Meridian 1

# Meridian Integrated Personal Call Director

## Description, installation, administration, and maintenance

Document Number: 553-3001-117
Document Release: Standard 2.00
Date: April 2000

Printed in Canada

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant. This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC rules, and the radio interference regulations of Industry Canada. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense. Meridian 1 is a trademark of Nortel Networks.

# Revision history

**April 2000**

Standard 2.00. This is a global document and is up-issued for X11 Release 25.0x.

**November 1999**

Standard 1.00

# Contents

# About this document

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

This manual explains how to install, configure, and maintain the Meridian Integrated Personal Call Director (MIPCD). Follow the instructions in sequence.

To configure preferences in user accounts, see the *Meridian Integrated Personal Call Director User Guide*.

The topics covered in this document are as follows:

- **"Product description" on page 13** provides a functional and physical description of the MIPCD.
- **"Install and configure the MIPCD cards" on page 47** describes how to:
  - — install the MIPCD
  - — connect MIPCD to a terminal and LAN
  - — configure the MIPCD card
  - — configure the Meridian 1
- **"Configure the MIPCD with the BUI" on page 69** describes the Browser User Interface system settings; it also describes MIPCD administration, configuration, maintenance, and report generation.
- **"Maintenance" on page 99** describes how to maintain and troubleshoot the MIPCD.

- **Appendix A** lists the MIPCD adapter pin assignments.
- **Appendix B** describes reliability, environmental specifications, product integrity, and regulatory standards.

# Product description

Meridian Integrated Personal Call Director (MIPCD) allows users to automatically forward incoming telephone calls to another number, such as a cellular or home telephone. MIPCD tries to reach the forwarding numbers until it reaches the user or exhausts all options. Users can define different call forwarding rules for different callers at different times of the day. MIPCD can also detect and route FAX messages to the appropriate FAX machines.

## Requirements

This section describes the hardware, software, and Meridian 1 requirements.

### Hardware requirements

The MIPCD is an Intelligent Peripheral Equipment (IPE) card compatible with Meridian 1 options 11C, 51, 51C, 61, 61C, 71, 81, and 81C.

SL-1 NT and XT systems upgraded to support IPE cards can use MIPCD cards.

### Software compatibility

You can install MIPCD in software releases X11 release 17 and up. Before release 22, you can configure only 16 ports. For release 22 and up, you can configure up to 32 ports through the Flexible Voice/Data TN feature.

### System software

The required software packages for MIPCD are:

- Digital set (88)
- End-to-End Signaling (EES) (10)
- Call park package (33)

- Automatic Call Distribution (ACD) basic package (45)
- ACD advanced features (41)
- Phantom TN (254) (required only if you use Phantom TN)
- Call Detail Recording (CDR) package (4): optional

## Required resources for each MIPCD card

Each MIPCD card requires the following resources:

**1** One slot per card in the IPE module.

**2** Three Amp current from the 5 V supply (IPE power supply provides 28 Amp total).

**3** Access DNs:

   - One ACD DN (and its associated queue and data block).
   - One agentless ACD queue for TUI access.

**4** Depending on configuration, MIPCD requires one Phantom TN per user, if not using the user’s set.

**5** Each configured port uses one digital ACD DN set block and one DN (for dialing out). This DN does not have to be accessible by DID.

**6** You can define 8, 16, 24, or 32 ports.

**7** Each MIPCD card needs one IP address, gateway, and subnet mask address.

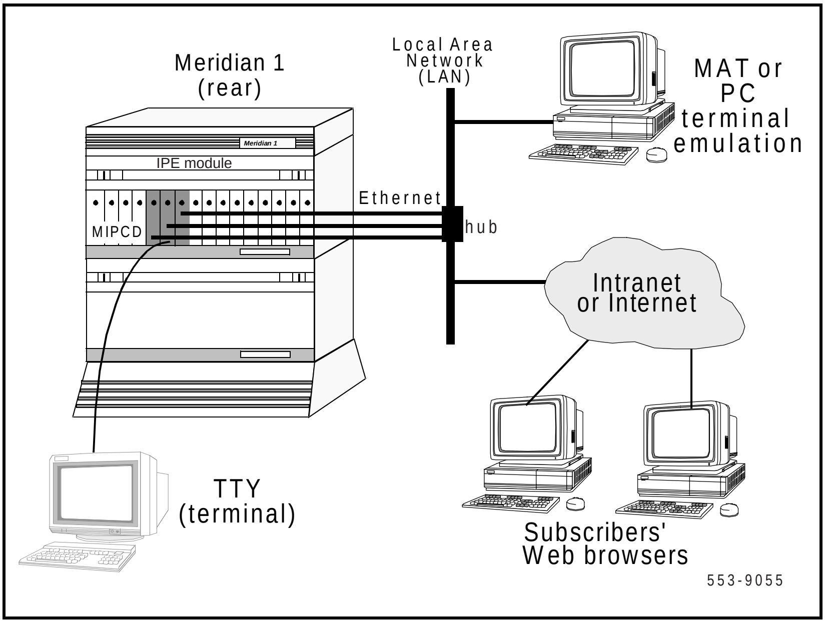
**8** System park DNs should be defined in the Meridian 1 system if the **No Call Reconnect** option is to be used.

# MIPCD overview

The MIPCD is enabled by the installation of one or more MIPCD cards in an IPE module. Each card provides service to a specific set of users.

You connect MIPCD cards to the corporate LAN through an Ethernet connection (see Figure 1).

**Figure 1**
**Basic MIPCD system configuration**



An embedded Web server in each card allows users and administrators to manage system settings and individual accounts with a standard Web browser. A maximum of 10 users can access the Browser User Interface (BUI) at a time.

Administrators connect a TTY terminal to the MIPCD card for system setup, maintenance, and report generation. When the card has an IP address, a PC can use Telnet to enter most Command Line Interface (CLI) commands.

## Network configuration

The MIPCD cards connect to a router as a subnet of the LAN. For proper operation of the TCP/IP, define the following network parameters in each MIPCD:

1. Assign each IP card a different address.
2. Subnet mask.
3. Gateway address (IP address of the router)

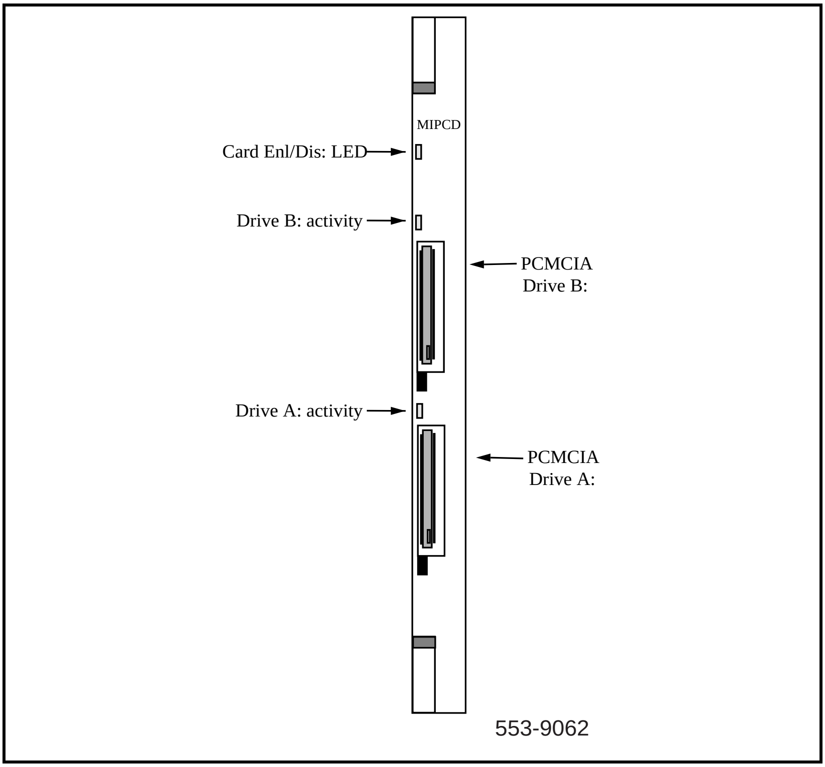
> ***Note:*** You cannot access the MIPCD BUI until you enter the IP settings. See “Configure the IP addresses and system attributes” on page 57 for more information.

Install one or more MIPCD cards into an IPE module or Option 11C cabinet.

# Hardware description

The MIPCD faceplate contains two PCMCIA disk drive slots (see Figure 2).

**Figure 2**
**MIPCD card faceplate**



## Drive A: (lower)

The lower disk drive (A:) is the main operation disk. This disk contains firmware files, database and log files, and voice prompt files. This disk must be present for the MIPCD to operate. Drive A: requires a 520 megabyte disk.

## Drive B: (upper)

You use the upper disk drive (B:) for upgrades and backup. You can remove this disk can when not in use. Drive B: can accept a 520 megabyte disk, or flash cards of 4, 8, and 20 megabyte capacity.

### PCMCIA drive LEDs

- Red LED ON: PCMCIA card is disabled.
- Red LED OFF: PCMCIA card is ready for use.
- Red LED blinking: PCMCIA card is in use.

### Card Enl/Dis LED

- Red LED ON: MIPCD card is disabled.
- Red LED OFF: MIPCD card is enabled.
- Red LED blinking: MIPCD card is conducting a self test.

## Firmware description

The firmware on the PCMCIA card in drive A: enables the operation of MIPCD hardware and features.

To upgrade the firmware, see “Upgrade the firmware or voice files” on page 104.

## Serial/Ethernet port adapter description

MIPCD ships with an adapter to connect the MIPCD card to a terminal (TTY) and an Ethernet network (see Figure 3).

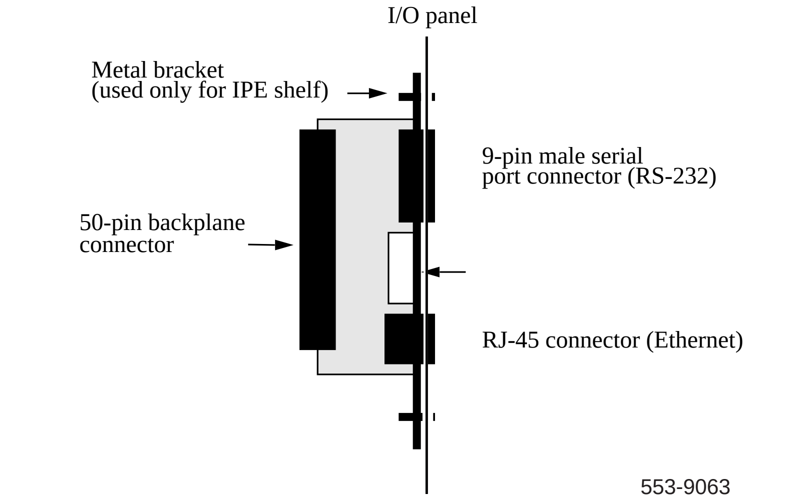
### IPE module (NT5D52AB)

The adapter attaches to the back I/O panel through a 50-pin connector to the backplane. The adapter provides a 9-pin RS-232 serial connector and an RJ-45 Ethernet connector.

### Option 11C (NT5D52BB)

The adapter attaches to a 50-pin Option 11C cabinet I/O connector. The adapter provides a 9-pin RS-232 serial connector and an RJ-45 Ethernet connector.

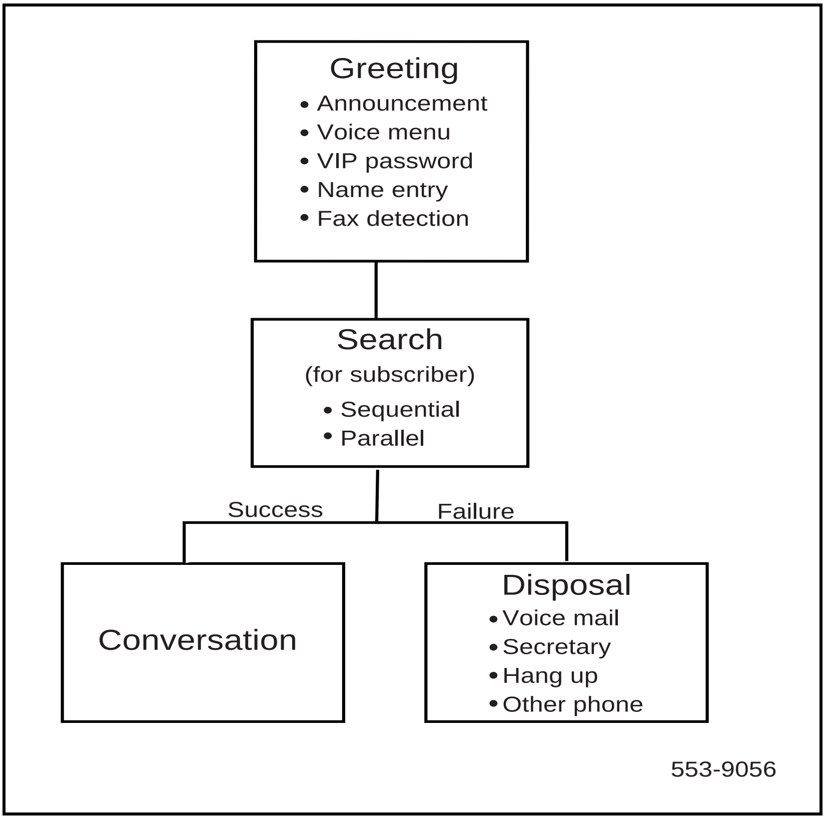
**Figure 3**
**NT5D52BB Option 11C I/O adapter**


I/O panel
Metal bracket (used only for IPE shelf)
9-pin male serial port connector (RS-232)
50-pin backplane connector
RJ-45 connector (Ethernet)
553-9063

# How MIPCD handles incoming calls

Each user has a personal number. Personal profiles associated with that number allows the user to set the rules under which MIPCD forwards incoming calls. Users modify their profile with a standard Web browser. MIPCD routes each call through the stages described in Figure 4.

**Figure 4**
**Stages for incoming calls**



## Greeting stage

The Greeting stage prompts callers to select from a different options and messages.

You can make each Greeting option inactive or active by the user through the Browser User Interface (BUI). You use the BUI to modify the settings for each option.

If you disable both the **Announcement** and **Voice** menu options, the MIPCD system immediately begins to search for the user.

### Announcement menu

The **Announcement** menu is either a system default greeting or a personal greeting recorded by the user. The system default greeting is either the factory-supplied greeting or a greeting recorded by the administrator. You can also make the Announcement inactive.

The user can have up to four personal greetings for different callers or times of the day.

### Voice menu

The **Voice** menu has six options as follows:

1. Digit 1: Begin the search for the user
2. Digit 2: Transfer to voice mail*
3. Digit 3: Transfer to secretary**
4. Digit 4: Transfer to fax machine***
5. Digit 5: transfer to a pager****
6. Star (*): VIP access

A timeout occurs when callers do not enter a digit for four seconds. A search for the user begins immediately.

*Available only if a voice mail number is defined in the user profile.

**Available only if the secretary number is defined in the user profile.

***Available only if the fax number is defined in the user profile. Note that this entry is intended only in a case where a call being started as a voice call by the caller is to be switched to a fax machine from which the fax is sent.

****Available only if the pager number is defined in the user profile.

***Note:*** You can make the **Voice** menu inactive.

### VIP password entry

The user can define a VIP password and provide the password only to specific people. Callers who enter the VIP password receive the treatment defined for VIPs in the user BUI.

The caller presses "*" during or after the greeting or the menu to activate the password entry prompt. MIPCD replies with a prompt for password, which the calling party can enter during the prompt.

The user can enable the **VIP password** option even when the Voice Menu option is disabled. If you disable the Announcement and Voice Menu options, MIPCD pauses to allow the caller to press "*" to enter the VIP password.

### Name entry

Before the search starts, MIPCD prompts the caller to say his or her name. MIPCD records the name (fixed, two-second interval) and plays it to the user when found.

The user can enable or disable the name entry option in their profile.

If a caller selects a menu entry different from **search** (Digit 1) or VIP access ("*"), the name entry does not apply.

## Incoming Fax Detection and Routing

When a call is from a fax machine, MIPCD automatically transfers the call to a fax number defined in the user profile. MIPCD follows the same dialing restrictions for fax numbers that apply for all dialed numbers.

MIPCD disconnects the call if it finds no appropriate fax number.

## Search stage

The MIPCD system dials out to the destination telephone numbers defined by the user. There are two options for the Search stage:

- **Sequential**
  MIPCD dials one number at a time, in order, until it locates the user. MIPCD considers busy and unanswered lines failed tries and the system continues with other destinations. If MIPCD is not successful at dialing all the destination numbers, the call passes on to the Disposal stage.
- **Parallel dialing**
  MIPCD dials all or some of the numbers at the same time. If MIPCD reaches the user, it disconnects all other parallel calls immediately. Busy and unanswered lines are considered failed attempts and the system continues with other destinations. If MIPCD tries all the destination numbers with no answer, the call goes to the Disposal stage.

## Search stage features

Additional user features add another level of security. The features related with the Search stage are:

1. **Basic outdialing**. To dial, MIPCD selects an idle port and sends the destination number to the switch. The source to determine the call result is:

    - Time Compression Multiplexing (TCM) messages from the switch
    - Call-progress tone detection

    A *busy* tone or TCM message indicates busy condition. The search fails and MIPCD tries the next entry. Overflow tone indicates call failure, MIPCD tries the next entry.

    In the normal condition, the call rings at the terminator, and the called party answers the call. If not a timeout occurs, MIPCD considers the call unanswered, and the search continues with the next entry.

2. **Dial restrictions.** Before MIPCD dials a selected destination, it checks the number against restrictions defined by the administrator. MIPCD does not dial a restricted call and logs the attempt in a report.

3 **Caller entertainment**. While the search is in progress, MIPCD plays an announcement until the search ends. The caller can press “*” to listen for the options that are still available on this stage, or directly above the search, by entering menu options **2** (voice mail) or **3** (secretary).

4 **Call Answering password** (optional feature). Users can define a personal user password in the BUI.

- When users answer a call, they must enter the password using a touch-tone telephone.
- A wrong password or no password causes failure of that call attempt and MIPCD tries the other destinations.

5 **Caller’s Number announcement** (optional feature). MIPCD announces the Caller’s Number (Calling Line IDentifier [CLID]) when the user answers the destination telephone. MIPCD prompts the user to press keypad keys to either accept or reject the call.

- If accepted, the call passes to the Conversation stage.
- If rejected, the call passes to the Disposal stage.
- MIPCD announces the caller’s number only after user enters a successful Call Answering password (when users enable both options).
- If you define the Caller’s Name announcement, MIPCD announces the Caller’s Number without requesting keypad input to accept or reject the call. MIPCD requests keypad input for call acceptance after announcing the Caller’s Name.

6 **Caller’s Name announcement**. The name entry occurs during the Greeting stage described above. MIPCD plays the recorded name to the user when they answer the call. The user enters a key response to accept or reject the call.

- If accepted, the call passes to the Conversation stage.
- If rejected, the call passes to the Disposal stage.
- MIPCD plays the Caller’s Name after users enter the **Call Answering** password, and after the CLID announcement, when those features are active.

