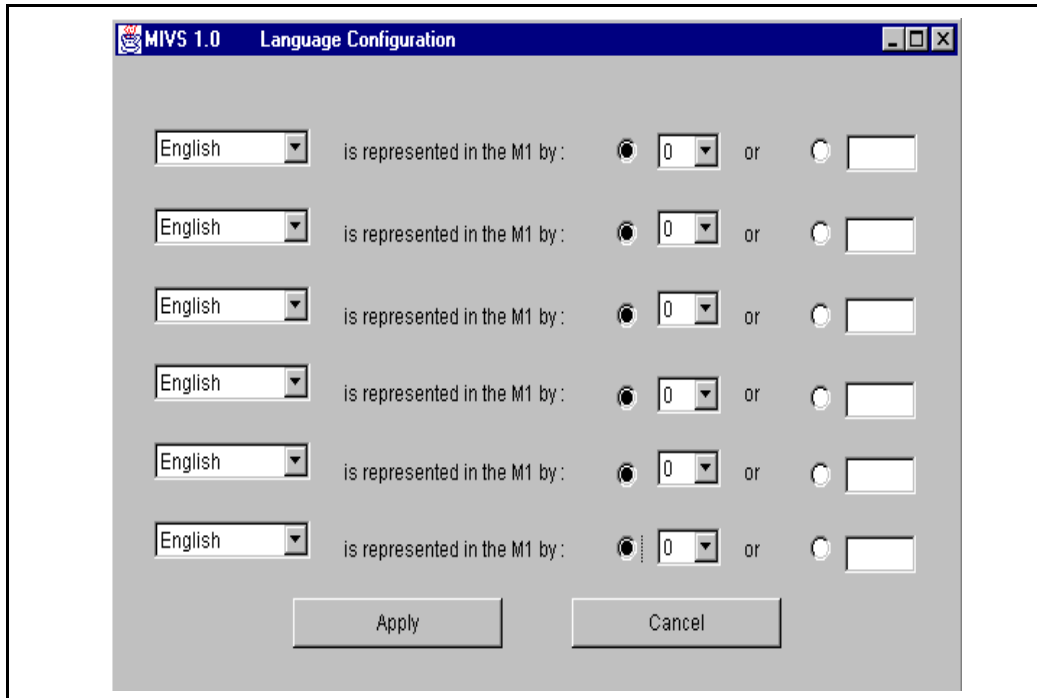
MIVS operation

This chapter describes the operation of MIVS. MIVS enables a guest to perform the following functions:

- Order, modify, or cancel AWU service

- Order or cancel DND service

MIVS enables the staff to perform the following functions:

- Order, modify, or cancel AWU service for a guest

- Order or cancel DND service for a guest

- Customize the greetings that guests hear when they dial into MIVS

The guests and staff perform each of these functions through a TUI. They access the TUI by dialing the appropriate DN, which you defined in "X11 system software configuration" on page 30 and "MIVS configuration" on page 52. Make sure the guests and staff are aware of the appropriate DNs to dial. The staff must also know the password for staff access.

The following sections provide the high-level procedure for performing each of these functions. The TUI menus are easy to follow and do not require special training. The procedures are provided here for reference. In the following sections, the TUI response appears in *italics* after each guest or staff action.

> *Note:* Guests can press **0** at any time to transfer to an operator/attendant.

Automatic Wake Up (AWU)

To order, modify, or cancel AWU service, a guest must dial the AWU service DN from his room.

To order AWU service

To order AWU service, the guest performs the following steps:

1   The guest dials the AWU access DN from his room.

Hello, you have reached the Automatic Wake Up service. (The staff can modify this greeting. See "To customize the greetings" on page 68.)

Please enter your wake up time. When done, press the number sign.

2   The guest enters the time on the telephone keypad. (The time entry can be three or four digits. MIVS requests whether the time is a.m. or p.m., if necessary. MIVS recognizes time requests according to both 12-hour clocks and 24-hour clocks.)

For a.m., press **1***. For p.m., press* **2***.* (This prompt occurs only if necessary.)

3   The guest presses **1** for a.m. or **2** for p.m., if necessary.

Your requested wake up time is today (tomorrow) at 'HH:MM'.

To approve, press **1***. To change the time, press* **2***. To hear the time again, press* **3***.*

4   The guest presses **1** to approve the request.

Your wake up request has been accepted. (MIVS then disconnects the call or transfers the guest to the special services DN.)

To modify AWU service

To modify AWU service, the guest performs the following steps:

1   The guest dials the AWU access DN from his room.

Hello, you have reached the Automatic Wake Up service.

Your wake up request is for today (tomorrow) at 'HH:MM'*.*

*To cancel your wake up request, press **1**. To change the time, press **2**. To exit, press **3**.*

2   The guest presses **2** to modify the wake up time.

Please enter your wake up time. When done, press the number sign.

3   The guest enters the time on the telephone keypad.

*For a.m., press **1**. For p.m., press **2**.* (This prompt occurs only if necessary.)

4   The guest presses **1** for a.m. or **2** for p.m., if necessary.

Your requested wake up time is today (tomorrow) at 'HH:MM'.

*To approve, press **1**. To change the time, press **2**. To hear the time again, press **3**.*

5   The guest presses **1** to approve the request.

Your wake up request has been accepted. (MIVS then disconnects the call or transfers the guest to the special services DN.)

To cancel AWU service

To cancel AWU service, the guest performs the following steps:

1   The guest dials the AWU access DN from his room.

Hello, you have reached the Automatic Wake Up service.

Your wake up request is for today (tomorrow) at 'HH:MM'.

