HOTWIRE DSLAM FOR 8540 AND 8546 DSL CARDS

USER'S GUIDE

Document No. 8000-A2-GB20-20

PARADYNE™

Notice

Warranty, Sales, and Service Information

Contact your sales or service representative directly for any help needed. For additional information concerning warranty, sales, service, repair, installation, documentation, or training, use one of the following methods:

- **Via the Internet:** Visit the Paradyne World Wide Web site at http://www.paradyne.com
- **Via Telephone:** Call our automated call system to receive current information via fax or to speak with a company representative.
  - — Within the U.S.A., call 1-800-870-2221
  - — International, call 813-530-2340

Trademarks

Printed on recycled paper

Contents

3 Initial Setup Instructions

4 Configuring the HotWire DSLAM

5 MCC Card Configuration

6 DSL Card Configuration

7 Monitoring the HotWire DSLAM

8 Diagnostics and Troubleshooting

A Checklist for Setting Up User Accounts on the MCC and DSL Cards

B Checklist for Setting Up SNMP Features

About This Guide

Document Purpose and Intended Audience

This guide describes how to configure and operate the software component of the HotWire Digital Subscriber Line Access Multiplexer (DSLAM) system. It is intended for administrators and operators who maintain the networks that support HotWire operation.

A basic understanding of internetworking protocols and their features is assumed. Specifically, you should have familiarity with Simple Network Management Protocol (SNMP), Network Management Systems (NMSs), and the following internetworking concepts:

- TCP/IP applications
- IP and subnet addressing
- IP routing (also referred to as IP forwarding)

It is also assumed that you have already installed either the HotWire 8600 or 8800 DSLAM. If you have not done so already, refer to the appropriate HotWire DSLAM Installation Guide for installation instructions.

NOTE:

It is highly recommended that you read the *HotWire DSLAM for 8540 and 8546 DSL Cards Network Configuration Guide.* before you begin to use this guide and the HotWire software. The *HotWire DSLAM for 8540 and 8546 DSL Cards Network Configuration Guide* provides introductory information about the HotWire DSLAM network model and theories.

Document Summary

Section	Description
Chapter 1	*HotWire DSLAM System Description.* Provides an overview of the HotWire 8600 and 8800 systems.
Chapter 2	*HotWire Menus and Screens.* Describes the operation of HotWire menus, screens, and commonly used navigation keys. Also provides instructions on how to log in and log out of the system.
Chapter 3	*Initial Setup Instructions.* Provides instructions on how to access the system for the first time, as well as instructions on performing initial setup tasks.
Chapter 4	*Configuring the HotWire DSLAM.* Describes the required procedures for configuring the HotWire system.
Chapter 5	*MCC Card Configuration.* Describes the optional procedures for configuring the MCC card on the HotWire system.
Chapter 6	*DSL Card Configuration.* Describes the optional procedures for configuring the DSL cards on the HotWire system.
Chapter 7	*Monitoring the HotWire DSLAM.* Describes operator programs that monitor the HotWire system.
Chapter 8	*Diagnostics and Troubleshooting.* Describes common HotWire operational problems and solutions.
Appendix A	*Checklist for Setting Up User Accounts on the MCC and DSL Cards.* Describes user accounts and how to set them up on the MCC and DSL cards.
Appendix B	*Checklist for Setting Up SNMP Features*. Describes how to set up SNMP features.
Appendix C	*Download Code and Apply Download.* Describes how to work with the Download Code and Apply Download menus.
Appendix D	*Navigation Keys*. Describes the keys that are used to navigate the HotWire system.
Appendix E	*Traps.* Describes the traps that are generated by the HotWire system.
Appendix F	*5446 RTU Setup*. Describes MIB details including the Injection MIB and other enterprise MIBs.
Appendix G	*Static Route Warning Messages.* Describes warnings and error messages displayed on the Static Routes screen.

Section	Description
Glossary	Defines acronyms and terms used in this document.
Index	Lists key terms, acronyms, concepts, and sections in alphabetical order.

Product-Related Documents

Document Number	Document Title
5020-A2-GN10	*HotWire POTS Splitter Central Office Installation Instructions*
5030-A2-GN10	*HotWire 5030 POTS Splitter Customer Premises Installation Instructions*
5034-A2-GN10	*HotWire 5034 POTS Splitter Customer Premises Installation Instructions*
5216-A2-GN10	*HotWire 5216 Remote Termination Unit (RTU) Customer Premises Installation Instructions*
5246-A2-GN10	*HotWire 5246 Remote Termination Unit (RTU) Customer Premises Installation Instructions*
5446-A2-GN10	*HotWire 5446 Remote Termination Unit (RTU) Customer Premises Installation Instructions*
7700-A2-GB23	*DCE Manager for HP OpenView for Windows User's Guide*
7800-A2-GB26	*DCE Manager User's Guide*
8000-A2-GB21	*HotWire DSLAM for 8540 and 8546 DSL Cards Network Configuration Guide*
8000-A2-GN11	*HotWire Management Communications Controller (MCC) Card Installation Instructions*
8540-A2-GN10	*HotWire 8540 Digital Subscriber Line Access (DSL) Card Installations Instructions*
8546-A2-GN10	*HotWire 8546 Digital Subscriber Line (DSL) Card Installation Instructions*
8600-A2-GN20	*HotWire 8600 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide*
8800-A2-GN21	*HotWire 8800 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide*

Contact your sales or service representative to order additional product documentation.

HotWire DSLAM System Description

1

What is the HotWire DSLAM?

The HotWire Digital Subscriber Line Access Multiplexer (DSLAM) is a DSL platform, which houses 18 DSL cards (8540 DSL cards, 8546 DSL cards, or a combination of both). The DSLAM interoperates with multiple types of HotWire Remote Termination Units (RTU) to deliver applications at multimegabit speed in support of packet services over a Digital Subscriber Line (DSL) link.