**7** **Voice Answer Recognition**. Voice Answer Recognition connects the call when a voice answers the telephone. MIPCD activates Voice Answer Recognition when the Call Answering password, Caller's Number announcement, and Caller's Name announcement are inactive. When MIPCD identifies a voice, the search ends, and the call passes to the Conversation stage.

***Note 1:*** MIPCD recognizes the recorded voice on voice mail or answering machine as a voice answer.

***Note 2:*** MIPCD does not play a voice prompt to the called party. The called party must speak first to make the connection.

## Conversation stage

This section describes the Conversation stage and the supported features are as follows:

### Call Reconnect

Users can enable the **Call Reconnect** option in the user BUI. This feature reconnects a disconnected call. If a call is dropped by the answering party, MIPCD plays to the caller a voice prompt, and the calling party can press "*" to reconnect the call again.

If users enable the **Call Reconnect** option, MIPCD establishes the Conversation stage through the MIPCD card. Two MIPCD ports are required for a conversation, in such a case, and the system uses both ports for the duration of the call. Therefore, it can have a negative impact on the capacity of the MIPCD card.

### No Call Reconnect

The administrator can disable the **Call Reconnect** option and force the Meridian 1 to handle all calls. Disabling this option reserves limited MIPCD resources for new calls. The connection takes place without the MIPCD card and both MIPCD ports become available for new calls.

The administrator enables or disables the **Call Reconnect** option in the MIPCD **System Properties** window. If enabled, users can enable the feature for their accounts through the user BUI. The user option states "If call dropped, allow user to reconnect".

## Disposal stage

The purpose of the Disposal stage is to remove the call from the MIPCD and free the port for new calls. Four options are available to the caller when the Search stage does not locate the user:

1. **Transfer to voice mail**: MIPCD routes the caller to Express Messaging. When the call is transferred to voice mail, MIPCD disconnects the call, and the port is free for new calls.

   The user defines the Express Messaging number and the mailbox number in the **Properties** window. The mailbox number should be followed by a character, such as “#”, if required by the voice mail system (Call Pilot and Meridian Mail).
2. **Blind transfer to the secretary**: The proper DN is defined by the user in the **Properties** window or another number. The call is transferred to free the MIPCD.
3. **Hang up**: MIPCD plays a standard announcement “the number cannot be reached” and disconnects the call. MIPCD performs this option as a default, if the other options fail.
4. **Transfer** to another number.

# User profiles

Each user has personal profiles (or databases) associated with their personal telephone number. The administrator makes the default settings for the personal profile, which are modified later by the user.

The administrator controls some settings. See “Administration interfaces” on page 29 for more information. The elements of the user profile fall under three main categories:

- Follow-me profiles
- Follow-me Schedule
- Programmed or immediate overrides

# Follow-me profiles

These are names entered by users that assign Call Forward rules for different callers at different times of the day. Examples of Follow-me profiles names are: “work hours”, “after-work hours”, or “Sunday afternoon”. These titles are determined by the user.

To set up a Follow-me profile, the user:

1. Defines a number of **Find Me at:** lists with the telephone numbers to be dialed when an attempt is made to locate the user.
2. Defines a number of **Calls from** lists the prefixes or specific Caller’s Numbers from which calls are expected.
3. Assigns the **Find Me at:** lists to specific **Calls from** lists so that call from certain prefixes, or callers, are forwarded to specific groups of telephone numbers.

**Example**: A call from the boss after work can be assigned a specific **Find Me at:** list, while a call from a friend during golf hours is assigned a different list.

See “Follow-me profiles overview” in the *MIPCD User Guide* for more information.

## Follow-me Schedule

The Follow-me Schedule links Follow-me profiles to actual time. For each weekday, the user specifies which Follow-me profile is active at which hour.

Different schedules can be defined for non-working times, such as National holidays.

## Programmed or immediate overrides

Users can override the schedule and force activation of a specific Follow-me profile.

Example: If a user is working late, they can activate the “working hours” profile to be active from 16:00 to 20:00 on that day.

Users can force a scheduled override through either a Web browser or over a telephone. See “User interfaces” on page 28 for more information.

# User interfaces

Users can utilize either a Web browser or telephone to change their MIPCD options and settings. See “Configure MIPCD Browser User Interface” and “Configure MIPCD Telephone User Interface” of the *MIPCD User Guide* for detailed instructions on the BUI and TUI for users.

## Browser User Interface (BUI)

Each MIPCD card contains an embedded Web server. Once the system is operational and connected to the corporate LAN, users can utilize a BUI to modify options and settings.

The BUI is accessed with any standard desktop Web browser, eliminating the need for installation and maintenance of specialized software. Up to 10 users can simultaneously operate the BUI.

The recommended browser applications are:

- Microsoft Internet Explorer, Version 4.01 or higher
- Netscape Navigator, Version 4.5 or higher

## Telephony User Interface (TUI)

The TUI allows users to change greetings, overrides, or passwords from remote locations via a telephone.

### Record personal greetings

This allows the user to record or modify personal greetings. These greetings are assigned numbers from 1 to 4. Those numbered greetings are assigned to the various **Find me at:** lists through the BUI.

The TUI commands are:

- Record a greeting
- Play and existing greeting
- Modify an existing greeting

Once the choice is made, the user is prompted with additional instructions.

### Overrides

These commands allow the user to select existing Follow-me profiles. Users can either force the activation of an existing Follow-me profile or force all calls to forward to a number entered by the user.

The methods to define the override are:

- **Programmed override:** The user specifies the start and end time of the programmed override. Each user can have up to eight programmed overrides.
- **Immediate override:** This override becomes active immediately and stays active until the user cancels it.

### Modify passwords

This allows the user to change the TUI password, the VIP password, and the answering password.

# Administration interfaces

System administrators use a Web browser and a terminal (TTY) to change MIPCD options and settings. Use a telephone to change customized system greetings.

## Command Line Interface (CLI)

During initial installation and setup, a terminal (TTY) is connected to the MIPCD serial port connector (on the I/O panel). Use the terminal’s CLI to enter the basic network and system settings, such as the IP address, and for a variety of maintenance and administration task, including software upgrades and debugging.

Once the MIPCD system is connected to a LAN, the CLI commands can be entered with a Telnet connection instead of a TTY.

See “CLI command description” on page 101 for information on specific commands.

## Browser User Interface (BUI)

Each MIPCD card contains an embedded Web server. Once the system is operational and connected to the corporate LAN, administrators use a BUI to modify options and settings.

Access the BUI with any standard desktop Web browser, eliminating the need for installation and maintenance of specialized software. Up to 10 users can simultaneously operate the BUI.

The recommended browser applications are:

- Microsoft Internet Explorer, Version 4.01 or higher
- Netscape Navigator, Version 4.5 or higher

Some user options and default settings can only be made by the administrator. See “Configure the MIPCD with the BUI” on page 69 for detailed instructions.

## Telephony User Interface (TUI)

Customized system greetings can be recorded and modified over a telephone using the administrator password for the TUI. These greetings can be modified for each supported language.

Administrators use the BUI to specify whether the custom system greeting or the **Built-In** system greeting is to be used.

Users can decide (through the BUI) whether to play a system greeting (Built-in or custom), a personal greeting, or no greeting at all. The administrator only decides if the system greeting is **Built-In** or **Customized**.

The administrator TUI commands are as follows:

- Choose a language from the languages supported (English is the default language)
- Record a new greeting
- Play an existing greeting
- Modify an existing greeting

# Billing user

The Meridian 1 CDR bills MIPCD users, in conjunction with the **CDR Charge Account** feature. Each time MIPCD dials out, it operates the Charge Account feature and includes the user number preceded by a prefix. This feature allows you to relate Meridian 1 CDR records originated by MIPCD to specific users.

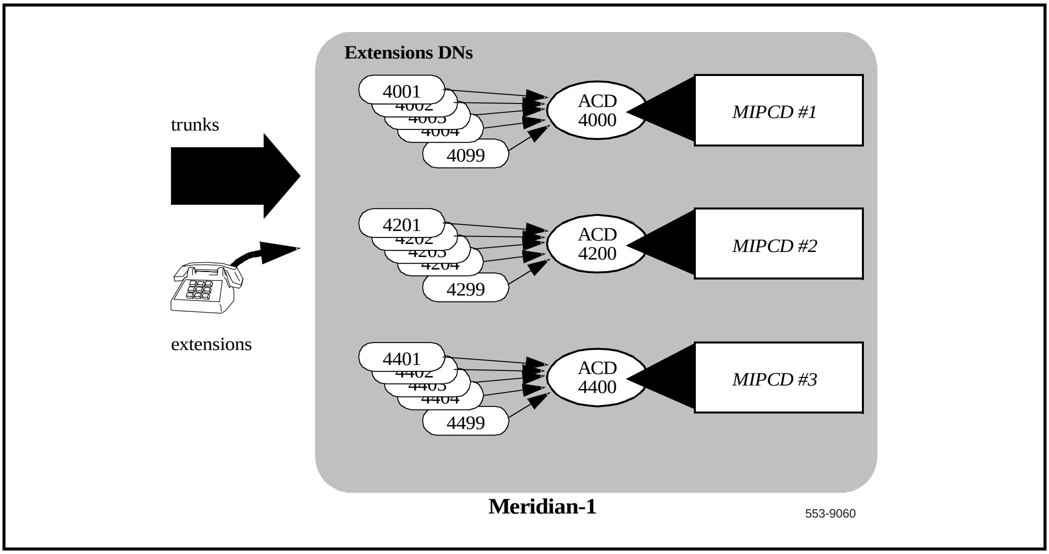
# Dial access to MIPCD service

This section contains a general overview of how telephone numbers are managed by the MIPCD cards. See “Install and configure the MIPCD cards” on page 47 for specific instructions to install and configure the system.

## Overview of user dial access

An example of MIPCD dial access is shown (see Figure 5).

**Figure 5**
**Dial access to MIPCD service**



Telephone calls enter the Meridian 1 through external *trunk* lines or internal *extensions*.

Each MIPCD card manages a specific set of user’s telephone numbers. All extensions 44xx, for example, are handled by one MIPCD card, while all extensions 42xx, are managed by another.

The MIPCD cards manage incoming calls based on the options outlined in “User’s personal number” on page 32.

## User’s personal number

The user’s number is a Directory Number (DN) of Meridian 1. This number can be implemented in three different ways:

- In-house service
- Service provider
- Direct access (**Auto Attendant** option)

### In-house service

The users of the service are the Meridian 1 users, so each one already has a personal extension that also serves as their MIPCD Follow-me number.

To forward calls, users operate the **Call Forward** feature on their telephone. Other redirection features, such as no-answer, busy, etc., also cause calls to forward.

### Service provider

The Meridian 1 owner provides a single telephone number to outside customers. The user’s number is a “Phantom” terminal number that forwards all calls to a dedicated MIPCD card.

### Direct access (Auto Attendant option)

Calls arrive directly to the MIPCD ACD DN. With direct access, callers are prompted to enter the MIPCD extension number to be accessed. The MIPCD extension number is a number identifying the MIPCD user inside the MIPCD card.

The direct access method gives an advantage of no need in either DID range to access from outside, nor special Phantom TNs.

### TUI access

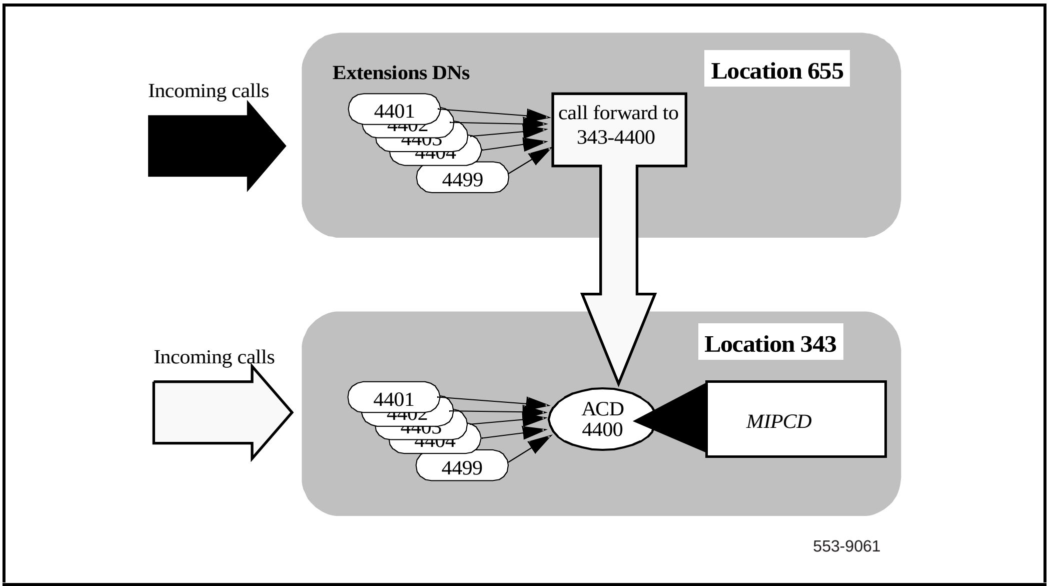
Each MIPCD has an additional number for TUI access. This number is implemented as an ACD DN with no agents (in “night” mode), which forwards all calls to the MIPCD, as a DN of a Phantom TN, or as a virtual extension number inside the MIPCD.

## Dial access to MIPCD in a network

In a networking environment, it is also possible to have the MIPCD in one node and the extensions’ DNs in another node. In this case, users forward their calls to LOC+ACD_DN (LOC is the location code of the node containing the MIPCD). In addition, the user number configured in MIPCD has to include the user’s location code.

A networked configuration is shown in Figure 6. The example shows the same DNs in two different locations.

**Figure 6**
**Dial access in a network**



In this example, user numbers configured in MIPCD at Location 343 would be 4401, 4402... 4499.

For users at location 655, the numbers would be H6554401, H6554402... H6554499.

# System features configured by the administrator

This section contains general descriptions of MIPCD system features that are configured or modified by the administrator.

For specific configuration instructions, see the relevant sections in “Install and configure the MIPCD cards” on page 47 and “Configure user properties” on page 89.

## User configuration

Each user profile must first be configured by the administrator before it can be accessed by the user.

Personal Profile attributes controlled by the administrator are:

- **Dial-out restrictions (call screening table)**: See “Call screening dial restrictions” on page 36.
- **Parallel search (allowed/denied)**: If Parallel search is allowed, the administrator can define the maximum entries in a parallel search (1–8). See “Search stage” on page 23.
- **Allow/deny call through MIPCD card**: See “Conversation stage” on page 25.
- **User passwords**: The administrator sets a user’s initial password in the MIPCD **System Properties** window of the administration BUI (**Administration** tab). Users should change this password immediately. The administrator cannot view users’ passwords. If the password is forgotten, the administrator can reset it to the initial password. Passwords are reset in the BUI **Main** Administration window.

## Network TCP/IP parameters

The TCP/IP parameters must be set by the administrator with a CLI terminal (TTY) before the card can be accessed through the Ethernet network.

## Administrator login

There is a separate administrator password for the BUI and the CLI. See “Log into the CLI Main Menu” on page 99 for more information.

### CLI login

The default administrator password is **user**.

The default administrator password should be changed after system installation.

### BUI login

The default administrator login and password is as follows:

login: **admin**

password: **admin**

The default administrator password should be changed after system installation.

## Multi-language service

MIPCD operates in a number of different languages.

### Browser User Interface (BUI)

Two languages are available for the BUI: English (default) and French.

### Voice prompts

MIPCD provides voice prompts in up to seven different languages: Chinese, English, French, Japanese, Korean, Portuguese, and Spanish. Each card is equipped with a set of languages according to customer request.

The administrator defines a default language for the system. Users can define their selected language, which they can adapt for a specific incoming telephone number.

### Telephony User Interface (TUI)

TUI system voice prompts are available in up to seven different languages: Chinese, English, French, Japanese, Korean, Portuguese, and Spanish. Each card is equipped with a set of languages according to customer request.

The administrator defines a default language for the system. Users can define their selected language.

The administrator defines the MIPCD default BUI language for the system. Users cannot change the default BUI language.

## System greetings

You can use a default system greeting or the administrator can record a custom greeting. Users can record and use personal greetings.

## System calendar

The system calendar defines National holidays. The administrator defines the system calendar for each year, up to three years in advance.

## Call screening dial restrictions

Administrators can control the telephone numbers to where users can forward a call. These restrictions, defined by “call screening tables”, define the telephone numbers or prefixes that MIPCD can, or cannot dial. The administrator assigns each user to one call screening table. Administrators can create up to 32 of these tables.

Administrators create call screening tables through the administration BUI (see “Configure call screening tables” on page 82).

The **Default Authorization** (**Free**), which administrators can modify, allows MIPCD to connect all calls.

> ***Note:*** For increased security, administrators can connect a TTY directly to the MIPCD to disable BUI access to the screening tables. Use **Lock/ Unlock** for this procedure.

### Call screening options

Each entry in the call screening table contains a prefix and the associated action. Possible actions for each entry are as follows:

- **Free**: Default; MIPCD can place the call.
- **Charged**: Call is allowed but charged to the MIPCD user.
- **Denied**: MIPCD cannot place the call.

> ***Note:*** If the IP address and the gateway address defined are identical, this indicates that there is no gateway present; define the subnet mask as 255.0.0.0 or 255.255.0.0.

Administrators can define a default option for numbers not in the call screening table. The default is **Free**.

### Example:

- The customer wants to allow access to all local numbers (default).
- Call screening tables deny calls through ESN access code **6**, **except** calls to ESN Location 646.
- The system allows calls through trunk access code **9** and charges the recipient.

The call screening table looks like Table 1 below.

**Table 1**
**Call screening table example**

| Prefix | Action |
|---|---|
| 6 | Denied |
| 6646* | Free |
| 9 | Charged |

***Note:*** *An entry can be the prefix of another entry.

The length of the defined prefixes can be up to 20 digits. Tables can contain up to 100 entries.

# Security

Hackers can try to steal telephone calls by breaking in to a user's account and forwarding calls to their destinations. The potential areas are:

### TUI

An intruder can try to steal a user's TUI password.

### Web interface

An intruder can try to steal a user's or administrator's BUI password.

### Telnet or File Transfer Protocol (FTP)

An intruder can try to access the MIPCD directly through Telnet or FTP and damage the files.

> ***Note:*** Most corporate networks are protected from the global Internet by firewalls or other security measures. Access to the MIPCD outside a firewall through the Web, Telnet, or FTP is not possible.

## Security Solutions

### Hacker alert

MIPCD triggers a "Hacker alert" when it sees multiple wrong login tries in a row. The system default for a Hacker alert is three incorrect login tries. The administrator can change this setting.

MIPCD counts the tries per session *and* per user (three errors in a row for the same user, even in separate sessions).

A Hacker alert triggers the following actions:

- MIPCD disconnects a TUI call and terminates the browser BUI.
- MIPCD disables the user's password. The user cannot access the BUI until the administrator resets the password.
- MIPCD issues a warning record. MIPCD can output the record to a local file on the PCMCIA, a network (TCP/IP) location, or to the card's serial RS-232 port.

### Login activity file

MIPCD records all TUI and BUI login tries (successful and not successful), in the Event Logger files. MIPCD stores one Event Logger file per day on the PCMCIA disk for the past month.

The administrator can view the information through the BUI or receive automatic daily e-mails of the Event Logger. The administrator sets the automatic e-mail parameter through the administrator BUI.