To cancel your wake up request, press **1**. *To change the time, press* **2**.
To exit, press **3**.

2   The guest presses **1** to cancel the wake up time.

*Your wake up request has been canceled. Thank you for using this
service.*

Do Not Disturb (DND)

To order or cancel DND service, a guest must dial the DND service DN from his room.

To order DND service

To order DND service, the guest performs the following steps:

1   The guest dials the DND access DN from his room.

Hello, you have reached the Do Not Disturb service. (The staff can modify this greeting. See "To customize the greetings" on page 68.

To activate Do Not Disturb now, press **1**.

2   The guest presses **1** on the telephone keypad.

Do Not Disturb has been activated.

Thank you for using this service. (MIVS then disconnects the call.)

To cancel DND service

To cancel DND service, the guest performs the following steps:

1   The guest dials the DND access DN from his room.

Hello, you have reached the Do Not Disturb service. (The staff can modify this greeting. See "To customize the greetings" on page 68.

Do Not Disturb is active for this room. To cancel now, press **1**. *To leave active, please hang up.*

2   The guest presses **1** on the telephone keypad.

Do Not Disturb has been cancelled.

Thank you for using this service. (MIVS then disconnects the call.)

Staff operation of MIVS

To customize the MIVS greetings or request AWU and DND services for a guest, the staff must dial the staff access DN from any Dual-Tone Multi-Frequency (DTMF) telephone within the Meridian 1.

To customize the greetings

WARNING

When you customize a greeting, MIVS writes over the original default greeting. If you must save the default greeting for possible future use, back up the MIVS software to a spare PCMCIA disk. Back up the MIVS software *before* you record the new greeting. Use the Archive Database command in the CLI (see "Archive Database" on page 82) to back up the MIVS software.

To customize either of the greetings that guests hear when they dial into MIVS, the staff performs the following steps:

1 The staff dials the staff access DN.

Please enter the password, followed by the number sign.

There is a single customized greeting for **all** languages.

2 The staff enters the password on the telephone keypad.

*To order Do Not Disturb, press **1**. To order Automatic Wake Up, press **2**. To customize your greeting, press **3**. To exit, press **4**.*

3 The staff presses **3**.

*To customize a Do Not Disturb greeting, press **1**. To customize an Automatic Wake Up greeting, press **2**. To exit without changing, press **3**.*

4 The staff presses **1** to customize the DND greeting or **2** to customize the AWU greeting.

The current customized greeting is...(MIVS then plays either the DND or the AWU greeting, whichever is appropriate.)

After the tone, please record your customized greeting up to a maximum of 15 seconds, followed by the number sign. (A tone beeps.)

---

5   The staff speaks the new greeting into the telephone handset, then presses **#** to finish the recording.

The recorded greeting is...(MIVS plays the new greeting)

*To accept, press **1**. To listen again, press **2**. To re-record, press **3**. To exit without changing the greeting, press **4**.*

6   The staff presses **1** to approve the new greeting.

*To order Do Not Disturb, press **1**. To order Automatic Wake Up, press **2**. To customize your greeting, press **3**. To exit, press **4**.*

7   The staff presses **4** to exit. (MIVS disconnects the call.)

To handle AWU service for a guest

To handle AWU service for a guest, the staff performs the following steps:

1   The staff dials the staff access DN.

Please enter the password, followed by the number sign.

2   The staff enters the password on the telephone keypad.

*To order Do Not Disturb, press **1**. To order Wake Up, press **2**.*
*To customize your greeting, press **3**. To exit, press **4**.*

3   The staff presses **2**.

Please enter the room's phone number, followed by the number sign.

4   The staff enters the guest's room phone number, followed by the number sign.

MIVS checks the room's status for AWU. The staff then orders, modifies, or cancels AWU for the guest the same way a guest does. See "Automatic Wake Up (AWU)" on page 64.

To handle DND service for a guest

To handle DND service for a guest, the staff performs the following steps:

1   The staff dials the staff access DN.

Please enter the password, followed by the number sign.

2   The staff enters the password on the telephone keypad.

*To order Do Not Disturb, press **1**. To order Automatic Wake Up, press **2**. To customize your greeting, press **3**. To exit, press **4**.*

3   The staff presses **1**.

Please enter the room's phone number, followed by the number sign.

4   The staff enters the guest's room phone number, followed by the number sign.

MIVS checks the room's status for DND. The staff then orders or cancels DND for the guest the same way a guest does. See "Do Not Disturb (DND)" on page 67.

MIVS administration

You perform administration tasks the Command Line Interface (CLI) and the Browser User Interface (BUI). This chapter describes the CLI. "Configure the MIVS administration parameters in the BUI" on page 56 describes the BUI.

Introduction to the CLI

The MIVS CLI enables an administrator to perform various system administrative functions, including upgrades. You can access the CLI through a VT100-type terminal or a PC running a terminal emulation program. The terminal can connect directly to the RS-232 port on the MIVS card. You can also access the CLI over the Ethernet through a hub that connects to the RJ-45 port on the MIVS card. The following system administration functions are accessible through the CLI:

- Keycode entry

- LAN parameter definition for the MIVS card

- MIVS card restarts

- CLI password control

- BUI password reset and screen lock

- MIVS functional and software upgrades

Before you can access the CLI, you must configure the terminal interface parameters, as described in "Configure the maintenance terminal" on page 54.