The 8540 DSL card interoperates with the following HotWire RTUs:

- 5170 RTU
- 5171 Remote PC Network Interface Card (NIC)
- 5216
- 5246 RTU

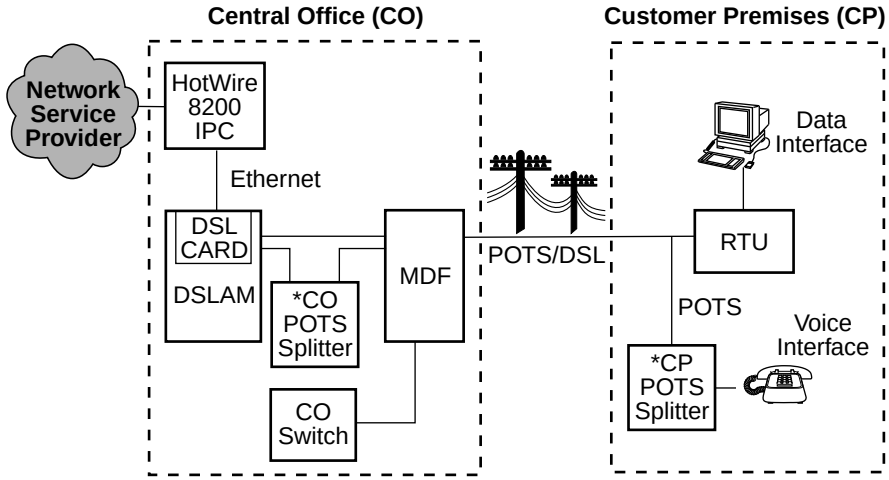
The 8546 DSL card interoperates with the following HotWire RTU:

- 5446 RTU

High-speed service traffic types from the DSL links are groomed and then concentrated for efficient forwarding to backbone routers. By enabling very high speeds using DSL technology and then concentrating Internet Protocol (IP) traffic, greater performance is realized. Backbone service nodes can be placed deeper into the network, dramatically improving the economics of service provisioning while taking advantage of the substantial speed increases of DSL.

In addition, the HotWire DSLAM with a HotWire RTU can be multiplexed with Plain Old Telephone Service (POTS) over the same copper line providing simultaneous usage of POTS and digital applications. That is, the optional POTS splitters (HotWire 5020 Central Office POTS Splitter and HotWire 5030 or 5034 Customer Premises POTS Splitter) allow simultaneous voice and data connections over a standard telephone line.

The following illustration shows a typical HotWire configuration connection using either an 8540 or 8546 DSL card in the DSLAM to a HotWire 5170, 5171, 5216, 5246, or 5446 RTU.



Legend: DSL - Digital Subscriber Line RTU - Remote Termination Unit
MDF - Main Distribution Frame POTS - Plain Old Telephone Service
IPC - Interworking Packet Concentrator

* Optional

97-15674-01

HotWire DSLAM Components

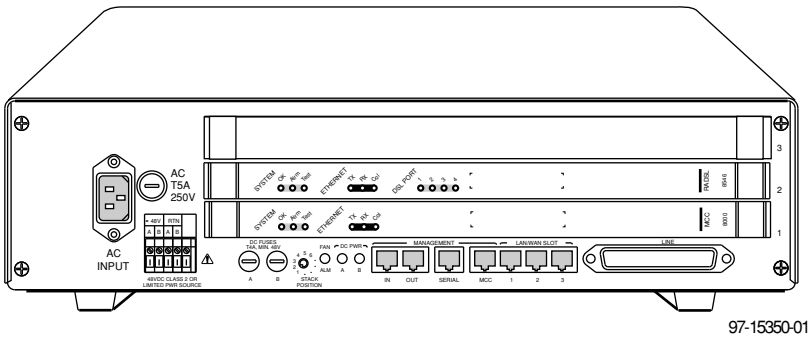
The HotWire DSLAM system consists of the following components:

- **HotWire DSLAM chassis**

  There are two types of chassis:

  — Each HotWire 8600 DSLAM is an independent, standalone system. The stackable design provides for up to six systems to share management access through a single Management Communications Controller (MCC) card, which in turn, allows an additional slot for a DSL card in each of up to five additional systems.

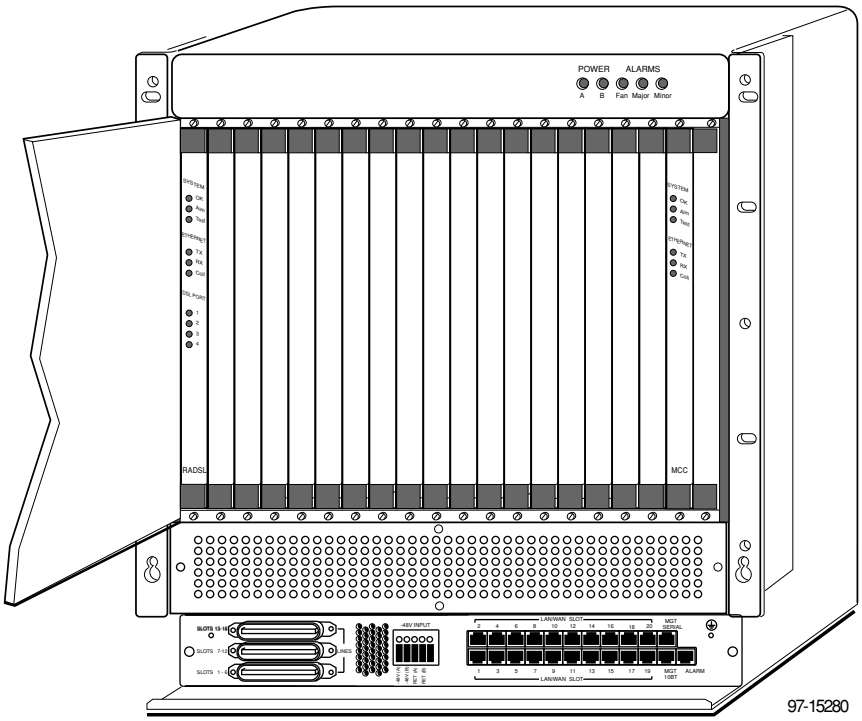
  In a stacked configuration, the first, or base chassis, must contain an MCC card in Slot 1. In addition to the MCC card, the base chassis can house up to two DSL cards. Each additional chassis in the stack houses up to three DSL cards.



97-15350-01

For more information about the HotWire 8600 DSLAM chassis, see the *HotWire 8600 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide*.

— The HotWire 8800 DSLAM chassis is a 20-slot chassis designed to house up to 18 DSL cards and one MCC card. (The remaining slot is reserved for future use.)



For more information about the HotWire 8800 DSLAM chassis, see the *HotWire 8800 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide*.