## Traffic data reports

MIPCD generates a daily traffic report file and stores it on the PCMCIA disk. MIPCD updates the file every hour. Traffic reports tell the administrator how many calls a user or MIPCD card receives for a period of hours or days.

Traffic reports are a record of the number of “pegs” for every user and for every MIPCD card. MIPCD counts a “peg” when a call occurs (see “Traffic Report categories (pegs)” on page 40).

MIPCD separates traffic reports by:

- **Common Traffic**: Data for the MIPCD card.
- **User Traffic**: Data accumulated for up to 50 selected users.

Administrators can view the traffic data for single users, or groups of users with the BUI **Main Administration** window (see “Reset user passwords” on page 94).

Administrators can retrieve traffic files from the card’s PCMCIA disk by:

- Automatic daily e-mails; “Configure system properties” on page 73 contains instructions to configure automatic e-mails
- Over the Ethernet through FTP
- Direct download from the PCMCIA disk

## Traffic Report categories (pegs)

Traffic Reports display a summary of the number of “pegs” that occur for each user and for the MIPCD card. The actions defined as “pegs” are:

### Monthly statistics

- **Outdial attempts free**: Number of outdial attempts, Free.
- **Outdial attempts charged**: Number of outdial attempts, Charged.
- **All-ports-busy fatal**: Number of all-ports-busy—origination failed in either sequential search or parallel search because MIPCD found no available port (total congestion).
- **All-ports-busy service degradation**: Not enough ports were available for full parallel search, performance degraded.
- **Reoriginations:** Number of reoriginations when MIPCD disconnected call and reconnected immediately.
- **Total calls through override**: Calls through override.
- **Immediate override, direct**: Calls through immediate override, direct number.
- **Immediate override, routing**: Calls through immediate override, routing profile.
- **Programmed override, direct**: Calls through programmed override, direct number
- **Programmed override, routing**: Calls through programmed override, routing profile.
- **Incoming fax calls**: number of Calls automatically identified as fax calls.
- **VIP calls**: Calls when MIPCD accepted VIP password.
- **Late connections**: Number of late connections—number of calls where time to connect was longer than the threshold set by the administrator.
- **Average time to connect**: Average time to connect, in seconds, for successful searches.

***Note 1:*** MIPCD counts “Total time to connect”, as a peg, which reflects the time needed for each connected call.

***Note 2:*** BUI calculates “Average time to connect” as “Total time to connect”/“Total successful connections” when displayed.

- **Express Messaging**: Caller requested to be transferred directly to voice mail or MIPCD transferred the call to voice mail under disposal treatment.
- **Call Screening Violations**: MIPCD tried to a call a user with a prefix denied to that user by the administrator.
- **Auto Attendant successful**: Successful calls through the **Auto Attendant** option.
- **Auto Attendant failed**: Calls through the **Auto Attendant** option failed.

### Daily statistics

- **Total calls**: Total number of incoming calls.
- **TUI calls**: Number of TUI calls (the user calls to change their database).
- **Follow-me calls**: Number of Follow-me calls (MIPCD calls searching for the user).
- **Service time exceeded**: Number of calls discontinued by service time exceeded.
- **Caller disconnects**: Number of abandoned calls, caller disconnects.
- **Total searches**: Number of searches in total.
- **Sequential searches**: Number of sequential searches.
- **Parallel searches**: Number of parallel searches.
- **Total successful connections**: Number of successful MIPCD connections.
- **Connections through card**: Number of successful through MIPCD connections.
- **Connections off card**: Number of successful off-MIPCD connections.
- **Search failures**: Number of search failures. Call passes to disposal stage.
- **Total outdial tries**: Number of outdial tries.

- **TUI change pswd**: Tries to use password change feature.
- **TUI record greeting**: TUI record greeting tries.
- **TUI immediate override**: TUI immediate override defining.
- **TUI programmed override**: TUI programmed override defining.

# Event Logger reports

Event Logger reports are a record of different activities in a MICPD card. See “Call Process (CP) application reports” below for a description of those activities.

The administrator uses the administration BUI to define which Event categories to record on the PCMCIA disk. The administrator also uses the BUI to define how large the files can be, and which categories to view in the BUI. See “Configure system properties” on page 73 for more information.

MIPCD records events in order. The first three letters of each report (CP, TUI, and BUI) is an event category mnemonic.

## Call Process (CP) application reports

- **CP Screening violation**: The user defined a number to call with a prefix denied by the administrator and MIPCD tried a call to this prefix.
- **CP Answering pswd violation**: The dialed party did not enter a valid password twice and search moved on to next call or to disposal.
- **CP VIP pswd failure**: MIPCD detected an attempt to enter an incorrect VIP password three times during an MIPCD call and terminated the MIPCD session.

### Telephony User Interface (TUI) application

- **TUI Pswd failure**: Hacker alert. MIPCD discontinued a session after a TUI log-in try exceeded the maximum number of password tries.
- **TUI (BUI) Pswd reminder**: A TUI password moved into the reminder state, indicating that the user is reminded to change the password in each login.
- **TUI (BUI) Pswd expiration**: MIPCD disabled password, indicating that the user had passed reminder state, without changing the password being changed by the user.

### Browser User Interface (BUI) application

- **BUI Non-existent login**: User typed in an incorrect login name.
- **BUI User pswd violation, further login blocked**: A BUI password newly blocked, the successive login failure counter for the user reached the maximum level as set by administrator.
- **BUI Administrator successive login failure violation**: An administrator BUI account has a new invalid login try beyond the value of maximum level set by the administrator.
- **BUI User list overflow**: A BUI add account failed, caused by having the maximum number of users limited by the keycode.
- **BUI Login/pswd database distorted**: Login not found for BUI action that operates on itself (on its own open session).
- **BUI New user added**: Administrator added a new user.
- **BUI User pswd reset**: User password reset to initial value.
- **BUI User deleted by administrator**
- **BUI User pswd changed by user**
- **BUI Change login name by administrator**
- **BUI Successful login**
- **BUI Successful logout**
- **BUI Login session timeout**
- **BUI Login session polling disconnect**

### Command Line Interface (CLI) application

- **CLI Screening table locking/unlocking**
- **CLI Administrator BUI password reset**
- **CLI password reset**
- **CLI password changed**

- **INI Card Reset**: Records the reset reason, which can be one of the following:
  - Watchdog
  - S/W Reset
  - Cardlan Reset
  - BUS Error
  - Dongle Reset
  - Malloc Reset
  - Power-Up

## MIPCD cards per system

The following factors limit the number of MIPCD cards per system:

- Number of IPE shelves.
- 5 Vdc power consumption by other cards installed on the same IPE.
- Number of ACD DNs defined (per customer)
- Superloop blocking factor: For nonblocking applications (or a nonblocking part of the system), one superloop is required for every 120 TNs. MIPCD can have up to 32 TNs (ports) defined.

## MIPCD CPU capacity

CPU load is similar to M2616 ACD agents. However, the volume of calls depends on the number of users (not only number of calls).

## Power requirements

Table 2 describes the MIPCD power requirements.

**Table 2**
**MIPCD power requirements**

| Voltage | Source | Current (A) |
|---|---|---|
| +5 V | Backplane | 3 |
| +15 V | Backplane | 0.1 |
| Total power (maximum) | | 16.5 W |

# User capacity

If you enable the **Call Reconnect** feature, Meridian 1 establishes the Conversation stage through the MIPCD card. MIPCD requires two ports for the duration of the call. This can have an adverse impact on MIPCD capacity of the MIPCD card. If you disable **Call Reconnect**, Meridian 1 handles all calls. The MIPCD card can answer new incoming calls.

# Install and configure the MIPCD cards

The initial configuration of the MIPCD card must be done with a CLI. The card is unable to communicate with the Meridian 1 system or the LAN until these settings have been made. Complete the following steps in order:

**1** “Install the card” on page 48.

**2** “Install the I/O adapter (terminal and Ethernet)” on page 50.

**3** “Connect the MIPCD to a LAN and terminal” on page 53.

**4** “Configure the IP addresses and system attributes” on page 57.

**5** “Configure the MIPCD on the Meridian 1” on page 61.

Once the MIPCD card is configured with an IP address, a Telnet program (terminal emulation) can be used on a PC to enter the remaining CLI commands.

# Install the card

**1** Review the “Requirements” on page 13 for descriptions of the hardware, software, and system requirements.

**2** Identify the IPE card slots selected for MIPCD card (see Table 3).

**Table 3**
**MIPCD installation by module type**

| Meridian 1 Modules | MIPCD Card Slots |
|---|---|
| NT8D37BA/EC IPE modules, NT8D11BC/ED CE/PE modules | All available IPE card slots. |
| NT8D37AA/DC IPE modules | 0, 4, 8, and 12 |
| NT8D11AC/DC CE/PE modules | 0 |

**3** Pull the top and bottom latches away from the MIPCD faceplate.

**4** Insert the MIPCD card into the card guides. Gently push the card until it makes contact with the backplane connector.

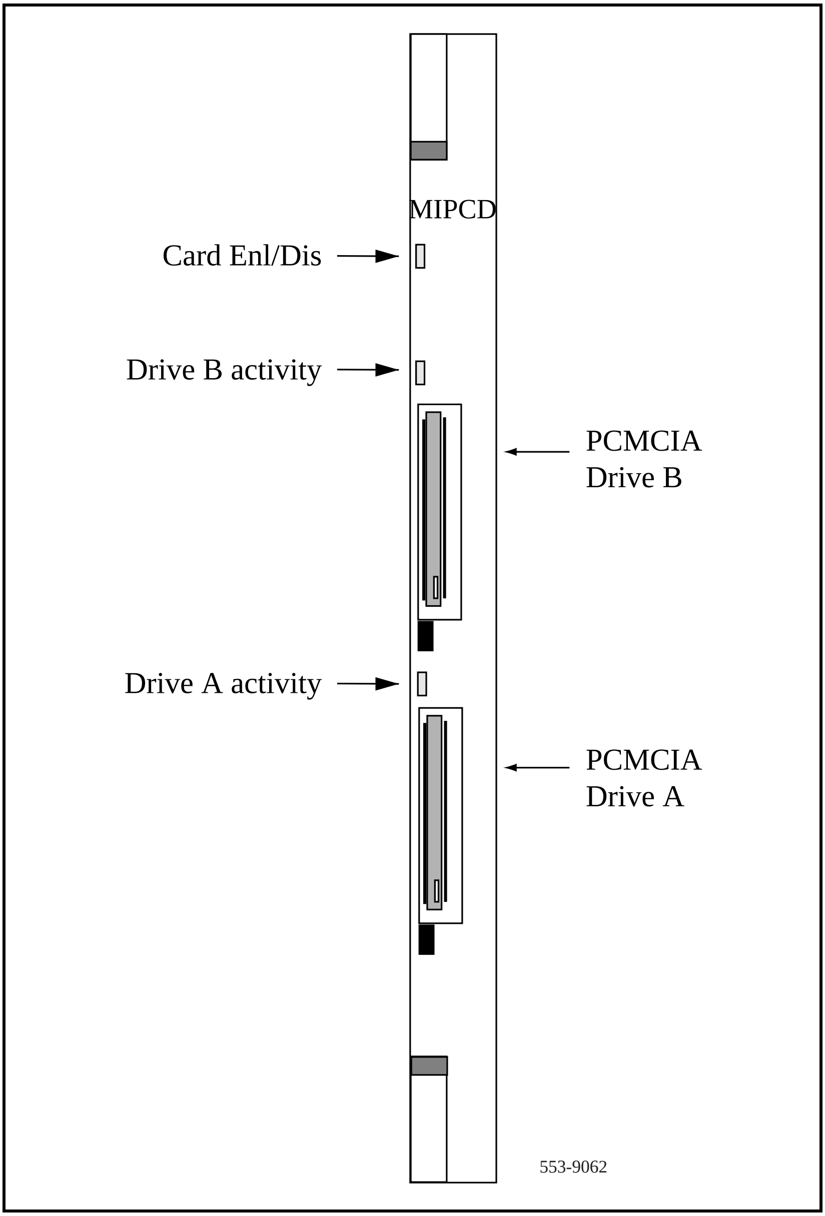
**5** Push the top and the bottom latches firmly towards the faceplate to lock the card in place.

**6** Verify that the PCMCIA card is properly seated in the lower PCMCIA drive A: (see Figure 7).

**7** The card Enl/Dis LED should blink three times and then remain ON. This indicates a successful self test.

**8** Repeat steps 1 through 6 for each MIPCD card.

**Figure 7**
**MIPCD card faceplate**



# Install the I/O adapter (terminal and Ethernet)

Each MIPCD card includes an adapter to connect the MIPCD card to a terminal (TTY) and a LAN.

Two different adapters are available: the NT5D52AB for an IPE module and the NT5D52BB for an Option 11C system.

## IPE module (NT5D52AB)

The adapter attaches to the back I/O panel, with a 50-pin connector to the backplane, a 9-pin RS-232 serial connector for a terminal, and an RJ-45 Ethernet connection (see Figure 10 on page 54).

**1** Remove the cover plate from the I/O panel at the rear of the IPE module.

**2** Remove the retaining screws from the I/O panel and lift it from the module.

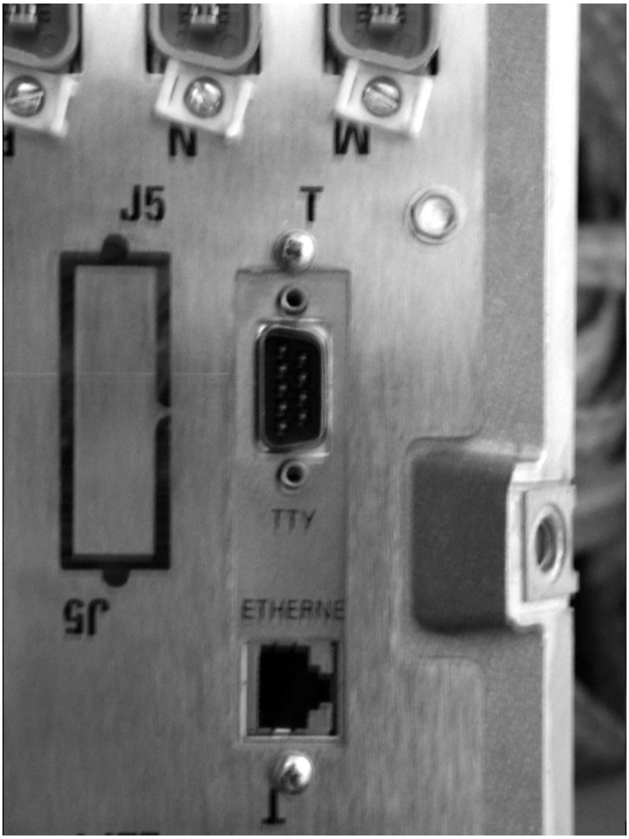
**3** Disconnect the backplane cable 50-pin connector from the I/O panel filter connector.

**4** Remove the existing filter connector from the I/O panel and save the retaining screws. This filter connector corresponds to the card slot designated for the MIPCD card installation.

**5** Use the saved retaining screws to install the NT5D52AB Ethernet adapter card into the designated I/O panel connector cutout (see Figure 8).

**6** Replace the I/O panel onto the module. Replace the module’s cover plate.

**Figure 8**
**Ethernet adapter card (NT5D52AB) in IPE I/O panel**



553-9074

## Option 11C tip/ring connector (NT5D52BB)

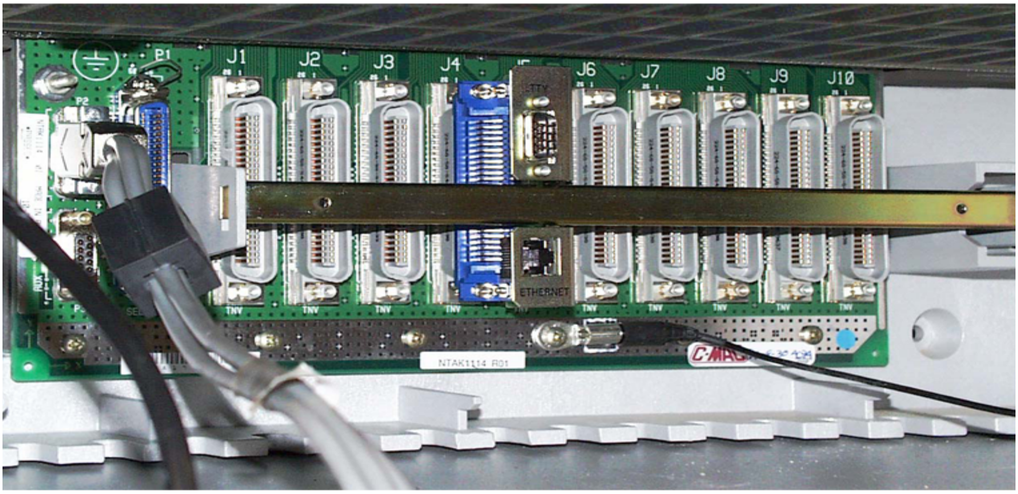
The adapter includes a 50-pin connector to the backplane 9-pin RS-232 serial connector for a terminal and an RJ-45 Ethernet connection (see Figure 9).

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

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

3 Secure the Ethernet adapter to the cabinet.

**Figure 9**
**Ethernet adapter (NT5D52BB) in a wall mount Option 11C**



# Connect the MIPCD to a LAN and terminal

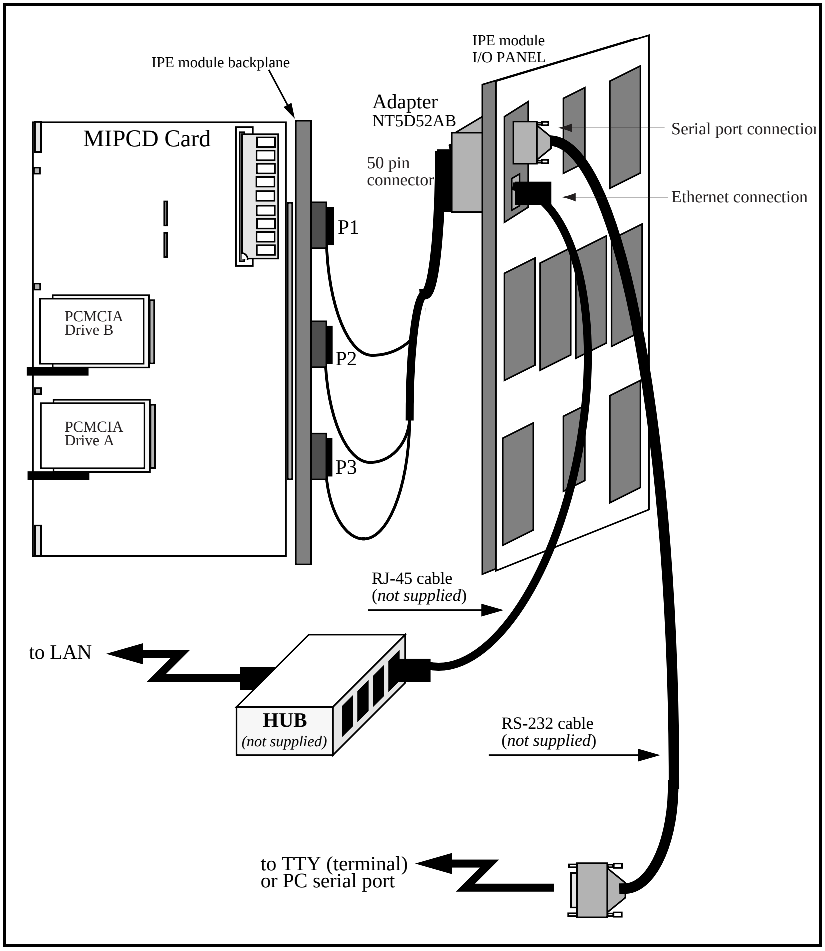
## Terminal

Connect the TTY terminal to the serial port RS-232 connection on the Ethernet adapter.