Log into the CLI

To log into the CLI, enter the password at the **Login:** prompt. The default
password is **user**, which you can change after you log in. You use the CLI to
perform the following functions:

- **System administration**, which includes defining the card name, setting
  the LAN parameters, and defining agent IDs

- **System maintenance**, which includes archiving and restoring the
  database, and restarting the card

- **Protected administration**, which includes editing and resetting
  passwords, upgrading and modifying software functionality, and locking
  the BUI screens

- **Port maintenance**, which allows you to display the status of the ports

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

```
Login: rst
Enter keycode1 (8 characters): 12345678
Enter keycode2 (8 characters): 81234567
Enter keycode3 (8 characters): 78123456
Passwords have been reset.

Login: user
```

You can then assign a new password by accessing the **CLI Protected
Administration** menu.

General administration procedures

General administration procedures are rules you must follow when you modify default or existing parameters. These apply when you use:

- General administration commands
- Object modify procedure
- Collection modify 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 re-displays the **Modify, Save,** or **Cancel:** command line for additional modification of parameters, if necessary.

To navigate between menus or to display **Help**, use the following terminal keys:

- The asterisk (*****) key returns you to the previous menu.
- The backslash (**/**) key returns you to the top-level menu.
- The **Help** (**?**) key 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 can respond in three ways:

- Enter **<cr>** to accept the current value.

- Enter **value** to change the attribute.

- Enter a dot (**.**) to terminate the session.

In some cases, the system displays the current value and a list of available values to select (where the value of **attribute_c** has been changed to **bbbb**); for example:

```
attribute_c (current_c, (1-aaaa, 2-bbbb, 3-cccc)): 2
```

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** – Used to modify the item in the list using object modify procedure

- **d** – Used to delete a selected item in the list

- **i** – Used to insert a list of items above the currently selected item

- **a** – Used 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 **.** (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.

CLI Main Menu

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

```
SAdmin, SMaint, PAdmin, PMaint, AAdmin, ADebug, MIVS, LOgout, ?:
```

To access one of the menus, enter the first two letters of the menu, and press **Enter**. For example, to access the **System Administration** menu, enter **sa**, **SA**, or the long form of the command (**SAdmin**). Enter **lo** or **LO** to log out.

Figure 12 illustrates the submenus for the CLI Main Menu. After you log in, you can access the various submenus; however, you must follow the general administration procedures.

Figure 12
CLI MIVS submenus
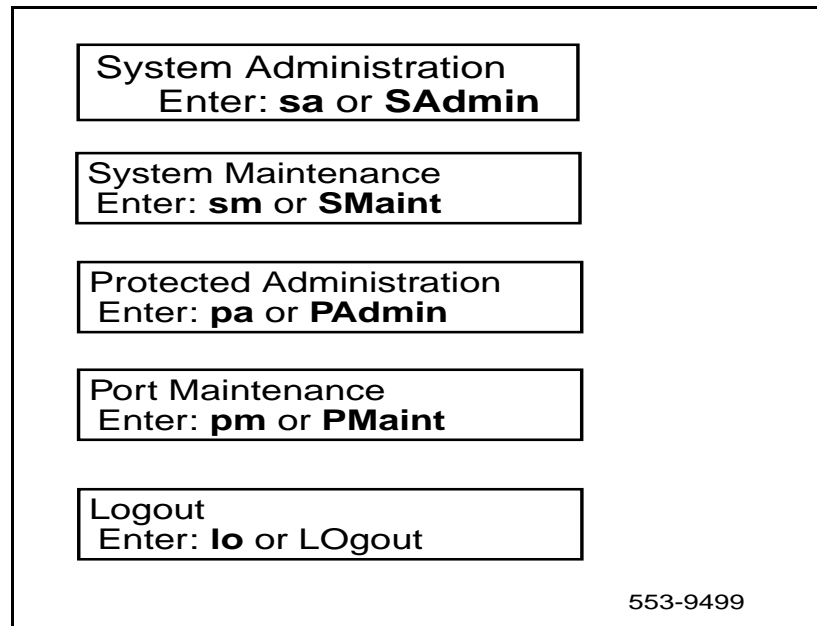
Help display

When you select the **Help** (**?**), the system lists the commands that relate to the **CLI Main Menu** (see Table 22).

Table 22
Help display—system commands

Short Command	Full Command	Description
sa or **SA**	**SAdmin**	System Administration directory
sm or **SM**	**SMaint**	System Maintenance directory
pa or **PA**	**PAdmin**	Protected Administration directory
pm or **PM**	**PMaint**	Port Maintenance directory
lo or **LO**	**LOgout**	Log out

CLI System Administration menu

To access the **CLI System Administration** menu from the **CLI Main Menu**, enter **sa**, **SA**, or the full command (**SAdmin**). Figure 13 illustrates the **CLI System Administration** menu and all the accessible submenus.

Figure 13
CLI System Administration menu
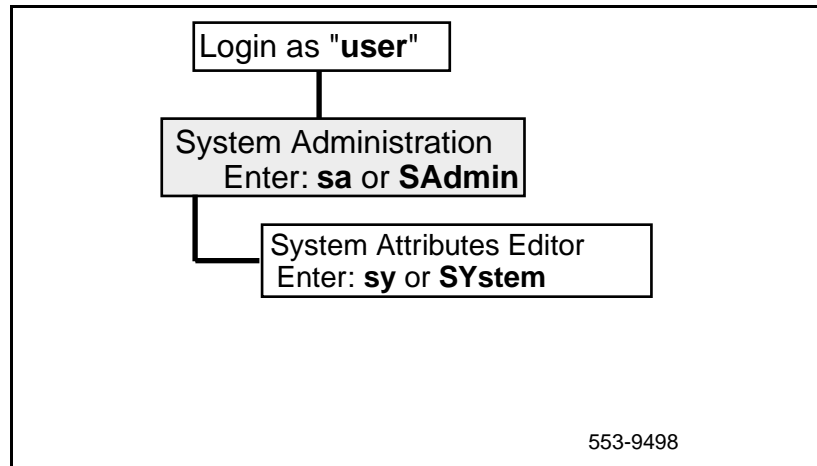
System Attributes Editor

Use this menu to modify system attributes as follows:

- **Card name** – A character string with maximum length of 10 characters. The name appears at the top of the **MIVS BUI Login** window, if you specify one.