- **One Management Communications Controller (MCC) card**

  The chassis requires one MCC card, which is a processor card that administers and provides diagnostic connectivity to the DSL cards. It acts as a mid-level manager and works in conjunction with a Simple Network Management Protocol (SNMP) system, such as Paradyne's DCE Manager for HP OpenView, via its LAN port. It gathers operational status for each of the DSL cards and responds to the SNMP requests. It also has a serial port for a local user interface to the DSLAM.

- **At least one Digital Subscriber Line (DSL) card**

  The chassis requires at least one DSL card, which is a circuit card that contains four Rate Adaptive Digital Subscriber Line (RADSL) modem ports, an Ethernet interface to the ISP, and a processor/packet forwarder. The processor/packet forwarder controls the modems and forwards the packet traffic via the Ethernet and DSL interfaces. When the 8600 DSLAM chassis is fully populated, it provides a total of 68 RADSL modem ports. When the 8800 DSLAM chassis is fully populated, it provides a total of 72 RADSL modem ports.

Features

The HotWire DSLAM system provides the following features:

- High speed Internet or Intranet access.
- Rate Adaptive Digital Subscriber Line ports.
- Subscriber authentication and security access and permission features that prevent users from accessing unauthorized services.
- Status polling, alarm indicators and logging, diagnostics, and performance capabilities.
- Primary network management support via SNMP agent for monitoring and traps; telnet for configuration and diagnostics.
- Dynamic IP addressing, allowing Network Service Providers the ability to reuse IP addresses.

Levels of Access

There are two levels of diagnostic/administrative access in the HotWire DSLAM system:

- **Administrator**

  The Administrator has complete read/write access to the DSLAM system. With Administrator permission, you can set specific parameters and variables to configure cards, ports, interfaces, user accounts, next hop routes, and SNMP security.

- **Operator**

  The Operator has read-only access. With Operator permission, you can view card status, physical layer status, interfaces, and Internet Protocol (IP) routes, and run non-disruptive tests.

HotWire DSLAM Software Functionality

Depending upon your system access, you can:

- Configure the system,
- Monitor the system, and/or
- Run applications and diagnostic tests to troubleshoot the network

Configuring the System

The HotWire DSLAM software provides configuration submenu options to:

- Configure the MCC card, DSL cards, and RTU connectivity
- Configure the interfaces and ports
- Set up user accounts
- Upload or download a copy of a card's configuration data to or from a Trivial File Transfer Protocol (TFTP) server
- Download a new version of the DSLAM software
- Define an IP routing table
- Define and enable filters to prevent unauthorized network access
- Configure the SNMP agent to send traps to a specific SNMP NMS manager

NOTE:

You must have administrator permission to configure the system. For more information about configuring the system, see Chapters 4, 5, and 6.

Monitoring the System

The HotWire DSLAM software provides submenu options to monitor the activity of the HotWire MCC and DSL cards. The monitoring screens allow you to:

- List the status of active ports and interfaces in a card, as well as display statistics about other physical layers and interfaces.
- Display network protocol statistics, such as information about an application program assigned to a specific socket number, UDP statistics, TCP data and connection statistics, IP statistics, ICMP packet statistics, SNMP statistics including SNMP authentication statistics, HDLC statistics, and PPP statistics.
- Display information about the routing table and detailed information about each routing entry.
- Display the current Address Resolution Protocol (ARP) table.
- Display information about the configured IP router filters.

Use the monitoring screens to help you gather pertinent information and isolate potential problem areas. You can monitor the system with either administrator or operator permission. For more information about monitoring the system, see Chapter 7, *Monitoring the HotWire DSLAM*.

Troubleshooting and Diagnostics

The HotWire DSLAM system provides diagnostic submenu options that:

- Display selftest results for CPU, memories, and ports
- Perform ping tests and display results
- Show major and minor alarms
- Display or clear system error logs
- Enable or disable the A/B power supply alarm
- Perform a trace route to an IP address to display a list of intermediate nodes to the destination
- Run a nondisruptive packet echo test over the DSL line to an RTU

NOTE:

You must have administrator permission to perform most of the troubleshooting and diagnostic activities. However, you can run non-disruptive tests as a user with operator permission. For more information about troubleshooting and diagnostics, see Chapter 8, *Diagnostics and Troubleshooting*.

HotWire Menus and Screens

2

Overview

The HotWire DSLAM has a menu- and screen-driven user interface system that enables the user to configure and monitor the HotWire cards. This chapter covers:

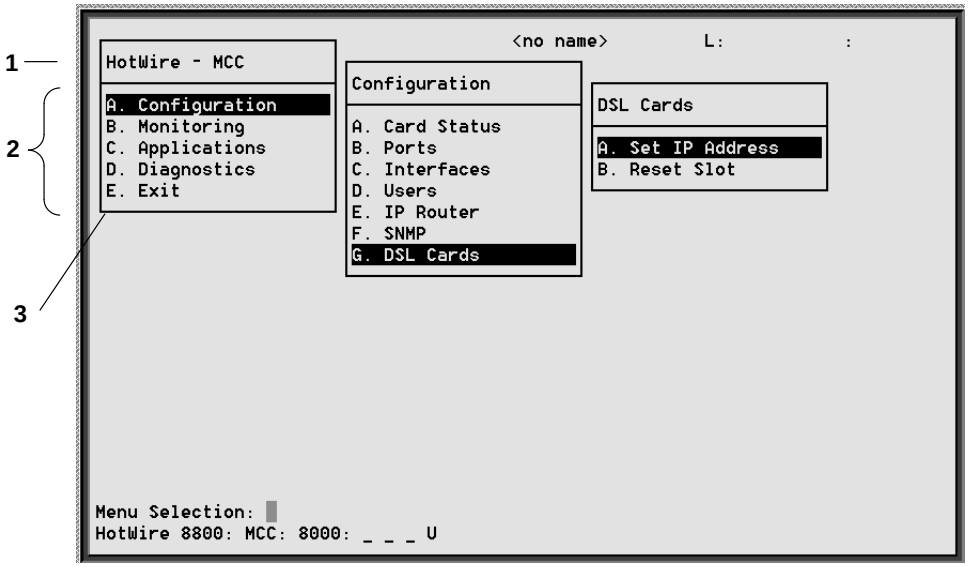
- Menu and screen format
- Commonly used navigation keys
- Menu trees
  - HotWire Chassis Main Menu
  - HotWire – MCC Menu
  - HotWire – DSL Menu
- Logging in to the system
  - Reviewing the Levels of Access
  - Operator Login Screen
  - Card Selection Screen
  - Accessing the HotWire – MCC Menu
  - Accessing the HotWire – DSL Menu
- Exiting from the system

Menu and Screen Formats

The HotWire DSLAM uses an ASCII-based text format for its menus and screens. This section describes the components of a typical HotWire menu and screen.