## Ethernet

Connect a RJ-45 Ethernet cable from the Ethernet port on the I/O adapter to the LAN hub. Multiple MIPCD cards can be connected to the same hub (see Figure 10).

### Figure 10
### Ethernet adapter in an IPE module (NT5D52AB)



# Connect a modem to the adapter

This procedure requires a modem, a 9-pin-to-DB-25 cable, an RJ-11 cable, and a null modem, if required (see Figure 11). Table 4 describes the adapter pins.

**Table 4**
**NT5D52 connector pin description**

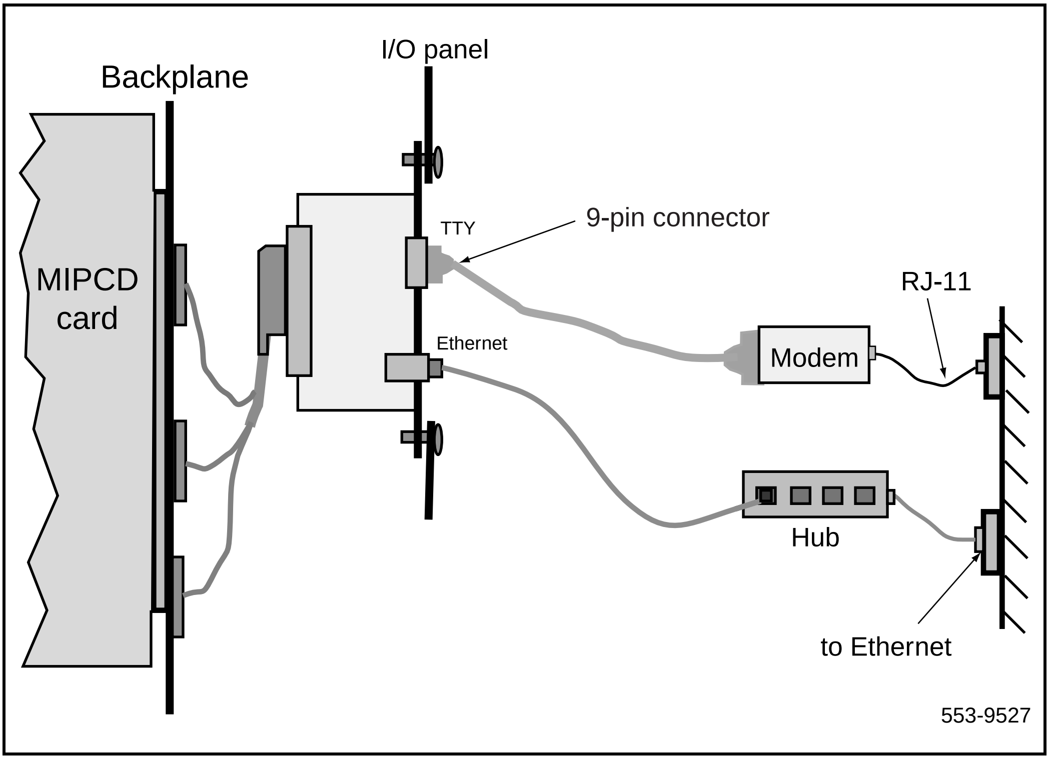
| Connector | Pin Number | Signal Description |
|---|---|---|
| 9-pin serial connector | 2 | RS-232 TX (transmit) |
| | 3 | RS-232 RX (receive) |
| | 5 | GND (ground) |
| RJ-45 Ethernet connector | 1 | LAN_TX + |
| | 2 | LAN_TX - |
| | 3 | LAN_RX + |
| | 6 | LAN_RX - |

**1** Connect cable between TTY adapter and modem. Use null modem, if required.

**2** Connect modem to phone plug.

**3** Connect Ethernet cable to adapter (see Figure 11).

**Figure 11**
**MIPCD modem and Ethernet connection example**



# Configure the IP addresses and system attributes

The IP address must be entered for BUI access. The BUI is used to configure individual and system user parameters. The IP address can only be entered with a terminal directly connected to the serial port of the card (via the I/O panel).

## Before you begin

If applicable, define Agent ID and MQA parameters. Load Overlay 23 using the system TTY, and enter the appropriate responses to the prompts as listed in Table 5. Increase the IDUB as required for the MIPCD ports for the customer. Add 32 ports for every MIPCD card. For example, IDLB is 2000. If you add one MIPCD (32 ports), enter 2032 as the limit. If the IDUB is 2500, change the upper boundary to 2532.

**Table 5**
**Define Agent ID and MQA parameters (LD 23)**

| Prompt | Response | Description |
|---|---|---|
| REQ | NEW | New |
| TYPE | ADS | Type of data block = Auxiliary Data System) |
| CUST | 0-99 | Customer number |
| AID | (NO) YES | Agent ID mode |
| - IDLB | (1)-9999 | Agent ID Lower Boundary |
| - IDUB | *IDLB*-(9999) | Agent ID Upper Boundary |
| - MQA | (NO) YES | (Don’t allow)/Allow agents to use MQA functionality. |

## Enter the port, user, and keycode data

The card performs a self test once it is inserted into the Meridian 1 module and powered up. At the end of the test, a system prompt asks for the number of ports, the number of users, and the keycode.

The keycode enables the number of ports and users. The correct values must be entered.

**1** Configure the terminal:

- Transmission speed: 9600 bps
- Data bits: 8
- Stop bit: 1
- Parity: No
- Flow control: none (do not use X-on/X-off flow control)

**2** Verify that the terminal is connected to the TTY adapter serial port.

**3** Locate the key code in the MIPCD shipping carton.

**4** At the **Modify, Save, Cancel** prompt, type **M**, and press **Enter**.

**5** At the **max ports (0):** prompt, enter the number of MIPCD prompts listed on the keycode label, and press **Enter**. 8, 16, 24, or 32 ports can be defined on an MIPCD card.

**6** At the **max users (0):** prompt, enter the maximum number of MIPCD users listed on the keycode label, and press **Enter**. Up to 300 users (in increments of 50) are supported by a single MIPCD card.

**7** At the **Modify, Save, Cancel** prompt, type **S**, and press **Enter**.

**8** Type in keycode1 and press **Enter**.

**9** Type in keycode2 and press **Enter**.

**10** Type in keycode3 and press **Enter**.

**11** At the **Modify, Save, Cancel** prompt, type **S**, and press **Enter**.
The MIPCD terminal displays a keycode confirmation message.

**12** MIPCD displays the user login prompt.

**13** Enter the default user ID (**user**). MIPCD displays the Main menu (see Figure 12).

## Change card name and enter network address attributes

**1** From the Main menu, enter **SA/SY** (see Figure 12).

**2** At the cursor, type **M**, and press **Enter**.

**3** If required, change the card name, and press **Enter** three times.

**4** Set card_acd definition.

**5** Set agent ID value.

**6** Set acd multiple queue value.

**7** Press **Enter** five times.

**8** Type in the subnet mask, gateway address, and IP address.

— The **subnet mask** has XXX.XXX.XXX.XXX format, where every XXX is in the range of 0-255. A subnet mask in binary presentation of 32 bits has, at least, the first eight digits “1” and the last digit is “0.”

— The **gateway address** has XXX.XXX.XXX.XXX format, where every token is in the range of 0-255.

— The **IP address** is the MIPCD Internet Protocol address. It has the same format as the gateway address.

**9** Press **Enter** three times.

**10** Enter the mail server address.

MIPCD uses the **mail server address** to send daily Event Logger and Traffic Report files through e-mail. “Traffic” on page 81.

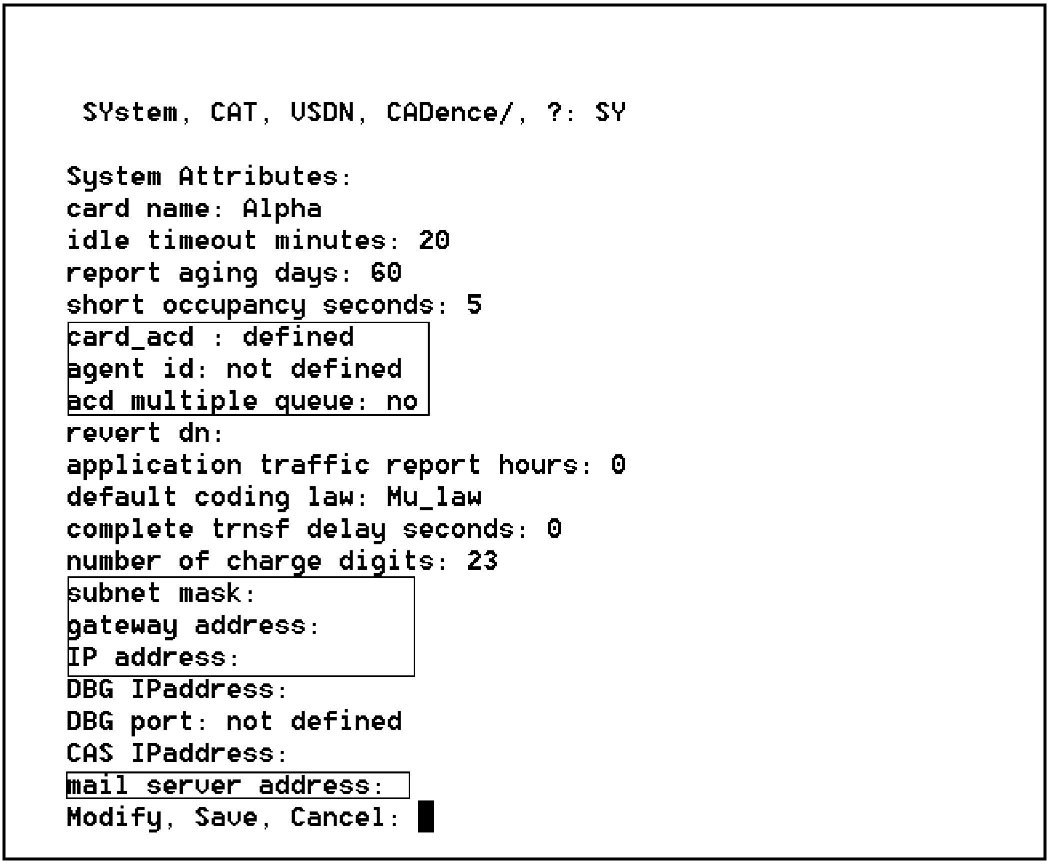
***Note:*** If the IP address and gateway address defined are identical, this indicates there is no established gateway; define the subnet mask as 255.0.0.0 or 255.255.0.0.

**11** Enter **S** and press **Enter** to save changes.

**12** MIPCD prompts a system message “restart card (Y or N)?”. Select **Y**. PCMICA LED flashes.

**13** MIPCD presents a login screen when the restart process is complete.

**Figure 12**
**MIPCD Main menu**



```
 SYstem, CAT, USDN, CADence/, ?: SY

System Attributes:
card name: Alpha
idle timeout minutes: 20
report aging days: 60
short occupancy seconds: 5
card_acd : defined
agent id: not defined
acd multiple queue: no
revert dn:
application traffic report hours: 0
default coding law: Mu_law
complete trnsf delay seconds: 0
number of charge digits: 23
subnet mask:
gateway address:
IP address:
DBG IPaddress:
DBG port: not defined
CAS IPaddress:
mail server address:
Modify, Save, Cancel: █
```

# Configure the MIPCD on the Meridian 1

The Meridian 1 configuration must be made for the MIPCD card to operate.

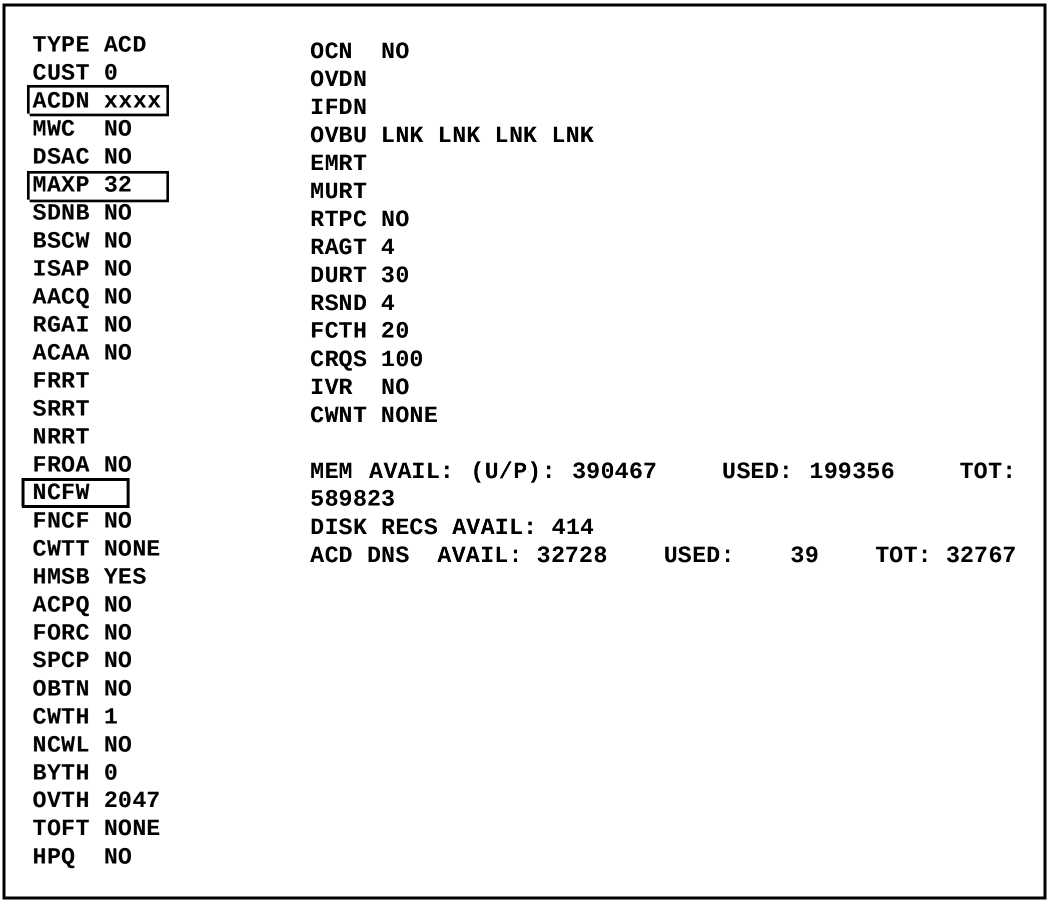
## Configure the ACD data block

To configure the Automatic Call Distribution (ACD) data block, load Overlay 23 using the system TTY, and enter the appropriate responses to the prompts as listed in Table 6 (see Figure 13).

**Table 6**
**Define an ACD data block (LD 23)**

| Prompt | Response | Description |
|---|---|---|
| REQ | NEW | New |
| TYPE | ACD | Automatic Call Distribution |
| CUST | 0-99 | Customer number |
| ACDN | xxx..x | Main ACD DN of the MIPCD card |
| MAXP | 32 | Maximum ports (the upper range) |
| NCFW | <voice mail DN directory> | Voice mail directory numbers |

**Figure 13**
**ACD definitions (LD 23)**



```
TYPE ACD            OCN  NO
CUST 0              OVDN
ACDN xxxx           IFDN
MWC  NO             OVBU LNK LNK LNK LNK
DSAC NO             EMRT
MAXP 32             MURT
SDNB NO             RTPC NO
BSCW NO             RAGT 4
ISAP NO             DURT 30
AACQ NO             RSND 4
RGAI NO             FCTH 20
ACAA NO             CRQS 100
FRRT                IVR  NO
SRRT                CWNT NONE
NRRT
FROA NO             MEM AVAIL: (U/P): 390467     USED: 199356     TOT:
NCFW                589823
FNCF NO             DISK RECS AVAIL: 414
CWTT NONE           ACD DNS  AVAIL: 32728    USED:    39    TOT: 32767
HMSB YES
ACPQ NO
FORC NO
SPCP NO
OBTN NO
CWTH 1
NCWL NO
BYTH 0
OVTH 2047
TOFT NONE
HPQ  NO
```

## Define the TUI access DN

Telephony User Interface (TUI) access DN is defined for an ACD queue with no agents and the night DN leading to the ACD DN defined as the “Main ACD DN” in Overlay 23. Another possibility for the TUI DN is to define it as Phantom TN (i.e. 500 type set on the Phantom Loop, in LD 10) with Call Forward to the Main ACD DN.

MIPCD users access DNs, depending on configuration:

- Phantom TNs for the users, with Call Forward to the Main ACD DN.
- Regular user sets (e.g. M2616). User activates Call Forward All calls to the Main ACD DN when the MIPCD service is to be activated (see Table 7).

**Table 7**
**Define TUI access DN (LD 23)**

| Prompt | Response | Description |
|---|---|---|
| REQ | NEW | Add a new |
| TYPE | ACD | Automatic Call Distribution |
| CUST | 0-99 | Customer number |
| ACDN | xxx..x | ACD DN of the MIPCD TUI |
| ... | ... | |
| NCFW | xxx..x | Main ACD DN (defined in Table 6) |
| ... | ... | |

An example of the Meridian 1 definitions for ACD is shown in Figure 13. ACDN is the main ACD DN.

## Phantom DN

Enter the Meridian 1 definitions for the Phantom DN (Overlay 10) as shown in Figure 14.

- The specific Terminal Number (TN) and Directory Number (DN) vary by site. Those variables are represented by “x” in Figure 14.