- **Agent ID** – Default = not defined. If necessary, enter the same information defined in the X11 software.

- **Subnet mask** – Has **XXX.XXX.XXX.XXX** format, where every **XXX** is in the range 0–255. The subnet mask in binary presentation of 32 bits has at least the first eight 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; has the same format as the gateway address.

Example:

login: user
Previous user login: Feb 11, 1997 10:00
SAdmin, SMaint, PAdmin, PMaint, LOgout, ?: **sa**
SYstem, ?: **sy**
System Attributes:
card name:
agent id: not defined
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**
agent id: not defined
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
    agent id: not defined
    subnet mask: 255.255.248.0
    gateway address: 141.226.199.254
    IP address:141.226.199.50
    Modify, **S**ave, **C**ancel: **s**

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

By entering **lo**, **LO**, or **LOgout**, this concludes the System Attributes Editor session, returns you to the **CLI Main Menu**, and logs you out.

Help display

When you select the **Help** (**?**) command, the system displays the **System Attributes Editor** command (see Table 23).

**Table 23**
Help display—system Attributes Editor command

Short Command	Full Command	Description
sy or **SY**	SYstem	System Attributes Editor. Edit: card name, subnet mask, gateway address, and IP address.

CLI System Maintenance menu

To access the **CLI System Maintenance** menu from the **CLI Main Menu**, enter **sm**, **SM**, or the full command (**SMaint**). Figure 14 shows the **CLI System Maintenance** menu structure.

Figure 14
CLI System Maintenance menu

```
┌──────────────────────────────────────────────────────────────┐
│              ┌────────────────────────────┐                   │
│              │  Login as "user"           │                   │
│              └────────────┬───────────────┘                   │
│              ┌────────────┴───────────────┐                   │
│              │ System Maintenance         │                   │
│              │  Enter: sm or SMaint       │                   │
│              └──┬─────────────────────────┘                   │
│                 │   ┌───────────────────────────────┐         │
│                 ├───│ Database Archive              │         │
│                 │   │  Enter: ar or ARchivdb        │         │
│                 │   └───────────────────────────────┘         │
│                 │   ┌───────────────────────────────┐         │
│                 ├───│ Database Restore              │         │
│                 │   │  Enter: re or REstordb        │         │
│                 │   └───────────────────────────────┘         │
│                 │   ┌───────────────────────────────┐         │
│                 └───│ Card Restart                  │         │
│                     │  Enter: cr or CRestart        │         │
│                     └───────────────────────────────┘         │
│                                              553-9500          │
└──────────────────────────────────────────────────────────────┘
```
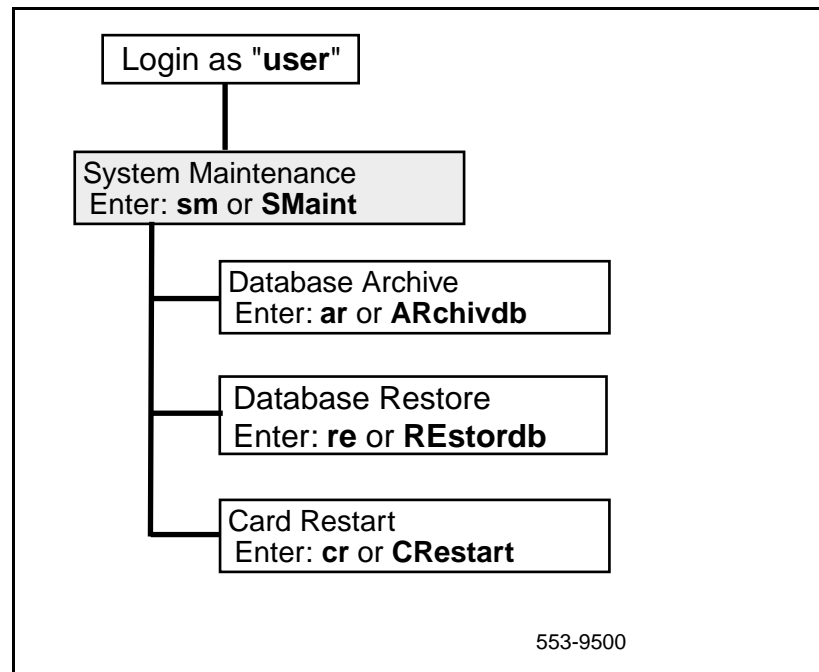
Archive Database

You must disable the MIVS in Overlay 32 before you archive the database. The **Archive Database** (**ARchivdb**) command enables you to back up the MIVS voice and data files, not firmware, BUI, or screens. Archive overwrites files on disk. 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 slot (drive B:). The DB Description file specifies the names of the files that Archive Database backs up. These files include configuration databases, as well as voice files.

> *Note:* Nortel Networks recommends that you archive the database to a backup disk, particularly if you plan to customize the AWU and DND service greetings. Customization of the greetings removes the original default greetings from the database.

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 database information, an error message appears.

Example:

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

Restore Database

Disable the MIVS using Overlay 32 before you restore the database. The **Restore Database** (**REstordb**) command 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:). The DB Description file lists the names of the files that Restore Database restores.