Components of a HotWire Menu

A typical HotWire menu format looks like this:

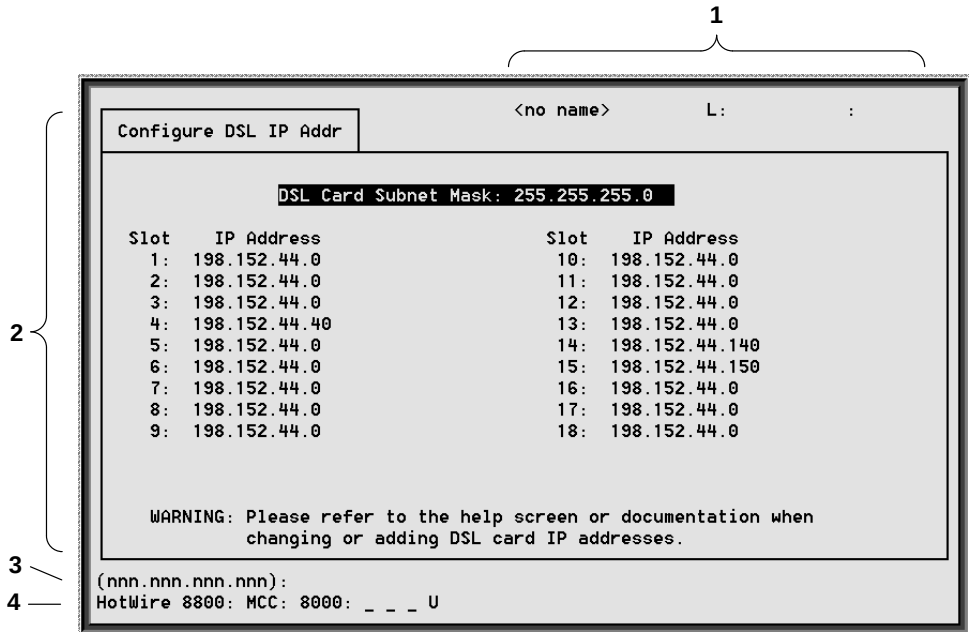


1. **Menu Title** is the top line of the menu window that displays the title of the menu or submenu.
2. **Menu List** is the portion of the menu window that displays the list of menu options. When selected, a menu option displays a submenu window or screen.
3. **Letter Navigation Keys** are provided within a menu list. These keys provide a convenient way (short cut) to select a menu item.

   For example, from the HotWire – MCC menu illustrated above, you can simply press the **A** key to select the Configuration menu item. The Configuration menu appears. You can then press the **G** key to select the DSL Cards menu item. This action displays the DSL Cards menu. (You can also use the arrow keys on your keyboard to select a menu item. See *Commonly Used Navigation Keys* on page 2-5 for more information.)
4. To back up one menu level, press Ctrl-z. To go to the Home screen, press Ctrl-a.

Components of a HotWire Screen

A typical HotWire screen looks like this:



1. **System Header Line** is the top line of the screen. This line has three fields that provide system login information.

   — The first field displays the chassis name or the individual card name. (Access the System Information screen by selecting the appropriate card in the chassis and then follow this menu sequence: *Configuration* → *Card Status* → *Card Info*.) If you do not define the system name, the DSLAM user interface will display `<no name>`.

   — The middle field displays the current login. This field will display either `L:<user_login>` or `R:<user_login>` where `L` indicates a local login, `R` indicates a remote login, and `<user_login>` is the login account of the user currently accessing the system. For example, if a user with a login account called *admin* logs into the system using the local console, this field will display `L:admin`.

   — The last field displays the previous remote or local login on what is currently displayed in the middle field (i.e., the current login). If the current login is local, the last field displays `previous R:<user_login>.` If the current login is remote, the last field displays previous `L:<user_login>.` `L` indicates a local login, `R` indicates a remote login, and `<user_login>` is the login account of the user that has accessed the system. For example, if a user with a login account called *admin* logs into the system remotely via a telnet session, this field will display `R:admin`. `R` displays only when a telnet session was active.

2. **Display Area** is the top portion of the screen on which pertinent DSLAM system information is displayed. This is also the portion of the screen on which fields requiring input are displayed. However, you cannot enter values for the fields in this portion of the screen. You must enter field values in the Input Line at the bottom of the screen (see below).

3. **Input Line** is the area of the screen where you are prompted to enter values for the specific field that is highlighted on the screen.

   For example, in the Configure DSL IP Addr screen above, the DSL Card Subnet Mask field is highlighted. If you want to change the subnet mask, you must enter the new subnet mask at the `(nnn.nnn.nnn.nnn):` prompt at the bottom of the screen.

4. **Status Line** is the last line on the screen. This line displays status information about the selected card.

   For example, in the above illustration, the following line is displayed:

   `HotWire 8800: MCC: 8000: __ __ __ X`

   The first field indicates the chassis type. In this case, the system in use is the HotWire 8800 DSLAM system. The second field indicates the card selected. In this example, the MCC card is selected. The remaining fields indicate card status information, such as whether or not an alarm is present and the status of the Ethernet link. Similar information is displayed on the Card Selection screen. For information about these fields, see *Card Selection Screen* on page 2-14.

Commonly Used Navigation Keys

The following table lists the most commonly used navigation keys with their definitions. These commands are used to move around the menus and screens. For a complete list of keys, see Appendix D, *Navigation Keys*.