- CFXA is the Class of Service (CLS) that enables Call Forwarding.
- The last four variables in the screen (under FTR) is the main ACD DN in LD 23

**Figure 14**
**Phantom DN definitions (LD 10)**

```
DES  MIPCD
TN   xxx x xx xx  PHANTOM
TYPE 500
CDEN 4D
CUST 0
WRLS NO
DN   xxxx x     MARP
AST  NO
IAPG 0
HUNT
TGAR 1
LDN  NO
NCOS 0
SGRP 0
RNPG 0
XLST
SCI  0
SCPW
SFLT NO
CAC  3
CLS  CTD DTN FBD XFD WTA THFD FND HTD ONS
     LPR XRD CWD SWD MWD LPD XHD CCSD LND TVD
     CFTD SFD MRD C6D CNID CLBD AUTU
     ICDD CDMD LLCN EHTD MCTD
     GPUD DPUD CFXA ARHD OVDD AGTD CLTD LDTD ASCD
    MBXD CPFA CPTA HSPD UDI RCC HBTD DDGA NAMA MIND
     NRWD NRCD NROD SPKD CRD PRSD MCRD
     EXR0 SHL ABDD CFHD DNAA
     CWND USRD BNRD OCBD RTDD FAXD
PLEV 02
AACS NO
MLWU_LANG 0
FTR  DCFW 12  <ACD DN>
```

## Define each unit of the card as an M2616 digital set

In Overlay 11, define each unit of the MIPCD card as an M2616 digital set, agent of the ACD DN defined in Table 8. Keys should be defined as follows:

**Table 8**
**Define each unit of the card as an M2616 digital set (LD 11)**

| Prompt | Response | Description |
|---|---|---|
| REQ: | NEW | Add new data |
| TYPE: | 2616 | Digital telephone set M2616 |
| TN | l s c u | Terminal number of MIPCD port |
| DES | a...x | Designator |
| CUST | 0-99 | Customer number |
| CLS | CFXA | Call Forward eXternal Allow |
| ... | ... | |
| KEY | 0 ACD xxx yyy | xxx = Main ACD DN, yyy = CLID <any DN> |
| KEY | 1 SCN xxx | xxx = any DN of the port |
| KEY | 2 NRD | |
| KEY | 3 MSB | |
| KEY | 4 TRN | |
| KEY | 5 A03 | |
| KEY | 6 NHC | |
| KEY | 8 PRK | See *X11 Features Guide* under **Call Park** feature |
| KEY | 9 CHG | |

An example of the Meridian 1 system definitions for MIPCD ports is shown in Figure 15.

**Figure 15**
**MIPCD port definitions in the Meridian 1 (LD 11)**

```
TN   xxx x xx xx                                     HUNT
TYPE 2616                                            PLEV 02
CDEN 8D                                              SPID NONE
CUST 0                                               AST
AOM  0                                               IAPG 0
FDN                                                  AACS NO
TGAR 7                                               ITNA NO
LDN  NO                                              DGRP
NCOS 6                                               PRI  01
SGRP 0                                               MLWU_LANG 0
RNPG 0                                               DNDR 0
SCI  0                                               KEY  00 ACD xxxx 0  863702
SSU                                                              AGN
XLST                                                      01 SCN 863703 0     MARP
SCPW                                                      02 NRD
SFLT NO                                                   03 MSB
CAC  3                                                    04 TRN
CLS  UNR FBD WTA LPR MTD FND HTD ADD HFD                  05 AO3
     MWD AAD IMD XHD IRD NID OLD VCE DRG1                 06 NHC
     POD DSX VMD CMSD CCSD SWD LND CNDD                   07
     CFTD SFD MRD DDV CNID                                08 PRK
     ICDD CDMD LLCN MCTD CLBD AUTU                        09 CHG
     GPUD DPUD DNDD CFXA ARHD CNTD CLTD ASCD              10
     CPFA CPTA HSPD ABDD DELD CFHD FICD NAID DNAA         11
RDLA                                                      12
     UDI RCC HBTD AHD DDGA NAMA MIND PRSD NRWD NRCD       13
NROD                                                      14
     EXR0                                                 15
     USRD ULAD RTDD OCBD FLXD
CPND_LANG ENG
```

*Note 1:* CFXA is the Class of Service (CLS) that enables Call Forwarding.

*Note 2:* Access restrictions defined on the unit should take into consideration that MIPCD handles outdial screening.

*Note 3:* If only a subset of the card's units are configured, they should always begin from Unit 0 and on. In Release 22 and later, it is possible to configure also units 17–31 as voice units.

## Enable the MIPCD card

After the MIPCD ACD block is configured, the MIPCD card can be enabled.

MIPCD does not support the Meridian 1 Option 11C autoconfiguration feature. Each MIPCD unit must be defined manually before the card can be used.

To enable the MIPCD card, do the following:

**1** Load Overlay 32.

**2** Enable the MIPCD card.

— For large systems, use the system TTY to execute the **ENLC l s c** command, where **l** is the loop, **s** is the module or shelf, and **c** is the card to be enabled.

— For Option 11C, use the **ENLC** command, where **c** is the card to be enabled.

# Configure the MIPCD with the BUI

The Browser User Interface (BUI) is used to configure each MIPCD card and its associated users. The BUI is accessed with a standard Web browser, such as Netscape Navigator (4.5 or higher) or Microsoft Internet Explorer (4.01 or higher).

The BUI has two branches, one for users and one for the administrator. This section describes how to use the administration BUI to configure system properties, call screening tables, and the calendar. These parameters must be set before the individual user accounts can be created and configured.

Complete the steps in sequence.

**1** “Configure system properties” on page 73

**2** “Configure call screening tables” on page 81

**3** “Configure the calendar” on page 86

**4** “Configure user properties” on page 87

# Log into the MIPCD BUI

**1** To log into the MIPCD BUI with a World Wide Web browser, enter the MIPCD card's IP address followed by **/mipcd.html** in the **Location** field:

**http://xxx.xxx.xxx.xxx/mipcd.htm** (where "xxx.xxx.xxx.xxx" is the IP address assigned to the MIPCD card)
Example: **http://47.82.46.92/mipcd.htm**

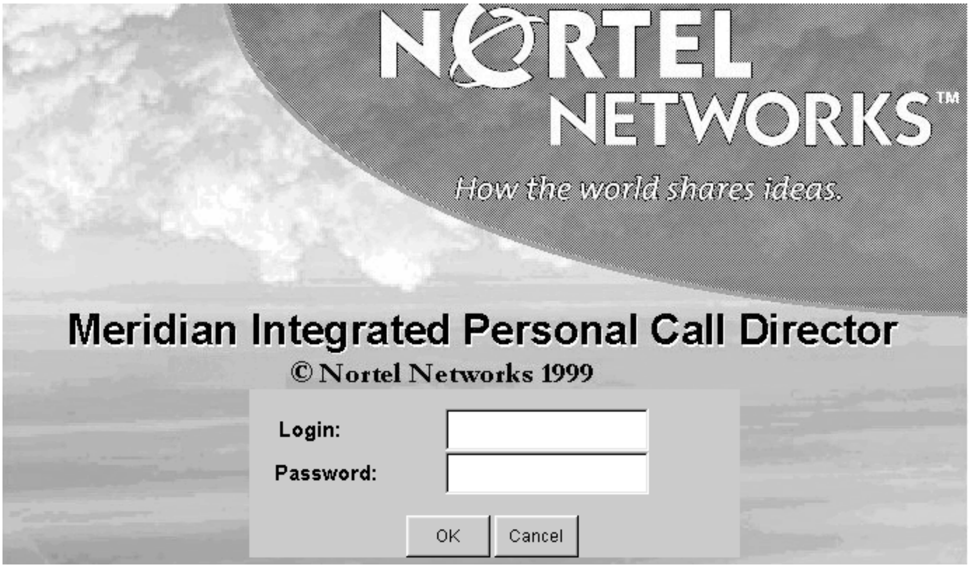
**2** The MIPCD **BUI Login** window appears (see Figure 16).

**3** Enter the **administrator** login and password (default: **admin**).

**4** Press **Enter**.

**5** To change default passwords, see "Administration tab configuration procedures" on page 75.

**Figure 16**
**MIPCD BUI Login window**



Meridian Integrated Personal Call Director

© Nortel Networks 1999

Login:

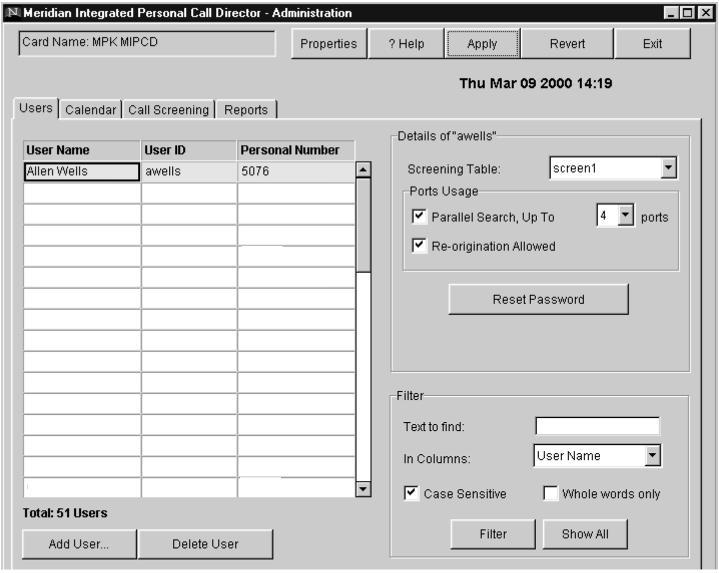
Password:

# User properties description

The MIPCB card presents different windows to administrators and users.

The BUI **Main Administration** window (see Figure 17) provides access to system and user configuration windows. The parameters entered in these windows are only used for that particular MIPCD card and associated users. System and user configurations must be made for each installed MIPCD card.

**Figure 17**
**BUI Main Administration window**



Meridian Integrated Personal Call Director - Administration

Card Name: MPK MIPCD

Thu Mar 09 2000 14:19

| User Name | User ID | Personal Number |
|---|---|---|
| Allen Wells | awells | 5076 |

Total: 51 Users

Details of "awells"

Screening Table: screen1

Ports Usage

☑ Parallel Search, Up To 4 ports

☑ Re-origination Allowed

Filter

Text to find:

In Columns: User Name

☑ Case Sensitive ☐ Whole words only

## BUI Main Administration window

The BUI **Main Administration** window provides access to four main pages. Click the appropriate tab to access a specific page described as follows:

#### *Users*

Used to add, delete, and configure individual user accounts; appears automatically when the BUI **Main Administration** window is accessed.

#### *Calendar*

Defines the National holidays.

#### *Call Screening*

Used to configure the call screening tables. These tables define users' dial restrictions. One table is assigned to each user.

#### *Reports*

Used to view and analyze Traffic and Event Logger reports.

### Top menu bar

The BUI **Main Administration** window includes a menu bar along the top:

#### *Properties*

Opens the MIPCD **System Properties** window, which is used to set the global parameters for each MIPCD card and its associated users. "Configure system properties" on page 73 describes the fields available in this window.

#### *? Help*

Opens the online **Help** window.

#### *Apply*

Used to permanently save the configuration changes. The changes are operable on the MIPCD card after about three minutes. The MIPCD remains in service throughout the process.

#### *Revert*

Used to clear the configuration changes made since the last **Apply** command. Changes made in the session are erased and the previously saved changes are used.

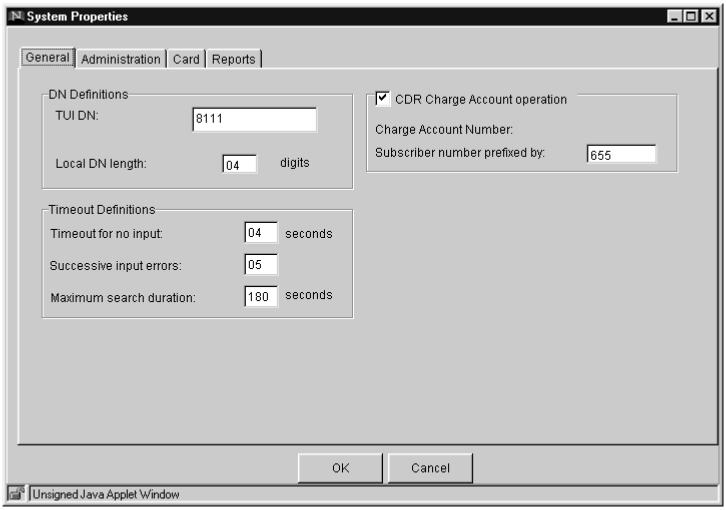
***Exit***

Used to quit the MIPCD BUI.

# Configure system properties

Click **Properties** at the top of the BUI **Main Administration** window. The MIPCD **System Properties** window appears (see Figure 18). By default, the **General** tab appears first.

**Figure 18**
**MIPCD System Properties window—General tab**



DN Definitions

TUI DN: 8111

Local DN length: 04 digits

Timeout Definitions

Timeout for no input: 04 seconds

Successive input errors: 05

Maximum search duration: 180 seconds

☑ CDR Charge Account operation

Charge Account Number:

Subscriber number prefixed by: 655

## General tab configuration procedures

### DN Definitions

1 Enter the **TUI DN**. This is the Directory Number to access the Telephony User Interface.

2 In the **Local DN length** field, enter the length of the local Directory Numbers. The range is 2—7; the default is **4**.

### Timeout Definitions

1 In the **Timeout for no input** field, enter the number of seconds the system waits for input from the caller. The default is **3**.

2 In the **Successive input errors** field, enter the number of input errors allowed.

3 In the **Maximum search duration** field, enter the maximum number of seconds allowed for a search.

### CDR Charge Account operation

1 Check the **CDR Charge Account operation** box to enter the prefix for a user's personal charge account number. The charge account number is a prefix added to the user's number for each phone call. For information on CDR Charge Account Reports, see *Meridian 1 Call Detail Recorder NTP*.

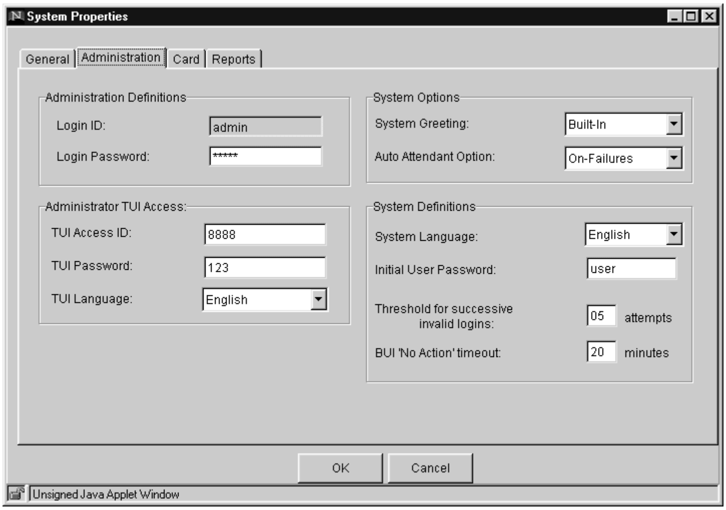
**CDR Charge Account operation description:** The Meridian 1 CDR bills MIPCD users, in conjunction with the CDR Charge Account feature. Every time MIPCD dials out, it operates the Charge Account feature and enters the user number preceded by a prefix. This feature allows you to relate Meridian 1 CDR records originated by MIPCD to specific users.

2 Click **OK** to accept all field entries.

## Administration tab configuration procedures

Click the **Administration** tab in the MIPCD **System Properties** window (see Figure 19).

**Figure 19**
**MIPCD System Properties window—Administration tab**



System Properties

Administration Definitions

Login ID: admin

Login Password: *****

Administrator TUI Access:

TUI Access ID: 8888

TUI Password: 123

TUI Language: English

System Options

System Greeting: Built-In

Auto Attendant Option: On-Failures

System Definitions

System Language: English

Initial User Password: user

Threshold for successive invalid logins: 05 attempts

BUI 'No Action' timeout: 20 minutes

### Administration Definitions

**1** The **Login ID** field is read only. The default login **admin** cannot be changed.

**2** In the **Login Password** field, enter a new administrator password. The password can be up to 10 characters and/or digits. Always change the **admin** password from the default.

### System Options

**1** In the **System Greeting** pull-down menu, choose either the **Built-In** or **Customized** voice greeting.

**2** In the **Auto Attendant Option** pull-down menu, choose among the following options:

- **Not Used**: Only the MIPCD Call Forward entry is used.
- **On-Failures**: The **Auto Attendant Option** is used when automatic recognition is unsuccessful. Automatic recognition is unsuccessful, if there is no personal number served by the MIPCD, or if there are no Call Forward instructions.
- **All Calls**: Automatic recognition of the personal number is disabled. The caller is immediately connected to the Auto Attendant.

### Administrator TUI Access

**1** In the **TUI Access ID** field, enter the touch tone code for the administrator login.

**2** In the **TUI Password** field, enter or change the administrator TUI password.

**3** In the **TUI Language** pull-down menu, choose the TUI language (English is the default language).

### System Definitions

**1** In the **System Language** pull-down menu, select the default language (**English**) for the voice prompts.

**2** In the **Initial User Password** field, enter the default user password (**user**). This is the password for new users. This is also the default password when a user’s password is reset by the administrator.

**3** In the **Threshold for successive invalid logins** field, enter the number of consecutive erroneous login attempts that can be made before a user's password is automatically disabled (from 3 to 10, the default is **3**).

This is a security feature to prevent unauthorized users from learning a user's password through trial and error.

If a user's password is disabled due to invalid login attempts, the password must be reset by the administrator. To reset a user password, click **Reset Password** in the **Users** tab of the BUI **Main Administration** window. The default password is **user**. The user's password is reset to the value in the **Initial User Password** field.

**4** In the **BUI 'No Action' timeout** field, enter the minutes for a user or administrator to perform a change to the BUI settings.

***Note 1:*** If an **Apply** or **Revert** command is not issued during this time, a warning window appears to inform the user that the BUI session is automatically disconnected in 60 seconds.

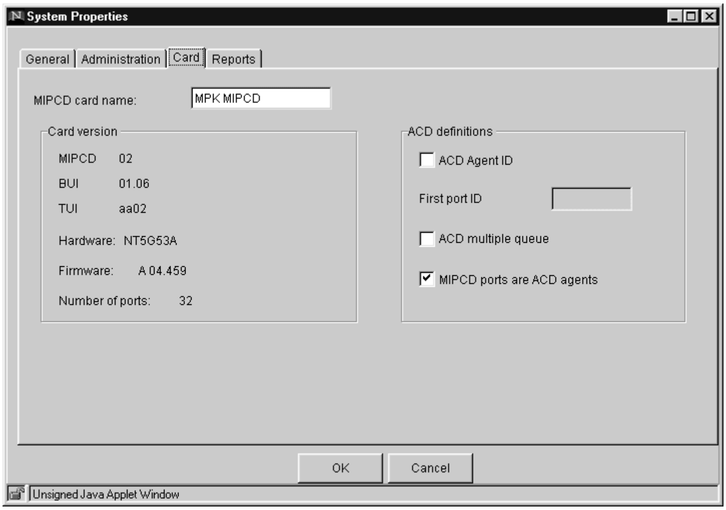
***Note 2:*** You can click **OK** in this window to prolong the session for one additional period (the value set in this field). If no action is taken during the second period, the BUI session automatically terminates.

Once the administration variables have been selected, click **OK** to accept the settings.

## Card tab configuration procedures

Click the **Card** tab in the MIPCD **System Properties** window (see Figure 20).

**Figure 20**
**MIPCD System Properties window—Card tab**



MIPCD card name: MPK MIPCD

Card version

MIPCD 02
BUI 01.06
TUI aa02

Hardware: NT5G53A

Firmware: A 04.459

Number of ports: 32

ACD definitions

☐ ACD Agent ID

First port ID

☐ ACD multiple queue

☑ MIPCD ports are ACD agents

### Card version

**1** In the **MIPCD card name** field, enter the text to be displayed in the BUI **Main Administration** window. Each MIPCD card requires a different name.

**2** The hardware version and firmware version are displayed. These fields are read-only.

**3** The number of ports configured by the keycode are displayed. This field is read-only.

### ACD definitions

The parameters for ACD definition setup must match the Meridian 1 configuration:

— **ACD Agent ID**: Indicates if the ACD is configured with the agent ID option. The default is **OFF**.