Example:

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

Card Restart

The **Card Restart** (**CRestart**) command restarts the MIVS card, which initiates a software reload.

Example:

```
ARchivdb, REstordb, CRestart, ?: cr
Restart MIVS card? (Yes, (No)) yes
```

This action returns the MIVS card to the initial screen and you must log in again.

Help display

When you select the **Help** (**?**) command, the system displays the **S**ystem Maintenance commands (see Table 24).

Table 24
Help display—system maintenance commands

Short Command	Full Command	Description
ar or **AR**	**ARchivdb**	Backs up customer database
re or **RE**	**REstordb**	Restores customer database
cr or **CR**	**CRestart**	Resets MIVS card

CLI Protected Administration menu

To access the **CLI Protected Administration** menu from the **CLI Main Menu**, enter **pa**, **PA**, or the full command (**PAdmin**). Figure 15 shows the **CLI Protected Administration** menu, which provides password administration, and port and software upgrade administration.

Figure 15
CLI Protected Administration menu

```
┌─────────────────────────────────────────────────────────────┐
│                                                              │
│           ┌──────────────────────────────┐                   │
│           │   Login as "user"            │                   │
│           └──────────────┬───────────────┘                   │
│                          │                                   │
│        ┌─────────────────┴────────────┐                      │
│        │ Protected Administration      │                     │
│        │ Enter: pa or PAdmin           │                     │
│        └──┬───────────────────────────┘                      │
│           │                                                  │
│           │    ┌──────────────────────────────┐              │
│           ├────│ Password Editor              │              │
│           │    │ Enter: ps or PSweditor       │              │
│           │    └──────────────────────────────┘              │
│           │    ┌──────────────────────────────┐              │
│           ├────│ Functionality Upgrade        │              │
│           │    │ Enter: fu or FUpgrade        │              │
│           │    └──────────────────────────────┘              │
│           │    ┌──────────────────────────────┐              │
│           ├────│ Software Upgrade             │              │
│           │    │ Enter: sw or SWupgrade       │              │
│           │    └──────────────────────────────┘              │
│           │    ┌──────────────────────────────┐              │
│           ├────│ Administrator BUI            │              │
│           │    │ Reset Password               │              │
│           │    │ Enter: ab or ABreset         │              │
│           │    └──────────────────────────────┘              │
│           │    ┌──────────────────────────────┐              │
│           └────│ Screening Table lock/unlock  │              │
│                │ Enter: scr or SCReen         │              │
│                └──────────────────────────────┘              │
│                                                              │
│                                         553-9502             │
└─────────────────────────────────────────────────────────────┘
```
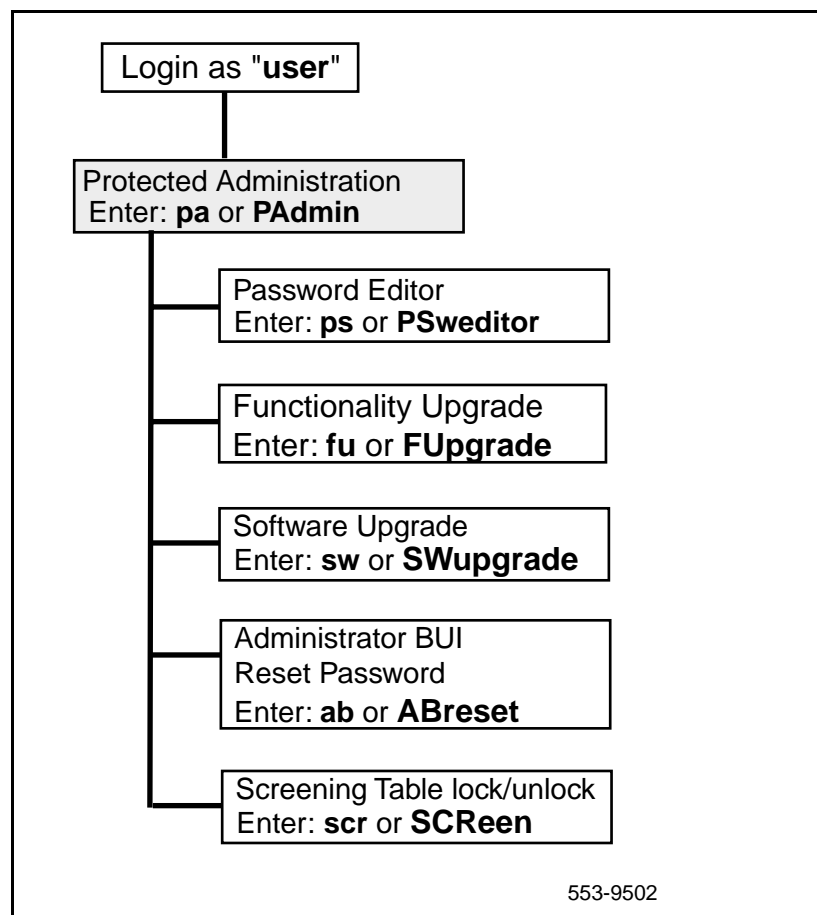
Password Editor