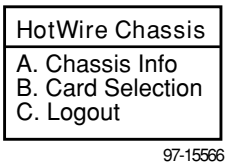
Keys	Definition
Ctrl-a	Moves Home or to the top of the menu.
Ctrl-k	Moves up to the previous menu selection or entry field.
Ctrl-l	Refreshes the screen.
Ctrl-p	Moves back a field.
Ctrl-t	Moves Home or to the top of the menu.
Ctrl-v	Displays a pop-up list of all interfaces on the IP Network screen. Displays a pop-up list of all accounts in system on the Configure Accounts screen.
Ctrl-z	Moves back one menu level or exits from screen.
Up arrow	Moves up to the previous menu selection or entry field.
Down arrow	Moves down to the next menu choice or entry field.
Left arrow	Moves left to the previous menu box or entry field.
Right arrow	Moves right to the next menu box or entry field.
Enter or Return	Accepts entry.
Tab	Moves down or to the next selection.
?	Displays Online help screens that correspond to the particular menu or system screen displayed.

HotWire Menus: A Hierarchical View

This section describes the menu structure of the HotWire user interface.

HotWire Chassis Main Menu

The following illustration shows the HotWire Chassis Main Menu.



From the HotWire Chassis Main Menu, you can select:

- **A. Chassis Info** to enter or display chassis information, such as the chassis name, name of person responsible for the system, and physical location of the chassis.

  For more information, see *Additional Setup Instructions* in Chapter 3.

- **B. Card Selection** to select a particular card in the chassis. This screen also displays status information about all cards in the chassis. The card you select determines which HotWire menu the system will display next (either the HotWire – MCC menu or the HotWire – DSL menu).

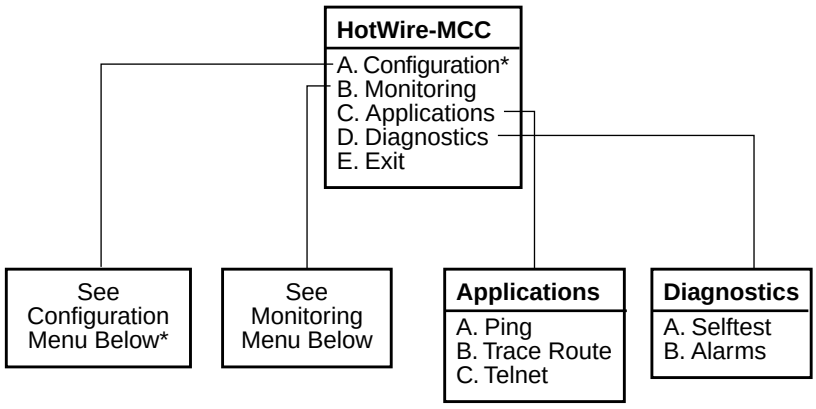
  For more information, see *Card Selection screen* on page 2-14.

- **C. Logout** to exit from the current login session on the HotWire DSLAM.

  For more information, see *Exiting From the System* on page 2-16.

HotWire – MCC Menu

After selecting the MCC card from the Card Selection screen, the DSLAM system displays the HotWire – MCC Menu.



* The configuration menu item appears only if you have administrator permission.

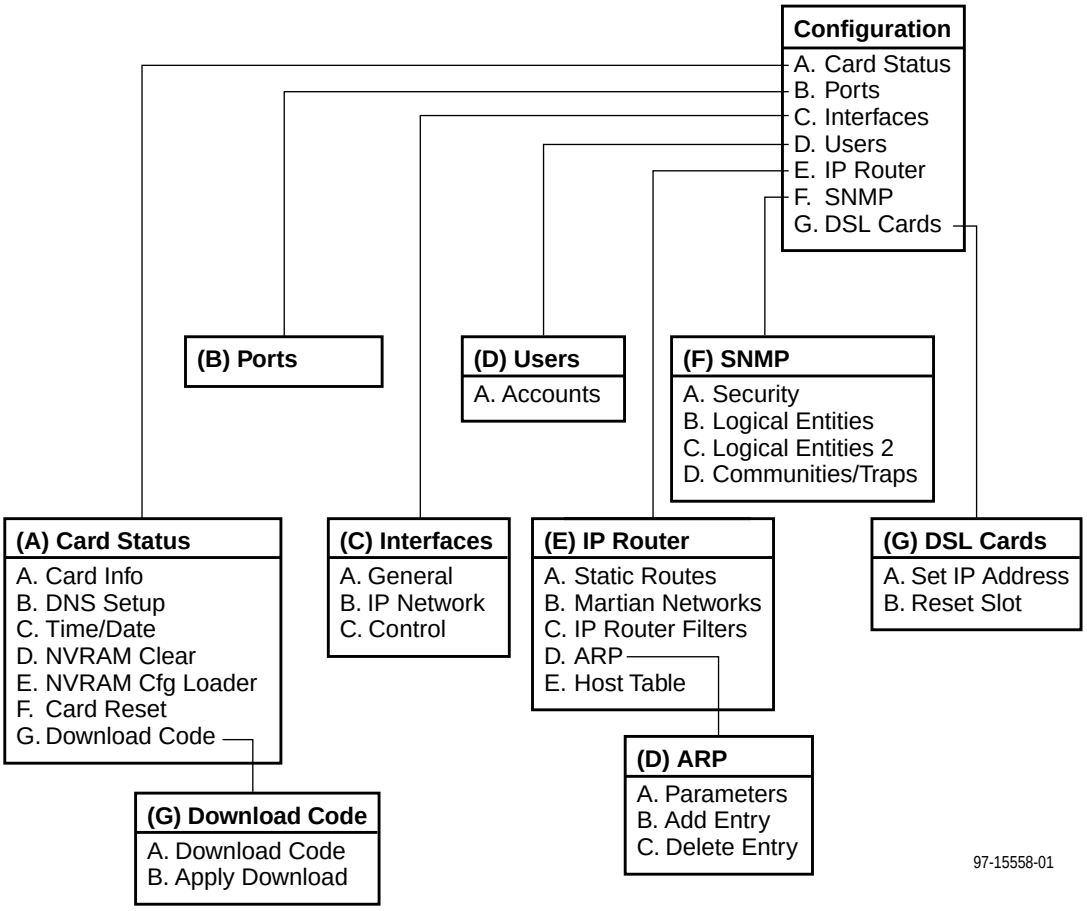
97-15557-01

From this menu, you can configure, monitor, run applications, and troubleshoot the MCC card.