— **First port ID**: If the agent ID is enabled (the **ACD Agent ID** box is checked), the **First port ID** field contains the four-digit first agent ID for MIPCD ports. The other ports use the succeeding agent IDs. For example, if the first agent ID is 3000 and MIPCD has 24 ports, the system uses agent IDs 3000 through 3023.

— **ACD Multiple queue**: Indicates if the ACD is configured with the multiple-queue option. This is required because it affects the agent login process. The default is **OFF**.

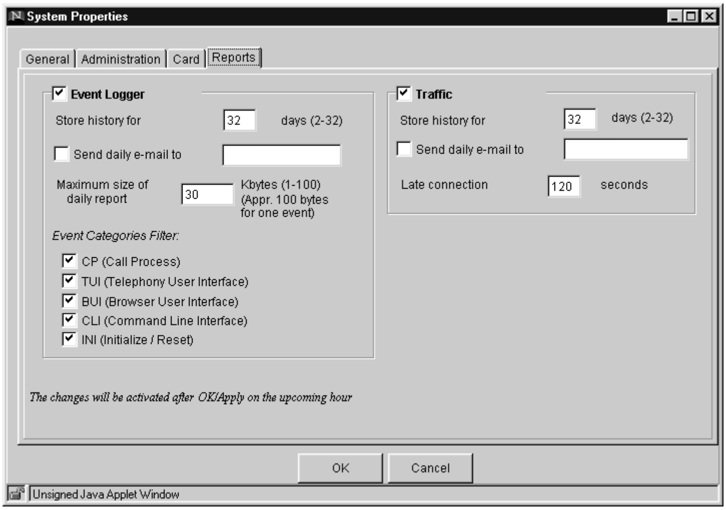
— Check the **MIPCD ports are ACD agents** box.

Click **OK** to accept field entries.

## Traffic tab configuration procedures

Click the **Reports** tab in the MIPCD **System Properties** window (see Figure 21). This feature is used to activate and deactivate traffic and log reports, identify events to record, and determine how long to save the log reports. See “Traffic data reports” on page 39 for descriptions of the various report categories.

**Figure 21**
**MIPCD System Properties —Reports tab**



☑ **Event Logger**

Store history for 32 days (2-32)

□ Send daily e-mail to

Maximum size of daily report 30 Kbytes (1-100) (Appr. 100 bytes for one event)

*Event Categories Filter:*

☑ CP (Call Process)
☑ TUI (Telephony User Interface)
☑ BUI (Browser User Interface)
☑ CLI (Command Line Interface)
☑ INI (Initialize / Reset)

☑ **Traffic**

Store history for 32 days (2-32)

□ Send daily e-mail to

Late connection 120 seconds

*The changes will be activated after OK/Apply on the upcoming hour*

Unsigned Java Applet Window

## Traffic

**1** Click the **Traffic** box to enable traffic reports.

**2** Enter the number of days between 2 and 32 that the records keep.

**3** To receive daily e-mails of the Traffic reports, click **Send daily e-mail to**, and enter the address of the person who receives the report.

**Traffic E-mail Report description:** MIPCD generates and stores traffic measurement files on the PCMCIA disk, one file for each day. MIPCD sends one traffic report every hour to the file. Traffic data includes the common card traffic data and per-user data accumulated for up to 50 selected users**.** The MIPCD administrator can program MIPCD to send traffic files for the previous day attached to an e-mail.

See “Reset user passwords” on page 91 for more information on Traffic Reports.

**4** In the **Late connection** field, enter the threshold for a call to be connected.

## Event Logger

**1** Click **Event Logger** to enable Event Logger reports.

**2** Enter the number of days between 2 and 32 that MIPCD keeps the Event Logger records.

**3** To receive daily e-mails of the Event Logger reports, click **Send daily e-mail to**, and enter the address of the person who receives the daily Event Logger file.

**Event Logger E-mail Report description:** MIPCD records all TUI and BUI login attempts (successful and unsuccessful) in the Event Logger files. MIPCD stores one file per day for the last month on the PCMCIA disk. You can view Event Logger data in the BUI **Traffic** window. The MIPCD administrator can also program MIPCD to send Event Logger files for the previous day attached to an e-mail. The administrator enters the recipient’s e-mail address in the MIPCD System Properties **Traffic** tab.

See “Event Logger reports” on page 42 for more information.

**4** Enter the maximum size of the daily report in Kbytes (1 to 100); (approximately 100 bytes for one event).

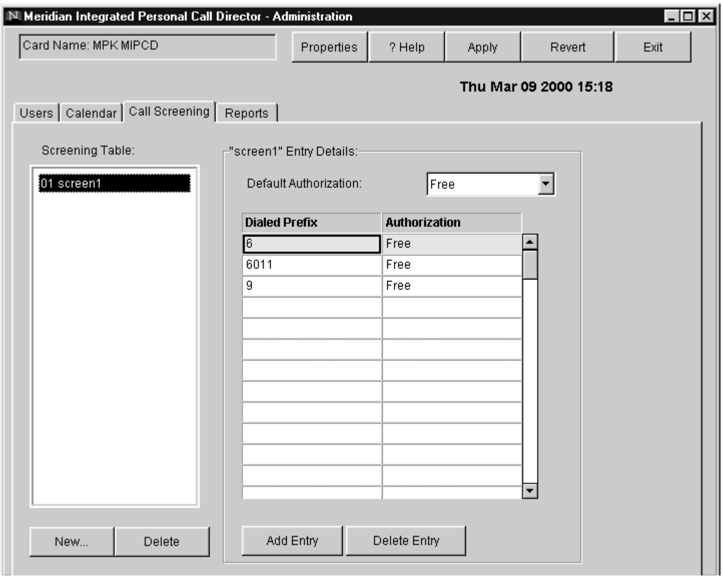
**5** Check the applicable **Event Categories Filter** options of Event Logger reports to be kept.

# Configure call screening tables

The **Call Screening** tab in the BUI **Main Administration** window (see Figure 22) is used to configure a maximum of 32 call screening tables. These tables define a user's dial restrictions. One table is assigned to each user.

> ***Note:*** For increased security, administrators can use a TTY directly connected to the MIPCD to disable BUI access to the screening tables.

**Figure 22**
**Call Screening window**



Card Name: MPK MIPCD

Thu Mar 09 2000 15:18

Screening Table:

01 screen1

"screen1" Entry Details:

Default Authorization: Free

| Dialed Prefix | Authorization |
|---|---|
| 6 | Free |
| 6011 | Free |
| 9 | Free |

## Call screening options

Each entry in the call screening table contains a prefix and the associated action. Possible actions for each entry are:

- **Free**: Default; the call can be placed.
- **Charged**: The call is allowed but charged to the recipient.
- **Denied**: The call cannot be placed.

## Default Authorization

Choose the appropriate **Default Authorization** from the pull-down menu for numbers not covered by the table.

## Guidelines

- The length of the defined prefixes can be up to 20 digits.
- Tables can contain up to 100 entries.
- An entry can be the prefix of another entry.

## Validation table

Table 9 contains an example call screening table based on the preferences below:

- The customer wants to allow access to all local numbers (default).
- Calls through ESN access code **6** are to be denied, **except** calls to ESN location 646, which are allowed.
- Calls through trunk access code **9** are allowed, but charged.

**Table 9**
**Validation table example**

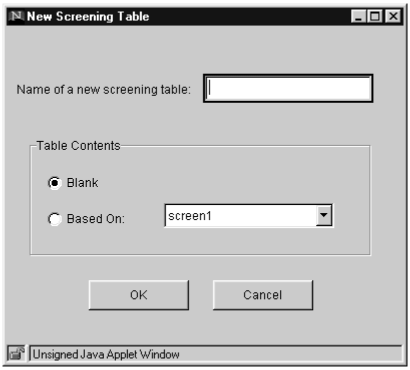
| Prefix | Action |
|---|---|
| Default | Free |
| 6 | Denied |
| 6646 | Free |
| 9 | Charged |

## Add a table

The **Screening Tables** field lists the currently defined tables.

1. To add a table, click **New**. The **New Screening Table** window appears (see Figure 23).
2. Name the table.
3. Under the **Table Contents** field, click the appropriate radio button to choose between a blank table or one based on an existing table.
4. Click **OK** to create the table or **Cancel** to exit the window. Once you click OK, the **Call Screening** window appears with the new screening table name.

**Figure 23**
**New Screening Table window**



Name of a new screening table:

Table Contents

● Blank

○ Based On: screen1

5 From the **Call Screening** window, you can add, modify, and delete restrictions in the **Details** field to the right.

— Click **Add Entry** to add a new restriction line.

— Enter the prefix in the **Dialed Prefix** line on the left.

— To enter the **Authorization** category, click once in the field.
A pull-down menu becomes accessible. Click again on the line to choose from the three categories (**Free**, **Denied**, or **Charged**).

— To delete an entry, highlight the appropriate line, and click **Delete Entry**.

6 Click **Apply** at the top of the window to save the changes.

## Delete a table

1. From the **Call Screening** window, click once on the table name to highlight it.
2. Click **Delete**.
3. Click **Apply** at the top of the window to save the changes.

## Modify a table

1. From the **Call Screening** window, click once on the table name to highlight it. The details for that table appears in the **Entry Details** field.
2. Click on the line you want to modify. To change the **Authorization** category, click once in the field. A pull-down menu becomes accessible. Click again on the line to choose from the three categories (**Free**, **Denied**, or **Charged**).

# Configure the calendar

From the Main Administration window, click the Calendar tab to define national holidays or other special non-working days (see Figure 24).

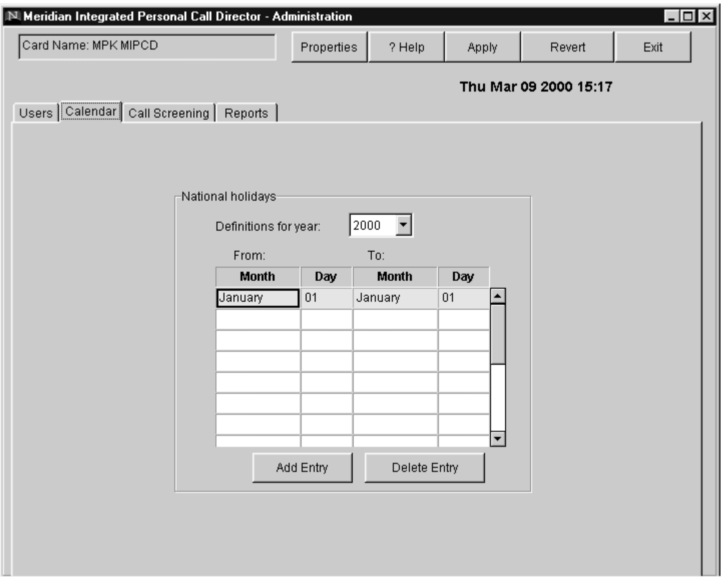
1 To add an entry line, click **Add Entry**.

2 To delete an entry, click once to highlight the line, then click **Delete Entry**.

3 Enter the range of dates for each holiday or non-working day.

4 For a single day, only the **From:** field is required. The **To:** field can be left blank..

**Figure 24**
**National holidays calendar**



Card Name: MPK MIPCD

Thu Mar 09 2000 15:17

National holidays

Definitions for year: 2000

| From: | | To: | |
|---|---|---|---|
| **Month** | **Day** | **Month** | **Day** |
| January | 01 | January | 01 |

## Modify the National Days table

The national holidays associated with each category are defined in the **From:** and **To:** columns.

# Configure user properties

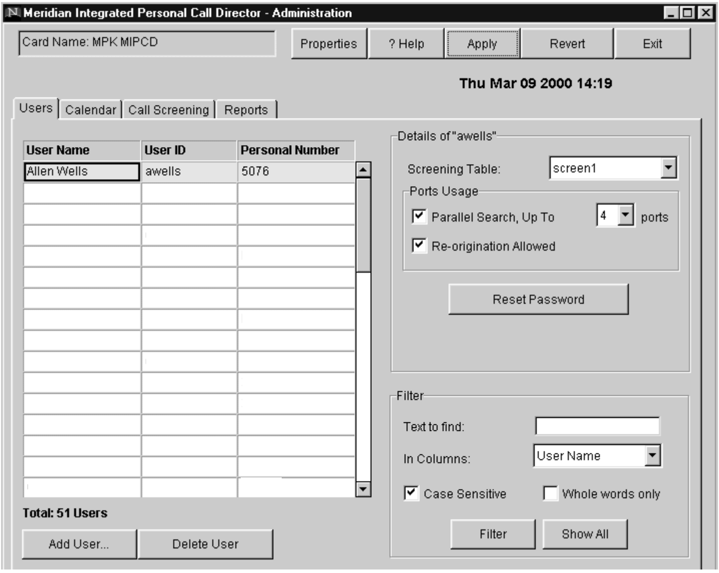
This section describes how to use the administration BUI to add and configure user accounts.

All system properties should be set before individual user accounts are configured. System properties contain the parameters that apply to all users. See “Configure system properties” on page 73 for instructions.

## Users

The **Users** tab (see Figure 25) automatically appears when you access the administration BUI. Use the **Users** tab to add, delete, and configure individual user accounts.

**Figure 25**
**Users tab**



Card Name: MPK MIPCD

Thu Mar 09 2000 14:19

| User Name | User ID | Personal Number |
|---|---|---|
| Allen Wells | awells | 5076 |

Total: 51 Users

Details of "awells"

Screening Table: screen1

Ports Usage

☑ Parallel Search, Up To 4 ports

☑ Re-origination Allowed

Filter

Text to find:

In Columns: User Name

☑ Case Sensitive □ Whole words only

### Users table

The Users table on the left lists all users assigned to the current MIPCD card:

- Select a line with a single click.

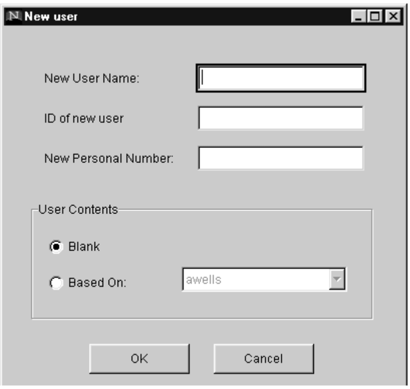
- Double-click a line to edit the line.
- To sort the table by user name, user ID, or personal number, click on the appropriate column title.

### Add users

Add MIPCD users to the MIPCD card as follows:

**1** From the **Users** tab, click **Add User...**. The **New User** window appears (see Figure 26).

**Figure 26**
**New User window**



New User Name:

ID of new user

New Personal Number:

User Contents

● Blank

○ Based On: awells

**2** Enter the user's information in the appropriate fields:

— **New User Name**: The user's actual name.

— **New User ID**: The user's BUI login ID.

— **New Personal Number**: The number dialed by callers to reach the user (this is the Directory Number [DN] from which the call is forwarded to MIPCD). If the forwarding set (or Phantom TN) is in the same Meridian 1 as MIPCD, only the local extension DN is entered here. If the forwarding set is in a remote ESN node, the remote ESN location code, or steering code must also be entered.

**3** If the **Details** parameters are based on an existing user, click the **Based on** radio button in the **User Contents** section. Choose the user whose **Details** parameters are to be copied, and then click **OK**.
The user account is now configured.

4 If an existing set of parameters are not used, click the **Blank** radio button, and then click **OK**.

5 Complete the **Details** section in the **Users** tab as follows:

— From the **Screening Tables** pull-down menu, choose a call screening table.

— From the **Caller List Size** pull-down menu, select the maximum number of callers the user can enter.

— Under the **Ports Usage** section, check the **Parallel Search** box to enable parallel searches. Enter the maximum number of ports allowed in the search. This number cannot exceed the number of ports supported by the MIPCD card.

— To enable the **Call Reconnect** feature, check the **Re-origination Allowed** box. The conversations of users who choose this feature occupy two ports on the MIPCD card for the duration of the call.

6 Click **Apply** to save the changes. Click **Revert** to restore the original settings.

### Delete users

1 From the **Users** tab, click once on the user entry to select the user line.

2 Click **Delete User** to delete the user entry.

3 Click **Apply** to save the changes or click **Revert** to restore the original settings.

## Modify user configurations

**1** From the **Users** tab, to modify a user entry, click once in the field to activate that field.

**2** Enter the new parameters.

**3** Modify the user information in the appropriate fields:

— **User Name**: The user's actual name.

— **User ID**: The user's BUI login ID.

— **Personal Number**: The number dialed by callers to reach the user (this is the Directory Number [DN] from which the call is forwarded to MIPCD. If the forwarding set (or Phantom TN) is in the same Meridian 1 as MIPCD, only the local extension DN is entered here. If the forwarding set is in a remote ESN node, the remote ESN location code, or steering code must also be entered.

**4** Revise the **Details** section in the Users tab as follows:

— From the **Screening Tables** pull-down menu, choose a call screening table.

— From the **Caller List Size** pull-down menu, select the maximum number of callers the user can enter.

— Under the **Ports Usage** section, check the **Parallel Search** box to enable parallel searches. Enter the maximum number of ports allowed in the search. This number cannot exceed the number of ports supported by the MIPCD card.

— To enable the **Call Reconnect** feature, check the **Re-origination Allowed** box. The conversations of users who choose this feature occupy two ports on the MIPCD card for the duration of the call.

**5** Click **Apply** to save the changes or click **Revert** to restore the original settings.

### Filter users

Use the **Filter** section to find and display a selected subset of users.

**1** Enter the appropriate name, user ID, or personal number in the **Text to find:** field.

**2** Choose the column to be searched from the **In Columns** pull-down menu.

**3** Click **Filter**. Matching entries display in the user table to the left.

**4** Click **Apply** to accept changes or **Revert** to restore original settings.

**5** Click **Show All** to display all the users on the MIPCD card.

### Reset user passwords

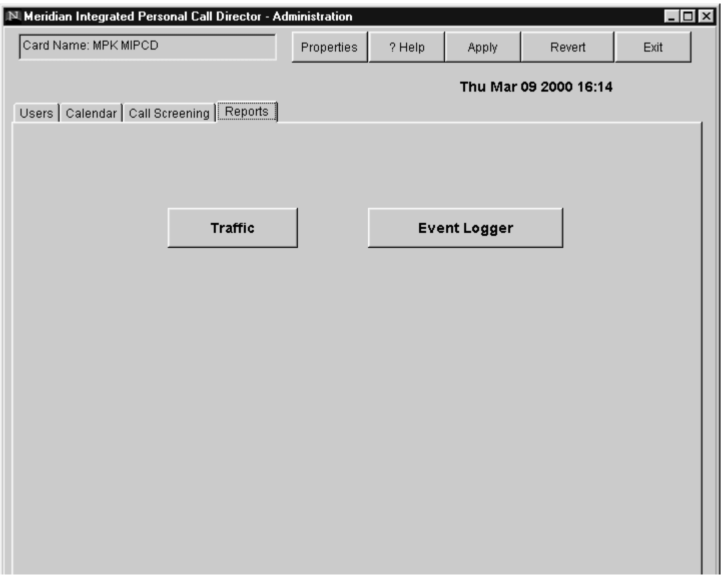
Click **Reset Password** to reset a user's password to the default password. The default is defined in the MIPCD **System Properties** window under the **Administration** tab.