To change the CLI password, log into the CLI and access the **Password Editor** menu from the **CLI 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, ABreset, ?: ps
Current Passwords:
admin: user
Modify, Save, Cancel: m
admin (user): administrator
New passwords:
admin: administrator
Modify, Save, Cancel: Save
Passwords have been updated.
PSweditor, FUpgrade, SWupgrade, ABreset, ?:
```

Functionality Upgrade

The **Functionality Upgrade** (**FUpgrade**) command enables you to change the number of available ports/channels on the MIVS card. To activate a change to the number of ports/channels, you must enter a new keycode, which the system compares to the one in the MIVS memory. After keycode authentication, the CLI displays the current number of MIVS ports/channels.

The CLI allows you three attempts to enter the correct keycode. If you fail to enter the correct keycode, the changes you made do not take effect. If MIVS authenticates the keycode, MIVS stores the changes you made in the memory. The changes take effect, allowing you to use the new number of MIVS ports.

Enter the keycode using three prompts: **keycode1**, **keycode2**, and **keycode3**. Each requires the entry of eight digits.

Example:

This example expands the number of available MIVS ports from 4 to 8:

```
PSweditor, FUpgrade, SWupgrade, ABreset, ?: fu
max conf_ports: 4
Modify, Save, Cancel: m
max conf_ports (4): 8
Modify, Save, Cancel: Save
Enter keycode1: 12121234
Enter keycode2: 23232345
Enter keycode3: 32222385
Incorrect key-code
Modify, Save, Cancel: Save
Enter keycode1: 12112234
Enter keycode2: 12128934
Enter keycode3: 32222385
PSweditor, FUpgrade, SWupgrade, ABreset, ?:
```

Software Upgrade

Disable the MIVS using Overlay 32 before you restore the database. The
Software Upgrade (SWupgrade) command allows you to upgrade the Main
Processor Unit (MPU) and the Digital Signal Processor (DSP) software on an
active MIVS card. The new software resides on a PCMCIA flash card, which
you must install in drive B: on the MIVS card before you execute 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.
```

To upgrade the software, do the following:

1   Place the PCMCIA flash card into the top PCMCIA slot (drive B:) on
the MIVS. Ensure that the PCMCIA hard drive card is still in the lower
PCMCIA slot (drive A:).

2   Log into the CLI and proceed as the example below shows.

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

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

Administrator BUI Reset Password

The **Administrator BUI Reset Password** (**ABreset**) command enables you to reset the password for access to the BUI. The default password for the BUI is **000000** (six zeros).

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

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

Help display

When you select the **Help** (**?**) command, the system displays the **Protected Administration** commands (see Table 25)

Table 25
Help display—protected administration commands

Short Command	Full Command	Description
ps or **PS**	**PSweditor**	Password Editor
fu or **FU**	**FUpgrade**	Functionality Upgrade; allows or restricts capabilities secured by the keycode
sw or **SW**	**SWupgrade**	Software Upgrade; upgrades MPU and/or DSP software
abr or **ABR**	**ABreset**	Administrator BUI Reset Password

CLI Port Maintenance Menu

To access the **CLI Port Maintenance** menu from the **CLI Main Menu**, enter **pm**, **PM**, or the full command (**PMaint**). Figure 16 shows the **CLI Port Maintenance** menu and its command. The command displays the status of the MIVS ports.

Figure 16
CLI Port Maintenance menu
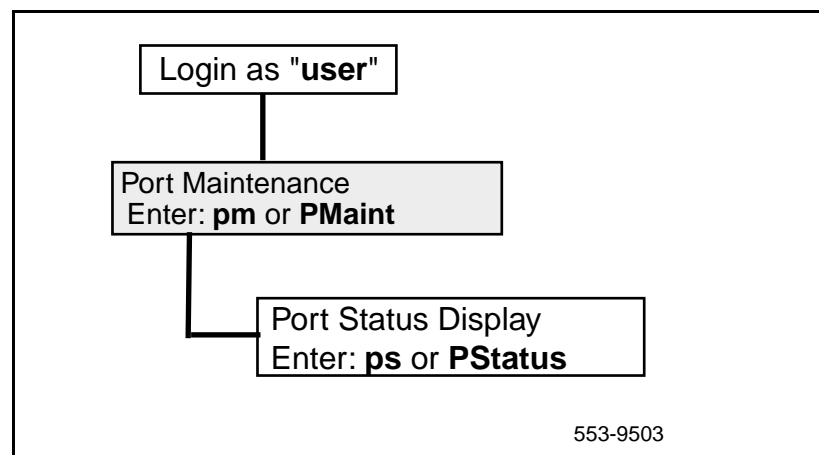
Port Status display

The **Port Status** (**PStatus**) command displays the status of all MIVS ports, regardless of their allocation. The possible status for any port is: **Idle**, **Dialing_out**, **Ringing**, **Talking**, or **Disable**.

Example:

PStatus, ?: **ps**

Table 26
Port Status information

Port_ID	Port_Status	Port_ID	Port_Status
0	DISABLE	4	IDLE
1	IDEL	5	TALKING
2	TALKING	6	RINGING (see Note)
3	RINGING (see Note)	7	TALKING
Note: Ringing is a very short event.			

PStatus, ?:

Help display

The following help information appears when you select the **Help** (**?**) command at the **Port Maintenance** level.

Table 27
Help display—port maintenance command

Short Command	Full Command	Description
ps or **PS**	**PStatus**	Displays status of all ports

MIVS maintenance

This chapter describes MIVS maintenance tools and procedures to guide you in:

- Identifying the MIVS faults

- Locating defective equipment

- Correcting problems by fixing or replacing defective equipment

- Verifying the operation of the MIVS after corrections or replacements have been made

MIVS maintenance overview

You must approach problem identification systematically. A problem can have more than one cause. To isolate the cause, a knowledge of MIVS 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 MIVS provide built-in self-diagnostic indicators and software and hardware tools. These diagnostic facilities simplify system troubleshooting and reduce the Mean Time To Repair (MTTR).