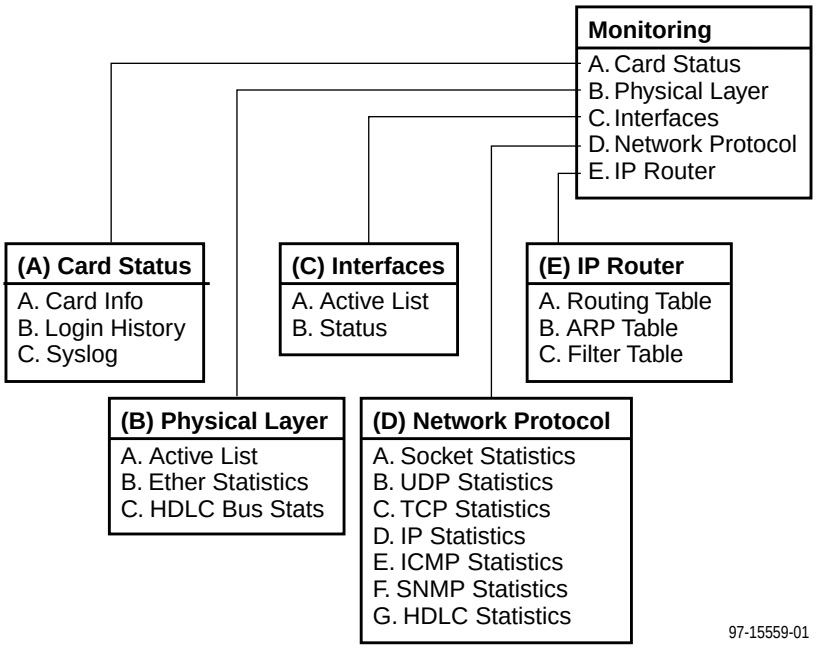
The following figure illustrates the complete Configuration menu hierarchy from the HotWire – MCC menu.

NOTE:

The Configuration menu and its submenus appear only when logging in to the system with a user account that has administrator permission.

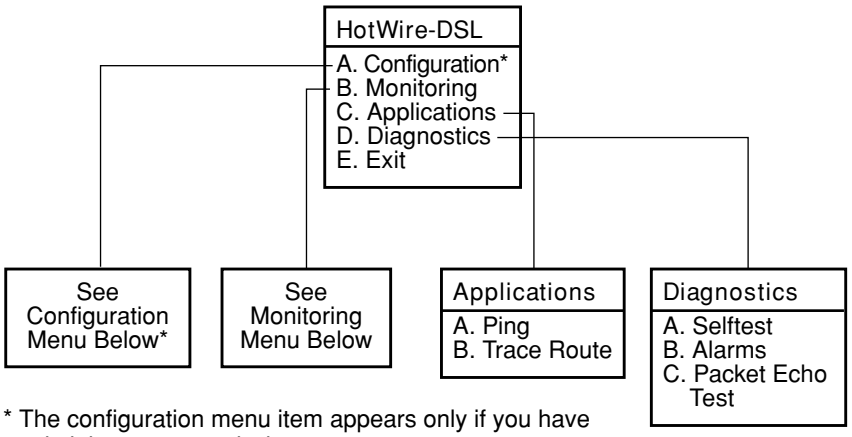


The following figure illustrates the complete Monitoring menu hierarchy from the HotWire – MCC menu.



HotWire – DSL Menu

After selecting a specific DSL card from the Card Selection screen, the DSLAM system displays the HotWire – DSL Menu.

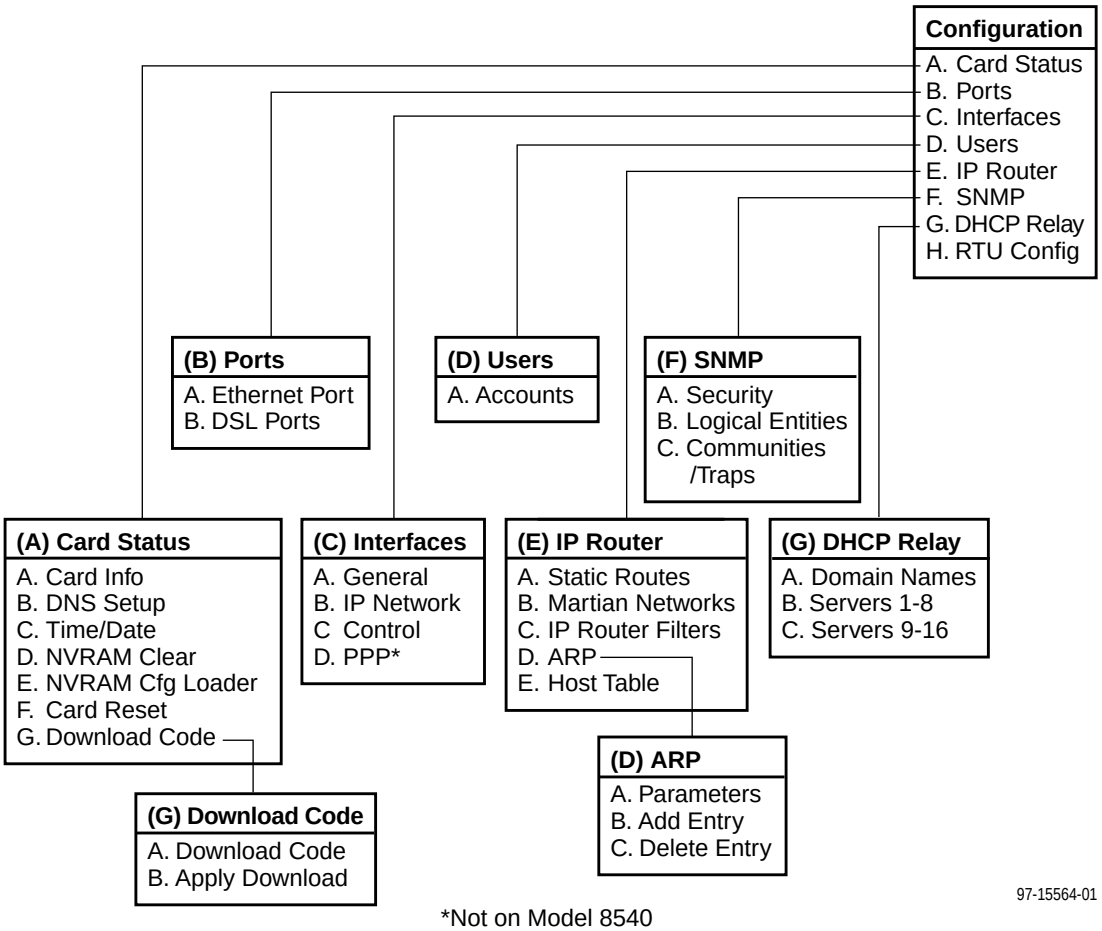


From this menu, you can configure, monitor, run applications, and troubleshoot a specific DSL card.