If a user's password is disabled due to invalid login attempts, the password must be rest by the administrator.

# Traffic Reports description

To access Traffic Reports, click the **Reports** tab from the BUI **Main Administration** window. Use the **Reports** tab to view and analyze Traffic and Event Logger reports (see Figure 27). For a complete description of the traffic reports and the various categories counted as "pegs", see "Traffic data reports" on page 39.

**Figure 27**
**Main Traffic Reports window**



Card Name: MPK MIPCD

Thu Mar 09 2000 16:14

## View monthly Traffic Reports

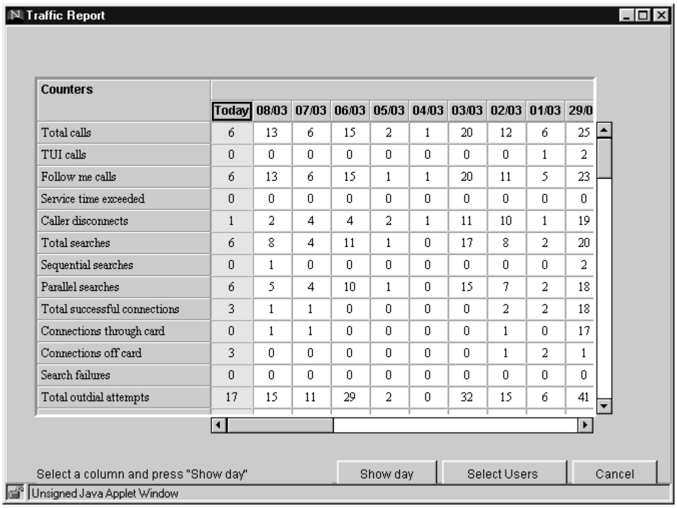
To view monthly Traffic Reports, click **Traffic** to display the **Traffic Report** window (see Figure 28). By default, the monthly reports appear first, once you click **Traffic**.

Traffic measurement files are generated and stored on the disk. One file is created and stored for each day. The file is updated every hour.

Monthly Traffic Reports include:

- Common traffic data
- User data for up to 50 selected users (scroll down to see the user data which is listed after all common report categories)

**Figure 28**
**Monthly Traffic Report window**



| Counters | Today | 08/03 | 07/03 | 06/03 | 05/03 | 04/03 | 03/03 | 02/03 | 01/03 | 29/0 |
|---|---|---|---|---|---|---|---|---|---|---|
| Total calls | 6 | 13 | 6 | 15 | 2 | 1 | 20 | 12 | 6 | 25 |
| TUI calls | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 2 |
| Follow me calls | 6 | 13 | 6 | 15 | 1 | 1 | 20 | 11 | 5 | 23 |
| Service time exceeded | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Caller disconnects | 1 | 2 | 4 | 4 | 2 | 1 | 11 | 10 | 1 | 19 |
| Total searches | 6 | 8 | 4 | 11 | 1 | 0 | 17 | 8 | 2 | 20 |
| Sequential searches | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 |
| Parallel searches | 6 | 5 | 4 | 10 | 1 | 0 | 15 | 7 | 2 | 18 |
| Total successful connections | 3 | 1 | 1 | 0 | 0 | 0 | 0 | 2 | 2 | 18 |
| Connections through card | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 17 |
| Connections off card | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 2 | 1 |
| Search failures | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total outdial attempts | 17 | 15 | 11 | 29 | 2 | 0 | 32 | 15 | 6 | 41 |

Select a column and press "Show day"

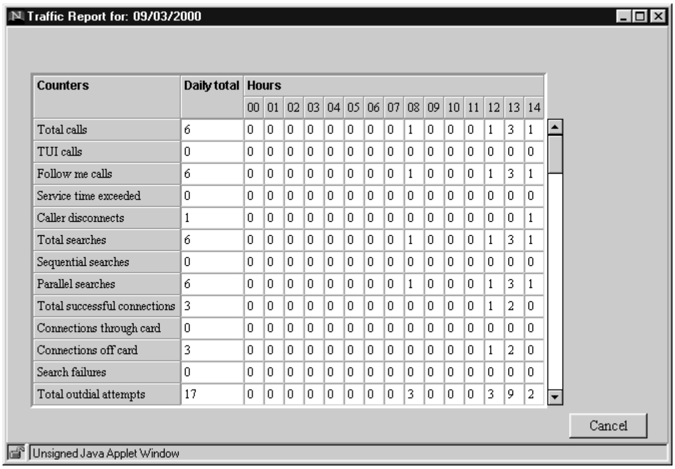
## View daily Traffic Reports

To view daily Traffic Reports, select an appropriate date column, and click **Show day** (see Figure 28).

The daily **Traffic Report** window appears (see Figure 29). This window displays the same data as the monthly report, but only for the chosen day. Data is broken down by hour.

Click **Cancel** to close the window and return to the monthly **Traffic Report** window.

**Figure 29**
**Daily Traffic Report window**



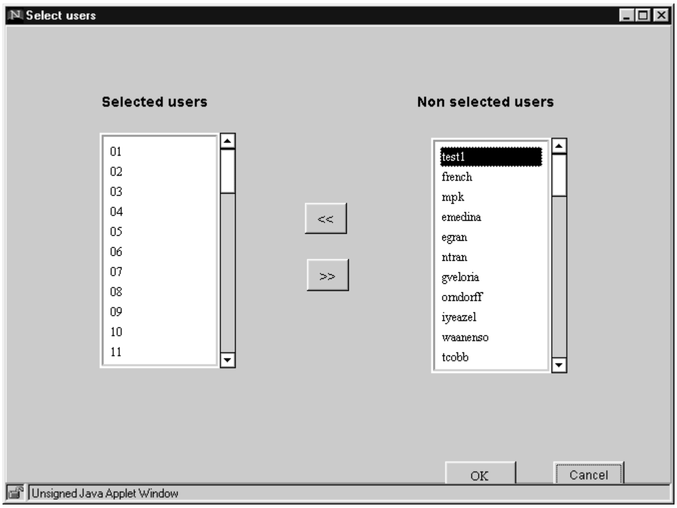
Traffic Report for: 09/03/2000

| Counters | Daily total | Hours | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 |
| Total calls | 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 3 | 1 |
| TUI calls | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Follow me calls | 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 3 | 1 |
| Service time exceeded | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Caller disconnects | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| Total searches | 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 3 | 1 |
| Sequential searches | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Parallel searches | 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 3 | 1 |
| Total successful connections | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 2 | 0 |
| Connections through card | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Connections off card | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 2 | 0 |
| Search failures | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total outdial attempts | 17 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 3 | 9 | 2 |

## User Traffic Data

The **User** section of the monthly and daily Traffic Reports displays data for a maximum of 50 users. To select the users to include in the daily and monthly reports, click **Select Users** in the monthly **Traffic Reports** window. The **Select Users** window appears (see Figure 30). To select or de-select a user for inclusion in the reports, click the username to highlight it, and then click the appropriate set of arrows.

**Figure 30**
**Select Users window**



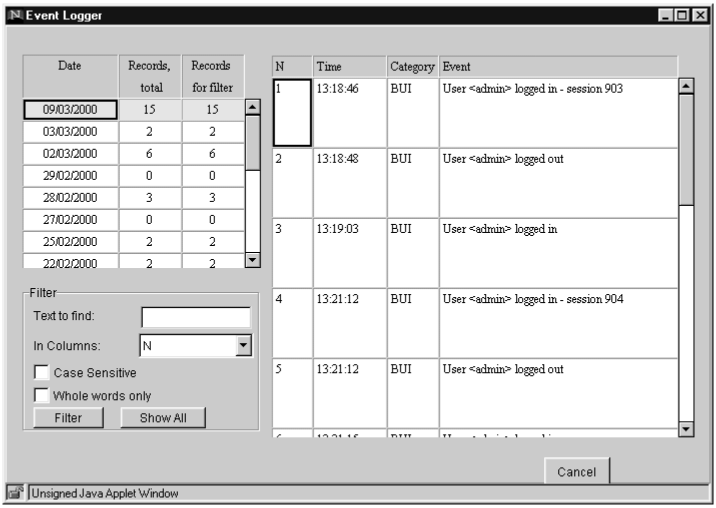
Click **OK** to accept selected entries or **Cancel** to go back to the monthly **Traffic Reports** window.

# Event Logger report description

Event Logger reports (see Figure 31) are a record of various activities in a single MICPD card. See “Call Process (CP) application reports” on page 42 for a description of those activities.

Events are recorded chronologically. One file (record) is saved per day.

**Figure 31**
**Event Logger window**



| Date | Records, total | Records for filter |
|---|---|---|
| 09/03/2000 | 15 | 15 |
| 03/03/2000 | 2 | 2 |
| 02/03/2000 | 6 | 6 |
| 29/02/2000 | 0 | 0 |
| 28/02/2000 | 3 | 3 |
| 27/02/2000 | 0 | 0 |
| 25/02/2000 | 2 | 2 |
| 22/02/2000 | 2 | 2 |

Filter

Text to find:

In Columns: N

☐ Case Sensitive

☐ Whole words only

| N | Time | Category | Event |
|---|---|---|---|
| 1 | 13:18:46 | BUI | User <admin> logged in - session 903 |
| 2 | 13:18:48 | BUI | User <admin> logged out |
| 3 | 13:19:03 | BUI | User <admin> logged in |
| 4 | 13:21:12 | BUI | User <admin> logged in - session 904 |
| 5 | 13:21:12 | BUI | User <admin> logged out |

Click **Cancel** to go back to the monthly **Traffic Reports** window.

## How to use Event Logger filter

Use the Event Logger filter to search for and display selected information contained in a Number, Category, Time or Event column for a specific date.

**1** In the **Event Logger** window, click on a date.

**2** In the **Text to find** field, enter the information you want to search for.

**3** In the **In columns** field, click the drop-down menu and select **N, Time, Category or Event**.

**4** Click **Case Sensitive** or **Whole words only** as required.

**5** Click **Filter**.

MIPCD searches for the text and displays the selected records. The number in the **Records for filter** column changes to reflect the number of records found in the search.

**6** Click **Show All** to return to the default Event Logger display.

# Maintenance

This chapter explains how to administer, troubleshoot, upgrade, and back up the MIPCD. Most of the maintenance and upgrade procedures detailed in this chapter are accomplished using the CLI.

## Log into the CLI Main Menu

Use Telnet or a serial emulation program to log in to the MIPCD CLI. Use the CLI to change passwords, backup, restore, upgrade the MIPCD and perform other administrative tasks.

If you use a terminal emulation program to access the CLI, configure the terminal to the settings listed below:

- Transmission speed: 9600 bps
- Data bits: 8
- Stop bit: 1
- Parity: No
- Flow control: none (do not use X-on/X-off flow control)

The login screen appears after you connect to the MIPCD card. The default login is **user**.

## Change or reset MIPCD CLI administration passwords

To change the default administrator password, do the following:

1. Access the MIPCD CLI with the default password **user**.
2. From the **Main Menu**, access the Password Editor (**PSweditor**) menu from the **Protected Administration** (**PAdmin**) menu.
3. Follow the instructions on the screen to change the default password.

### Example:

To modify the administrator passwords, the screen displays the following:

```
PSweditor, SWupgrade, ?: ps
Current Password:
admin: user
Modify, Save, Cancel: m
admin: newpassword
New password:
admin: newpassword
Modify, Save, Cancel: Save
Passwords have been updated.
PSweditor, SWupgrade, ?:
```

***Note 1:*** The maximum password length is 10 characters.

To reset a forgotten administrator password, do the following:

**1** Establish a serial connection directly to the MIPCD card adapter port. Enter the **rst** command when prompted.

**2** Follow the prompts to enter the MIPCD keycode.

**3** After MIPCD validates the keycode, MIPCD resets the password to the default **user**. The password is reset only if the keycode is correct.

**4** Log into the card and change the default password.

# CLI command description

This section describes the menus and commands most commonly used in MIPCD administration.

## System administration: SAdmin

- **SYstem**: Defines the card name, ACD settings, and IP address.

## System maintenance: SMaint

- **Archive Database (ARchivdb)**: Backs up the database from the active lower PCMCIA drive A: to a card in the upper drive B:. This command backs up only voice, data and report files, not application, firmware, or BUI. The MIPCD card must be disabled for this command.
- **Restore Database (REstordb)**: Restores the database from a backup disk in the upper PCMCIA drive B to the active lower PCMCIA drive A:. This command overwrites existing files with the same names. The MIPCD card must be disabled for this command.
- **Card Restart (CRestart)**: Use this command to reset the PCMCIA card after you restore the database.

## Directory PAdmin

- **Password Editor** (**PSweditor**): Allows modification of the CLI administrator password. This is the same password for FTP password access.
- **Functionality Upgrade** (**FUpgrade**): Allows modification of the number of ports being used on the card. To save the modification, a new key code must be inserted. The administrator is prompted to reset the card, because the card must be restarted for the change to take effect.
- **Software Upgrade** (**SWupgrade**): Used to upgrade the card firmware. The new firmware is copied from the upper PCMCIA drive B: to the active lower drive A:. New firmware takes effect after you restart the MIPCD. If the new firmware release is a major feature change, a new keycode is requested upon reset.

- **Administrator BUI Reset** (**ABreset**): Returns the administrator BUI password to its default value **admin**.
- **Screening Table Lock/Unlock** (**SCReen**): Used to “lock” or “unlock” screening tables. This prevents or allows their modification from BUI. This command has one parameter: **u** for unlock, **l** for lock. Type in **p** for print (prints current state). The default setting for screening tables is unlocked.

### Directory PMaint

- **PStatus**: Prints the MIPCD card’s port status.

### LOgout

- **LOgout**: Allows the user to log out of the CLI.

### ? Help

- **? Help**: Used to access the **Help** menu, which provides short explanations of the CLI commands.

## Backup or restore the MIPCD configuration database

When you back up the MIPCD configuration database, you do not have to re-enter the data when you upgrade the PCMCIA card. Use the *backup* procedure to back up the database from the active lower PCMCIA drive A: to a card in the upper drive B:. Use a PCMCIA ATA flash card (Type II and Type III cards) as the target backup disk. Be sure you select a backup disk with enough space to store the entire database. The backup procedure backs up only voice, data, and report files, not application, firmware, or BUI files. Disable the MIPCD card for this procedure.

> ***Note:*** If the target backup PCMCIA flash card memory is too small to accept the entire database, the CLI displays an error indicating that there is not enough memory.

**1** Disable the MIPCD using LD 32.

**2** Place a PCMCIA disk in the secondary drive B: of the first MIPCD.

**3** Type the **SMaint (SM)** command.

**4** Type **AR** (**Archive Database** command) and follow the prompts.

**5** Type **CR** to restart the MIPCD.

**6** Enable the MIPCD using LD 32.

### Example:

```
MReport, ARchivdb, REstordb, CRestart, ?: AR
Backup Database? (Yes, (No)) Y
Please wait, performing backup... completed.
MReport, ARchivdb, REstordb, CRestart, ?: CR
```

Use the procedure below to restore the customer database to the MIPCD PCMCIA card in the lower PCMCIA drive A:. The files from the backup PCMCIA card in upper drive B are copied to the active PCMCIA card in the lower drive A:. Filenames are restored are specified in the DB Description file.

**1** Place the backup PCMCIA disk in the MIPCD secondary drive B:.

**2** Type the **SMaint** (**SM**) command to access the **System Maintenance** menu.

**3** Type **RE** for the **Restore Database** command and follow the prompts.

### Example:

```
MReport, ARchivdb, REstordb, CRestart, ?: RE
Restore Database? (Yes, (No)) Y
Please wait, performing restore... completed.
MReport, ARchivdb, REstordb, CRestart, ?: CR
```

# Upgrade the firmware or voice files

The firmware and voice files needed for MIPCD operation are stored on a PCMCIA card in lower drive A:. This card must be installed before the software upgrade command is executed.

A card with the new files is inserted into the upper drive B:. Those files are then copied onto drive A:. The old files are overwritten.

- **Voice files (language set)**: To add a new language, all necessary voice files must also be copied before the MIPCD card is reset. If the necessary language directory is not loaded, the language is unavailable.
- **Firmware**: When the firmware upgrade includes a functionality change, a new keycode file must also be transferred. The administrator can also enter the keycode through the CLI.

To upgrade the firmware or voice files, do the following:

**1** Insert the PCMCIA flash card with the new files into the top PCMCIA drive B:. The PCMCIA card must still be installed in the lower PCMCIA drive A:.

**2** Enter **PAdmin (PA)** to access the **Software Upgrade** menu.

**3** Follow the steps outlined in the example below.

```
PSweditor, SWupgrade, ?: SW
software release: 03, issue: 07
Modify, Save, Cancel: M
Modify software? (Yes, (No)) Y
Modify, Save, Cancel: S
Installation of software in progress...
New s/w will be used following MIPCD restart.
Restart MIPCD? (Yes, (No)) Y
PSweditor, SWupgrade, ?:
```

**4** After the upgrade is complete, remove the PCMCIA card from the upper PCMCIA drive B:.

***Note 1:*** Because all upgrades (except voice files) are enabled by keycode, the new keycode file must also be transferred. The keycode can also be entered through the CLI.

***Note 2:*** Restart the MIPCD to load the new firmware. The exception is for voice files, which do not require you to restart the card.

# View maintenance reports

Maintenance reports are used to analyze system problems based on error messages compiled for a specified date. Use the **MReport** command to access these reports.

The selected date must be in the past, not future. Old files that exceed the report aging number of days are discarded. If a date entered is too old, an error message is displayed. If the date is within the correct date range, but there are no report entries for that day, a message indicating there are no entries is displayed.

**1** Enter **sm** or **SM** or the full command (**SMaint**) to access the **System Maintenance** menu from the **Main Menu**.

**2** Follow the instructions as shown in the example below.

**Example:** Display the maintenance report for March 15, 1996.

```
STest, MReport, SCon, ARchivdb, REstordb, CRestart, ?: mr
year(1996): 1996
month (11): 03
day (22): 15
1234:timer101 ch01 16:16:18:111 9000 “Num: 100 Timing Stop. 00.”
1235: sig100 ch00 16:17:05:234 9900 “SIG: Q_APP in msg:0000005A”
0001:HW PCMCIA001 ln0077 ch01 16:25:29:836 PCMCIA card
inserted in socket 1
year (1996): .
STest, MReport, SCon, ARchivdb, REstordb, CRestart, ?:
```

**3** To exit the report, enter “**.**” (dot); to interrupt the report display, and enter ***<cr>** (asterisk and press **Enter**).

***Note:*** All reports are time-stamped and contain information regarding the cause of the problem. After the data is displayed, the system returns to the *year-month-day* prompt using the last selected date as default.

### Report format

The maintenance reports have the following format:

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

## Identify the card type in the field

In the Meridian 1, the contents of the ID EEPROM is displayed by the **IDC** command in Overlay 32. MIPCD has a specific NT code burned in its ID EEPROM. The contents of this EEPROM can be read by the core software.

## Replace the MIPCD card

To replace an MIPCD card, do the following:

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

**2** Remove the faulty MIPCD card.

**3** Remove all PCMCIA cards from the faulty MIPCD card. Insert the PCMCIA card(s) into the replacement MIPCD card. The keycode installed on the original PCMCIA card is reused.