This document focuses on the maintenance of the MIVS equipment. It requires that the Meridian 1 operate correctly before you start diagnosing the MIVS problems. System installation and maintenance guide documents—*Meridian 1 general maintenance information* (553-3001-500), *Meridian 1 fault clearing* (553-3001-510), and *Meridian 1 hardware replacement* (553-3001-520)—describe how to maintain the entire system. This chapter describes how to maintain the MIVS as an integral part of the system.

Diagnostic tools

Use diagnostic tools to troubleshoot problems in the system, including problems with the MIVS. When diagnosing MIVS problems, you might need to use more than one of the following diagnostics tools:

- LED indicators

- Display codes

- Card self-tests

- Sanity monitoring

- Overlay commands

- History files

MIVS status LED indicator

The MIVS 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 MIVS card automatically performs a self-test when you insert it into an operating system module or when you power up or reset the system.

The self-test checks general MIVS 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 provides 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 MIVS card by checking the processor, the RAM capacity, the Flash memory, the DSP, and so on (see Table 28.)

Table 28
MIVS 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 Logic Cell Array (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 MIVS check configuration information.

Sanity monitoring

Sanity monitoring is a background routine that checks the operation of system resources, such as CPU activity, memory allocation, and so on. 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 Switch Management Processor (SMP) (when equipped). See the NTP titled *Meridian 1 system maintenance* (553-3001-520).

The MIVS card appears as an Extended Digital Line Card (XLDC) to the system in which it is installed. Therefore, you can use all relevant system maintenance commands for an XLDC with the MIVS. Enabling and disabling of the ACD digital telephone set M2616 is done in LD 32.

Table 29 lists some of the commands used to control the MIVS status and functions.

Table 29
Commands to enable/disable MIVS channels

LD 32 Commands	Operation performed
DISC/ENLC	Disables/Enables specified card
DISU/ENLU	Disables/Enables 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 MIVS

The MIVS card handles all the above commands exactly as the XLDC does, transparently to the system.

History file

Information on any fault conditions is stored on the MIVS card to provide a history file for the craftsperson. The file is in the form of a cyclical buffer containing up to 15 KB of error/log reports. User can access those files by using the **FTP** command (default user name is **user** and default password is **user)**. which is overwritten from the top when it runs out of space. It is configured to use memory resources efficiently.

MIVS keeps history files under the directory on the name **a:\oam** for up to 32 days. There are two kinds of history files:

a   Logger – History of actions like password change and other actions. MIVS stores Logger files under the a:\oam\log directory

b   Error Report for Debug – MIVS stores error reports in the **a:\oam\err** directory

Errors and logs are generated daily and kept in a separate file named **Eyyymmdd.err/Lyyyymmdd.lgr**, where:

yyy – year (e.g., 099 for 1999, 100 for 2000, etc.)

mm – month

dd – day

MIVS fault isolation and correction

Fault clearing procedures for the MIVS are the same as for other IPE cards; refer to *Meridian 1 fault clearing* (553-3001-510) for more information.

Table 30 deals specifically with MIVS 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 30
MIVS equipment problems

Symptoms	Diagnosis	Solution
Red card LED on the MIVS is permanently on.	Card is disabled or faulty.	Go to "MIVS self-test steps" on page 98 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 "MIVS self-test steps" on page 98 and "Reset MIVS card command" on page 99 to check self-test and self-test on reset. Also refer to *X11 input/output guide* (553-3001-400) for a list of codes.
Error messages printed on the terminal or the Meridian 1 TTY.	Hardware or software problems with the MIVS.	Note various error messages. Refer to *X11 input/output guide* (553-3001-400) 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.

MIVS 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 MIVS card waits until it receives the configuration data (trunk type, signaling type, balance impedance, and so on) via the DS-30X, but it then discards this data.

8   The card goes into its main program loop.

Reset MIVS 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 MIVS 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, and so on) via the DS-30X, but it then discards this data.

10   The card goes to its main program loop.

Respond to an "acquire failed" message

In some instances you may have a situation where your MIVS has more ports equipped than you are using. For example, you have purchased eight ports and only have enough available Agents in your ISM (Incremental Software Management) to support five additional agents. Another possibility is that you have planned expansion into your purchase of MIVS and you have equipped more ports than you currently need.

Each equipped port on the MIVS application attempts to log in when the card comes up. The "acquire failed" messages are indicating the application on MIVS is attempting to log in and communicate with the Meridian 1 ports. When ports are not assigned on the Meridian 1 you will receive the message.

To stop excessive generation of "acquire failed" messages on the MIVS use the procedure below:

> *Note 1:* If you reset the card you will have to perform this task after the reset.

1   At the CLI Main Menu: SAdmin/, SMaint/, PAdmin/, AAdmin/, ADebug/, MIVS/, LOgout, ?
         enter AA;

2   At the prompt - LOading/, MAnaging/, BAckup/?
         enter MA;

3   At the prompt - List, SHdow, TErmin, RUN,?
         enter TE 7; TE 6;TE 5;TE 4

> *Note:* Terminate only the number of applications equal to the unused ports. E.g. If you are only using 6 of eight ports only terminate two instances of the application TE 7 and TE 6.

Card replacement

The MIVS is based on PCMCIA technology. This allows you to remove the MIVS from the IPE shelf indefinitely without losing the configuration data.

To replace the MIVS card:

1   Disable the MIVS card by loading the LD 32 overlay and executing the **DISC l s c** command, where **l** is the loop, **s** is the shelf or module, **c** is the card in the module.