The following figure illustrates the complete Configuration menu hierarchy from the HotWire – DSL menu.

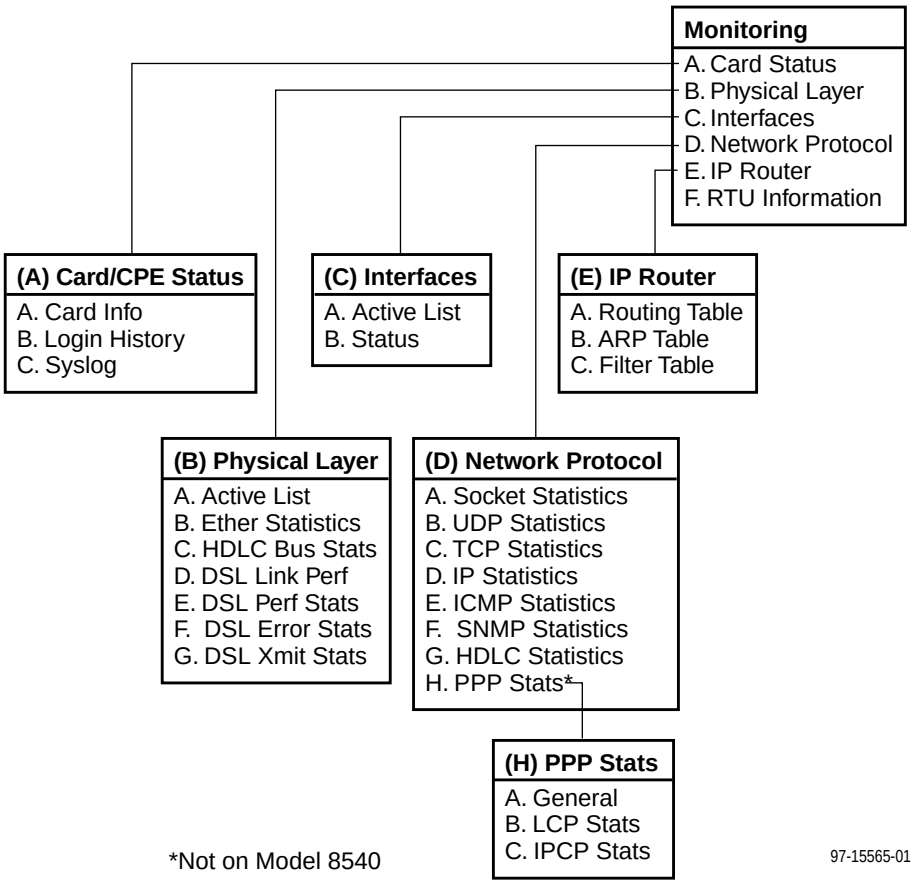
NOTE:

The Configuration menu and its submenus appear only when logging in to the system with a user account that has administrator permission.



*Not on Model 8540

The following figure illustrates the complete Monitoring menu hierarchy from the HotWire – DSL menu.



Logging in to the System (After the System Has Been Configured)

NOTE:

When you power on the system for the first time, the system displays the Who Am I screen. This screen can be accessed only from the local console. For information about this screen, see *Accessing the System for the First Time* in Chapter 3.

This section describes how to log in to the HotWire DSLAM system after the system has been configured for the first time.

Reviewing the Levels of Access

There are two levels of privileges on the HotWire DSLAM system. Your user accounts can be configured with a user name, password, and privilege of:

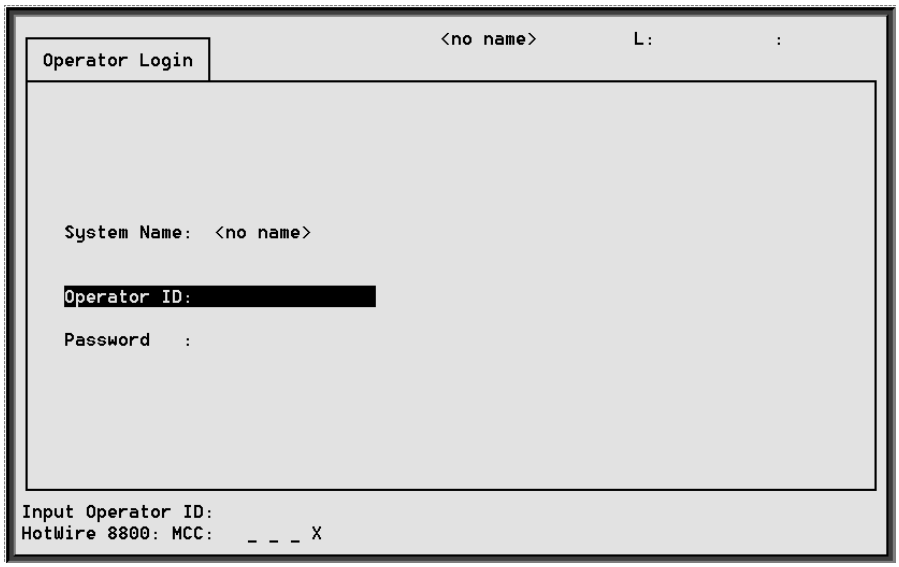
- Administrator, giving you access to all of the features of the system including configuration options, or
- Operator, giving you read-only access.

The default access is no login and password with administrator status. To provide login security to the DSLAM, user accounts must be configured. See *MCC Configuration Users Screens* in Chapter 5.

Operator Login Screen

You can log into the HotWire DSLAM system using either a local VT100-compatible terminal or a remote Telnet connection. However, the HotWire DSLAM system accepts only one login session at a time.

At the Operator Login screen, enter your login ID and password.