**4** Transfer the Security Device from the faulty MIPCD card to the replacement.

**5** Locate the card slot for installation of the replacement MIPCD card.

Table 10 lists the Meridian 1 module slots suitable for MIPCD installation.

**Table 10**
**MIPCD installation by PE type**

| Meridian 1 modules | MIPCD card slots |
|---|---|
| NT8D37BA/EC IPE modules, NT8D11BC/ED CE/PE modules | All available IPE card slots. |
| NT8D37AA/DC IPE modules | 0, 4, 8, and 12 |

**6** Pull the top and bottom latches away from the MIPCD faceplate.

**7** Insert the replacement MIPCD card into the card guides. Gently push the card until it makes contact with the backplane connector.

**8** Push the top and the bottom latches towards the faceplate to insert and lock the card into the faceplate connector.

**9** To enable the MIPCD card, load the Network and PE Diagnostic program LD 32. Type the **ENLC l s c** command, where **l** is the loop, **s** is the module or shelf, and **c** is the card to be enabled.

# Diagnostic tools

Use the diagnostic tools to troubleshoot problems with the MIPCD. More than one of these tools can be used to diagnose a problem.

System diagnostic tools include the following:

- LED indicators
- Sanity monitoring
- Overlay commands

## LED indicators

The LED indicator at the top of the MIPCD faceplate indicates the status of the card.

- If the MIPCD card functions correctly during start up, the LED blinks three times and stays ON.
- If the MIPCD card does **not** function correctly during start up, the LED turns ON and stays ON without blinking.
- The LED turns OFF when the card is software enabled.
- If the LED stays ON when the card is software enabled, the card is faulty or disabled.

## Sanity monitoring

Sanity monitoring is a background routine that checks the operation of system resources, such as CPU activity and memory allocation.

- If the system performance has degraded to an unacceptable level, this background routine attempts to restore normal system operation.
- If normal operations cannot be restored, this routine resets the system.
- If the system reset is not effective, a full-board level reset is initiated.
- If the board level reset is unsuccessful, the maintenance LED stays ON.

## Overlay commands

The Meridian 1 recognizes the MIPCD card as an Extended Digital Line card. All relevant system maintenance commands for an Extended Digital Line card are used with MIPCD (see Table 11).

Meridian 1 diagnostics are performed for every card as part of the daily routines. See *Meridian 1 system maintenance* (553-3001-520) for more information.

**Table 11**
**Commands to enable/disable MIPCD channels**

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

Use LD 32 to enable and disable ACD digital telephone set M2616.

## MIPCD fault isolation and correction

MIPCD faults are cleared with the same procedures as other IPE cards. Refer to *Meridian 1 fault clearing* (553-3001-510) for more information.

Table 12 details service problems specific to MIPCD cards. Use the two test procedures below to resolve these problems. Also refer to *X11 Administration* (553-3001-311) for a list of messages and their description. Based on the code’s description, take the appropriate action to resolve the problem.

If the problem is not resolved after all available diagnostic tools and test procedures are attempted, make a list of all the symptoms and contact the field service representative.

**Table 12**
**MIPCD equipment problems**

| **Symptoms** | **Diagnosis** | **Solution** |
|---|---|---|
| Red card LED on the MIPCD is permanently on. | Card is disabled or faulty. | Check the card status. |
| Display on the controller card shows fault codes. | Card faulty, failed self-test or communication problem with peripheral equipment. | Go to *Reset MIPCD card command*.<br>Refer to *X11 Administration* (553-3001-311) for a list of codes. |
| Error messages printed on the terminal or the Meridian 1 TTY. | Hardware or software problems with the MIPCD. | Note various error messages. Refer to *X11 Administration* (553-3001-311) for a list of these messages and their description. Based on the code's description, take the appropriate action to resolve the problem. |

## Reset MIPCD card command

1. Software sends a reset message to the card if no channels are busy.
2. The card sets all appropriate resources to a disabled state and turns on the faceplate LED.
3. The MIPCD card resets.
4. The card LAN polls the card.
5. Card LAN requests configuration data.
6. The card returns configuration data (card type, X11 signaling type, and TN mapping Type 2) and enables the DS-30X link.
7. Card LAN enables the DS-30X signaling channel.
8. The MIPCD card waits until the configuration data (trunk type, signaling type, and balance impedance) is received via the DS-30X. The data is then discarded.
9. The card enters its main program loop.

# Hardware descriptions

## MPU

The Micro Processor Unit (MPU) is the QUad Integrated Communications Controller (QUICC) MC68EN360 running at 25 MHz. The MPU is using a 128 Kbytes boot flash, downloading the firmware from the PC card to a 16 Mbytes Dynamic Random-Access Memory (DRAM). The communication to the card LAN and the Ethernet controller is done by the Serial Communication Channels (SCCs) and the maintenance port by the Serial Management Controller (SMC). The interfaces to the DS-30X is done by access to a voice memory buffer.

## Digital Signal Processor (DSP)

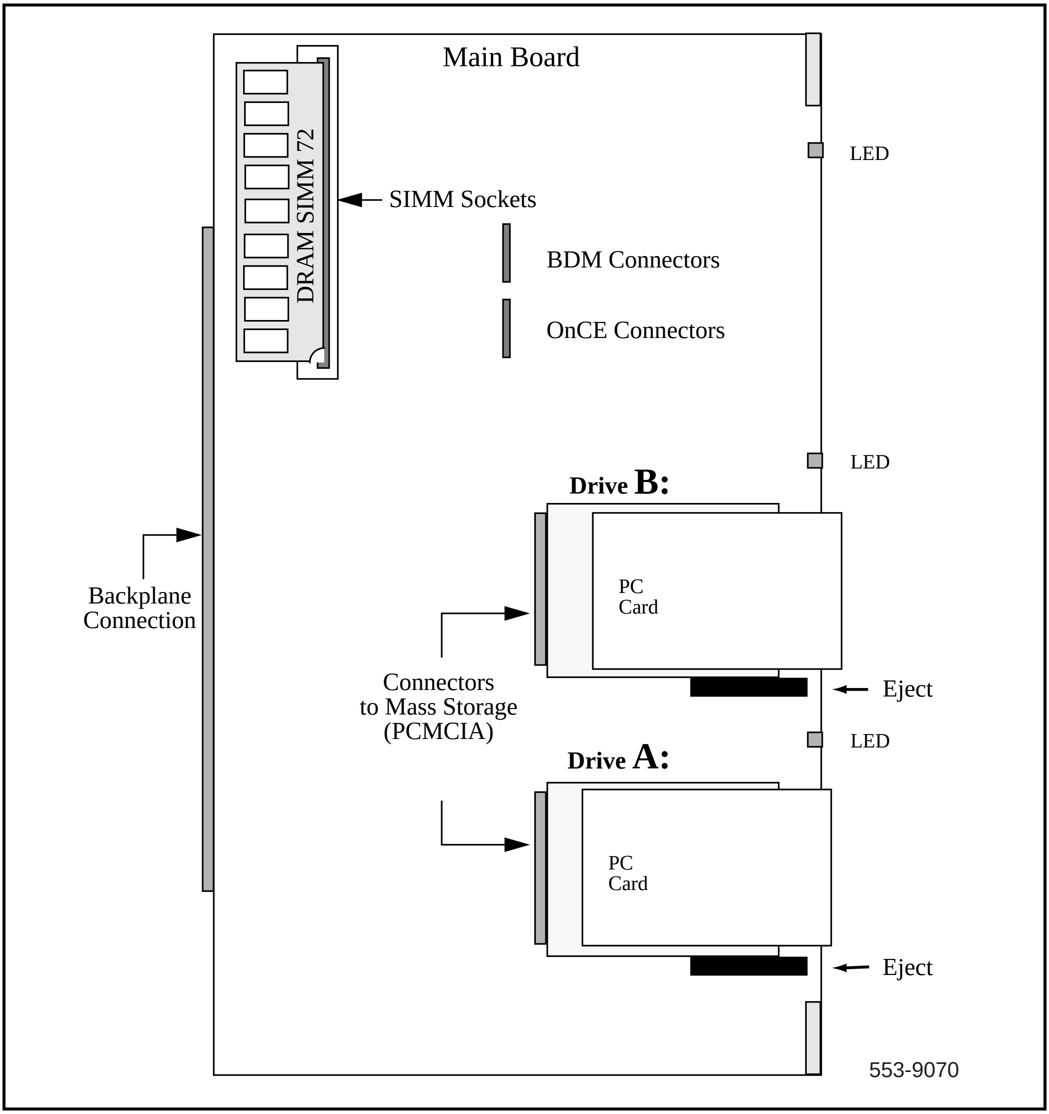
The DSP is a Motorola 56002 running at 66 MHz. The DSP has access to fast local memory. This memory is divided into program memory and two data memory areas. It also has access to a voice memory buffer, which is used to interface the DSP to the DS-30X. The DSP communicates with the MPU via a Host Interface (HI), and another set of memory buffers.

## PCMCIA specifications

The mass storage interface is a PC card-compatible 520-MegaByte disk used to store the voice prompts and the MPU and DSP firmware. The MPU communicates with the PC card through a CL-PD6720 (CIRRUS LOGIC PCMCIA host adapters). MIPCD has two PCMCIA sockets.

The lower disk drive (drive A:) is the main operation disk. It contains firmware files, database files, log files, and voice prompt files. It must always be present. The upper disk (drive B:) is used for upgrades and backup. It can be removed when not in use.

**Figure 32**
**MIPCD side view**



# Appendix A: Maintenance terminal cable pin assignments

Table 1 lists the pin assignments for the maintenance terminal cable that connects the IPE module I/O panel connector to the null modem for direct terminal connection. Use this table to connect a modem for a remote maintenance terminal connection.

**Table 1**
**A0660348 maintenance cable (Part 1 of 2)**

| J2 Pin Number (DB 25-pin Connector) | J1 Pin Number (50-pin I/O Panel Connector) | Description |
|---|---|---|
| 1 | 25 | Reserved |
| 2 | 22 | RS-232 Tx |
| 3 | 20 | RS-232 Rx |
| 4 | 18 | Reserved |
| 5 | 10 | Reserved |
| 6 | 16 | Reserved |
| 7 | 21 | GND |
| 8 | 17 | Reserved |
| 9 | 11 | Reserved |
| 10 | 24 | LAN_Tx+ |
| 11 | 49 | LAN_Tx- |

**Table 1**
**A0660348 maintenance cable (Part 2 of 2)**

| J2 Pin Number (DB 25-pin Connector) | J1 Pin Number (50-pin I/O Panel Connector) | Description |
|---|---|---|
| 12 | 12 | Reserved |
| 13 | 23 | LAN_Rx+ |
| 14 | 48 | LAN_Rx- |
| 15 | 13 | Reserved |
| 16 | 14 | Reserved |
| 17 | 15 | Reserved |
| 18 | 36 | Reserved |
| 19 | 37 | Reserved |
| 20 | 19 | Reserved |
| 21 | 38 | Reserved |
| 22 | 39 | Reserved |
| 23 | 40 | Reserved |
| 24 | 41 | Reserved |
| 25 | N.C. | Not Connected |

# NT5D52AB/BB Ethernet adapter pinout

**Table 2**
**NT5D52AB/BB Ethernet adapter pinout**

| Connector | Pin | Description |
|---|---|---|
| 9-pin for CRT | 2 | RS-232 TX |
| | 3 | RS-232 RX |
| | 5 | GND |
| RJ-45 Ethernet | 1 | LAN_TX + |
| | 2 | LAN_TX - |
| | 3 | LAN_RX + |
| | 6 | LAN_RX - |

# Appendix B: Product integrity

This chapter contains information on

- "Reliability" on page 117
- "Environment specifications" on page 117
- "Electrical regulatory standards" on page 119

## Reliability

The MIPCD card Mean Time Between Failure (MTBF) is better than 20 years.

## Environment specifications

Measurements of performance in regards to temperature and shock were made under test conditions as described in Table 13.

The MIPCD pack is capable of withstanding the following environmental conditions without any performance degradation or damage. The phrase "short term" means 72 consecutive hours with a maximum of 15 days per year. The temperatures indicated in Table 13 are used for the environment of the circuit pack and not for the total system. The following environmental parameters are affected by the presence of the PCMCIA disk (Viper 8340PA of INTEGRAL). The card without the disk has better performance.

## Temperature-related conditions

Table 13 displays the acceptable temperature and humidity ranges for the MIPCD.

**Table 13**
**MIPCD environmental specifications**

| Specification | Minimum | Maximum |
|---|---|---|
| ***Normal Operation*** | | |
| Operating temperature | 0° C | 45° C |
| Short-term operating temperature | 0° C | 50° C |
| Relative humidity | 5% to | 90% (non-condensing) |
| Rate of change | Less than 1° C per three minutes | |
| ***Storage*** | | |
| Relative Humidity | 5% | 95% (non-condensing) |
| Temperature | -40° C to +70° C, non-condensing | |
| ***Temperature Shock*** | | |
| In three minutes | -40° C | 25° C |
| In three minutes | 25° C | 70° C |
| | -40° to 70° C, non-condensing | |

# Electrical regulatory standards

The following three tables list the safety and electromagnetic compatibility regulatory standards for the MIPCD by geographic region. Specifications for the MIPCD meet or exceed the standards listed in these regulations.

## Safety

Table 14 lists the safety regulations met by the MIPCD by country/region.

**Table 14**
**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, TS00–TS004, TS006 | Safety/Network (Australia) |
| JATE | Safety/Network (Japan) |

## Electromagnetic compatibility (EMC)

Table 15 lists electromagnetic emissions regulations met by the MIPCD card.

**Table 15**
**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 16 lists electromagnetic immunity regulations met by the MIPCD card.

**Table 16**
**Electromagnetic immunity**

| **Regulation Identifier** | |
|---|---|
| CISPR 22 Sec. 20 Class B | I/O conducted noise |
| IEC 801-2 (level 4) | ESD (Basic Standard) |
| IEC 801-3 (level 2) | Radiated Immunity (Basic Standard) |
| IEC 801-4 (level 3) | Fast transient/Burst Immunity (Basic Standard) |
| IEC 801-5 (level 4, preliminary) | Surge Immunity (Basic Standard) |
| IEC 801-6 (preliminary) | Conducted Disturbances (Basic Standard) |
| BAKOM SR 784.103.12/4.1/1 | EMC/Safety (Switzerland) |
| SS-447-20-22 | Sweden EMC standard |
| AS/NZS 3548l | EMC (Australia/New Zealand) |
| NFC 98020 | France EMC standard |

# List of Terms

**ACD**

Automatic Call Distribution

**AS**

American Standard

**ASIC**

Application Specific Integrated Circuit

**ATA**

Analog Terminal Adapter

**AVTS**

Application Voice & Tone Server

**BUI**

Browser User Interface

**BUS**

Broadcast and Unknown Server

**CALA**

Caribbean and Latin America

**CCITT**

The International Telegraph and Telephone Consultative Committee

**CDR**

Call Detail Recording

| | |
|---|---|
| **CE** | Common Equipment |
| **CE-MUX** | Common Equipment MUltipleXed |
| **CFXA** | Call Forward eXternal Allow |
| **CLI** | Command Line Interface |
| **CLID** | Calling Line IDentification |
| **CO** | Central Office (Public Switch) |
| **CP** | Call Processor |
| **CPU** | Central Processing Unit (Main Processor) |
| **CRT** | Continuous Ring Tone |
| **CSA** | Canadian Standards Association |
| **dB** | Decibel |
| **dBm** | Decibel (w.r.t) Milliwatt |
| **DID** | Direct Inward Dialing (from CO to PABX) |

**DIP**

Dual In-Line Package

**DMA**

Direct Memory Access

**DN**

Directory Number

**DRAM**

Dynamic Random-Access Memory

**DS-30X**

A 32-time slot (10 bits per time slot, 8000 time slots per second) link between the controller and IPE peripheral cards, serving both for voice connections and signaling connection to the CPU

**DSP**

Digital Signal Processor

**DTMF**

Dual-Tone Multi-Frequency

**EEPROM**

Electrically Erasable Programmable Read-Only Memory device

**EES**

End-to-End Signaling

**EMC**

Electromagnetic Compatibility

**ESD**

Electro-Static Discharge

**ESN**

Electronic Switched Network

**FCC**

Federal Communications Commission

**FTP**

File Transfer Protocol

**GUI**

Graphical User Interface

**HI**

Host Interface (for example, DSP56002)

**ID**

IDentification

**INI**

INItialization

**IEC**

International Electro-Technical Commission; based in Geneva, Switzerland

**I/F**

Interface

**I/O**

Input/output

**IP**

Internet Protocol (layer of TCP/IP)

**IPE**

Intelligent Peripheral Equipment (i.e. Viking)

**LAN**

Local Area Network

**LCA**

Logic Cell Array

**LED**

Light Emitting Diode

**OOS**

Out of Service

**Option 11**

Meridian 1 small system, with different architecture than the large system

**Mbps**

Megabits per second

**Mbyte**

1,048,576 megabytes

**MDF**

Main Distribution Frame

**MIPCD**

Meridian Integrated Personal Call Director

**MMI**

Man-Machine Interface

**MPU**

Micro Processor Unit on cards (not the CPU)

**MSD**

Mass-Storage Device, e.g., a disk

**MTBF**

Mean Time Between Failure

**NEBS**

Network Equipment Building System

**NFC**

New Flexible Code

**NTP**

Nortel Networks technical publication

**OA&M**

Operation, Administration, and Maintenance

**PBX**

Private Branch Exchange

**PC**

Personal Computer

**PCI**

Present Call Information

**PCM**

Pulse Coded Modulation

**PCMCIA**

PC Memory Card International Association

**PE**

Processor Element

**PGA**

Pin Grid Array

**PRD**

Product Requirements Document

**RISC**

Reduced Instruction Set Computer

**ROM**

Read-Only Memory

**R/W**

Read-Write

**SCC**

Serial Communication Channel

**SIMM**

Single In-Line Memory Module

**SMT**

Surface Mounting Technology

**SOS**

Support Operating System/Switch Operating System

**SR**

Service Request

**SRAM**

Static Random Access Memory

**SSD**

Signal Scan & Distribution; the generic name for messages from the MSL-1 CPU and Peripheral Equipment cards

**TCM**

Time Compression Multiplexing

**TN**

Terminal Number

**TCP/IP**

Transmission Control Protocol / Internet Protocol.

**TTY**

Teletypewriter

**TUI**

Telephony User Interface

**UART**

Universal Asynchronous Receiver/Transmitter

**UI**

User Interface

### User

An MIPCD user; the MIPCD administrator defines the list of users

### XDLC

eXtended Digital Line Card

### XPEC

eXtended Peripheral Equipment Controller

### XT

eXtended Tone

### XUS

X-Calibur Universal Server; an IPE card for tone and announcement services, developed by Telrad

### X12

Signalling mechanism between XDLC and XPEC

# Index

Meridian 1

# Meridian Integrated Personal Call Director

Description, installation, administration, and maintenance

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant. This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC rules, and the radio interference regulations of Industry Canada. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense. Meridian 1 is a trademark of Nortel Networks.

Publication number: 553-3001-117
Document release: Standard 2.00
Date: April 2000
Printed in Canada

NORTEL NETWORKS
How the world shares ideas.