2   Remove the card from its card slot in the IPE module.

3   Remove the PCMCIA card from the faulty MIVS card.

4   Transfer the PCMCIA card to the new MIVS card.

5   This procedure moves all software, configuration, and records to the replacement MIVS card.

6   Transfer the Security Device from the faulty MIVS to the replacement.

Note: The new card re-uses the keycode. The keycode is still on the PCMCIA card, which you removed from the faulty MIVS.

7   Enable the new card by executing the **ENLC l s c** command.

8   Configure the newly installed MIVS card.

9   Package the faulty MIVS 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 "Archive Database" on page 82.

Appendix A: MIVS product integrity

This chapter presents information about:

- MIVS reliability

- Environmental specifications

- Electrical regulatory standards

Reliability

Reliability is measured by the Mean Time Between Failure (MTBF).

The MIVS card 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 Table 31.

Refer to Table 31 for a display of acceptable temperature and humidity ranges for the MIVS.

Table 31
MIVS environmental specifications

Specification	Minimum	Maximum
Normal Operation		
Recommended	15° C	30° C
Relative humidity	20%	30% (non-condensing)
Absolute	10° C	45° C
Relative humidity	20% to	80% (non-condensing)
Rate of change	Less than 1° C per three minutes	
Storage		
Long term	-20° C	60° C
Relative Humidity	5%	95% (non-condensing
	-40° C to 70° C, non-condensing	
Short term (less than 72 hrs.)	-40° C	70° C
Temperature Shock		
In three minutes	-40° C	25° C
In three minutes	70° C	25° C
	-40° to 70° C, non-condensing	

Electrical regulatory standards

The following three tables list the safety and ElectroMagnetic Compatibility (EMC) regulatory standards for the MIVS, listed by geographic region. Specifications for the MIVS meet or exceed the standards listed in these regulations.

Safety

Table 32 provides a list of safety regulations met by the MIVS, along with the type of regulation and the country/region covered by each regulation.

Table 32
Safety regulations

Regulation Identifier	
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)

ElectroMagnetic Compatibility (EMC)

Table 33 lists electro-magnetic emissions regulations met by the MIVS card, along with the country's standard that lists each regulation.

Table 33
ElectroMagnetic Emissions

Regulation Identifier	
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 standard)
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 34 lists ElectroMagnetic Immunity regulations met by the MIVS card, along with the country's standard that lists each regulation.

Table 34
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 3548I	EMC (Australia/New Zealand)
NFC 98020	France EMC standard

List of Terms

A03

    Three-Party Conference

ACD

    Automatic Call Distribution

AML

    Application Module Link

ATT

    attendant

AWU

    Automatic Wake Up

BGD

    Meridian 1 "Background Terminal" facility

BPS

    bits per second

BST

    busy tone

BUI

    Browser User Interface; an interface that enables the performance of various administrative functions over an intranet through a Web browser

CCOS

    Control Class of Service

CE

Common Equipment

CE-MUX

Common Equipment bus MUltipleXed

CISPR

Comité International Spécial des Perterbations Radioélectriques

CLI

Command Line Interface; an interface that an administrator can access either
through a serial terminal connection or through Telnet to perform various
administrative tasks

CLID

Calling Line IDentification

CSA

Canadian Standards Association

DID

Direct Inward Dialing

DLC

Digital Line Card

DN

Directory Number

DND

Do Not Disturb

DRAM

Dynamic Random-Access Memory

DSP

Digital Signal Processor

DTMF

Dual-Tone Multi-Frequency

EEPROM

Electrically Erasable Programmable Read-Only Memory

EMC

ElectroMagnetic Compatibility

ESD

Electro-Static Discharge

FCC

Federal Communications Commission

FFC

Flexible Feature Code

FTP

File Transfer Protocol

ICI

Incoming Call Indicator; an indicator on an attendant console that signals the type of incoming call

IDLB

Agent ID Lower Boundary.

IDUB

Agent ID Upper Boundary.

IEC

International Electro-Technical Commission; based in Geneva, Switzerland

I/O

input/output

IP

Internet Protocol

IPE

Intelligent Peripheral Equipment

ISM

Incremental Software Management

LAN

Local Area Network

LCA

Logic Cell Array

LDN

Listed Directory Number

LED

Light Emitting Diode

Mbps

Megabits per second

MB

Megabyte (1,048,576 bytes)

MDF

Main Distribution Frame

MHz

Megahertz

MIVS

Meridian Integrated Voice Services

MLWU

Multi-Language Wake-Up

MM

Meridian Mail

MPU

Main Processor Unit

MSB

Make Set Busy

MSPS

Miscellaneous/SDI/Peripheral Signaling

MTBF

Mean Time Between Failures

MTTR

Mean Time To Repair

NCFW

Night Call Forward

NFC

New Flexible Code

NRD

Not Ready

OA&M

Operation, Administration, and Maintenance

Option 11/11C/11E

Meridian 1 small systems with a different architecture than the large system

PBX

Private Branch Exchange

PC

Personal Computer

PCI

Peripheral Component Interface

PCMCIA

PC Memory Card International Association

PMS

Property Management System

PMSI

Property Management System Interface

RAM

Random Access Memory

RAN

Recorded Announcement

RMS

Room Status

SCN

Single Cell Non-Ringing

SDI

Serial Data Interface

SMP

Switch Management Processor

TCP/IP

Transmission Control Protocol/Internet Protocol

TRN

Call Transfer

TTY

TeleTYpe

TUI

Telephone User Interface; a menu-driven interactive interface that enables the performance of certain functions from a DTMF telephone

XDLC

eXtended Digital Line Card

XSDI

eXtended Serial Data Interface

Index

Meridian 1
Meridian Integrated Voice Services
Description, installation, administration, and maintenance

P0909573

NORTEL NETWORKS™