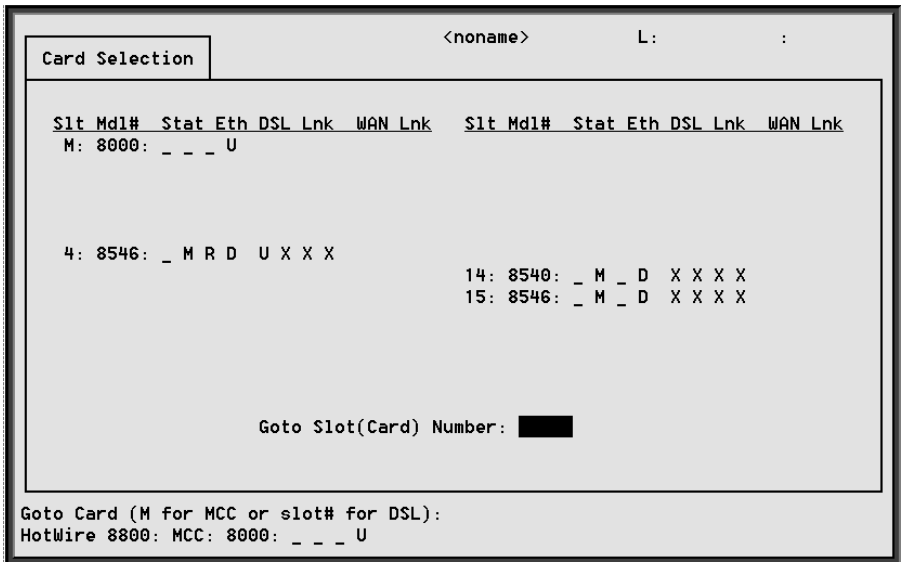
NOTE:

The login ID and password are case sensitive; that is, the system recognizes both upper- and lower-case letters. For example, if you enter your user name and password information in upper case letters and your assigned user name and password are in upper- and lower-case letters, the system will not let you log in.

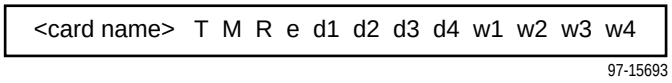
After entering your login ID and password, the system displays the HotWire Chassis Main Menu.

Card Selection Screen

From the HotWire Chassis Main Menu, select Card Selection to display the status of any of the 18 cards present in the chassis by type and slot number. The Card Selection screen also displays general and interface status for each card.



The following figure illustrates the positional display of the card selection screen:



97-15693

On the chassis display, the following information is shown.

NOTE:

If an option is not active, an underscore is shown in its place.

Position	Display	Description
	<card type>	MCC
1	T (Test mode)	Card currently in test mode
2	M (Major alarm)	Major alarm present on card
3	R (Minor alarm)	Minor alarm present on card
4	e (Ethernet)	Status of Ethernet link (U=UP, D=Down, or X=Disabled)
5	d1 (DSL)#	Status of DSL card Port 1 (U=UP, D=Down, or X=Disabled, or H=Handshaking)
6	d2 (DSL)#	Status of DSL card Port 2 (U=UP, D=Down, or X=Disabled, or H=Handshaking)

Position	Display	Description
7	d3 (DSL)#	Status of DSL card Port 3 (U=UP, D=Down, or X=Disabled, or H=Handshaking)
8	d4 (DSL)#	Status of DSL card Port 4 (U=UP, D=Down, or X=Disabled, or H=Handshaking)
9	w1 (WAN)*#	Status of WAN link (U=Up, D=Down, L=Loopback)
–	w2 (WAN)*#	Status of WAN link Port 2 (U=Up, D=Down, L=Loopback)
–	w3 (WAN)*#	Status of WAN link Port 3 (U=Up, D=Down, L=Loopback)
–	w4 (WAN)*#	Status of WAN link Port 4 (U=Up, D=Down, L=Loopback)
* Not applicable for 8540 or 8546 DSLAM RADSL circuit cards of MCC cards. # Not used for MCC cards.		

If an option is not active, an underscore is shown in its place.

Also on this screen, there is a prompt used to select a specific card in the DSLAM chassis. When a DSL slot number is entered, you are telneted (in the background) to the card you selected.

NOTE:

When you select MCC on this screen, there is no telnet session involved. The login screens and the top level menu reside on the MCC.

For more information about the status displayed on this screen, such as major and minor alarms, see *Troubleshooting* in Chapter 8.

Accessing the HotWire – MCC Menu

▶ Procedure

To access the HotWire – MCC menu:

1. From the HotWire Chassis Main Menu, select **B** for Card Selection.
   The Card Selection screen appears.
2. At the `Goto Card (MCC or DSLnn):` prompt, enter **MCC** or **M**.
   The HotWire – MCC menu appears.

Accessing the HotWire – DSL Menu and Selecting a Specific DSL Card

▶ Procedure

To access the HotWire – DSL menu:

1. From the HotWire Chassis Main Menu, select Card Selection.

   The Card Selection screen appears.

2. Verify that the DSL card you want to access appears on the Card Selection screen. (See *Card Selection Screen* on page 2-14 for more information.)

3. At the `Goto Card (MCC or DSLnn):` prompt, enter **DSL** and the number of the slot. Then, press Return. For example, if you want to configure the DSL card in Slot 13, enter **DSL13** or **13**.

   The HotWire – DSL menu appears.

Exiting From the System

You can manually log out of the system or, after five minutes of inactivity, the system will automatically log you out.

Manually Logging Off

▶ Procedure

To exit from the HotWire DSLAM system:

1. Return to the HotWire Chassis Main Menu by selecting Exit from either the HotWire – MCC menu or the HotWire – DSL menu.

   The HotWire Chassis Main Menu appears.

2. From the HotWire Chassis Main Menu, select Logout.

   The system exits from the current login session on the HotWire DSLAM.

Automatically Logging Off

The DSLAM system has an automatic timeout feature that logs you out of the system after five minutes of inactivity. You will need to log back in to continue your work.

To log back in, press Return to display the Operator Login screen and log in.

Initial Setup Instructions

3

Overview

This chapter provides instructions on how to access the system for the first time and perform initial setup instructions.

NOTE:

It is highly recommended that you read the *HotWire DSLAM for 8540 and 8546 DSL Cards Network Configuration Guide* before you attempt to configure the system. The Network Configuration Guide provides worksheets to help you plan and configure your network.

Accessing the System for the First Time

When you power on the HotWire DSLAM for the first time, the system displays the Who Am I screen on the console terminal. On this screen, you must set the management IP address and subnet mask for the MCC card. Follow the instructions in the following section, *Setting the Management IP Address and Subnet Mask on the MCC*.

Setting the Management IP Address and Subnet Mask on the MCC

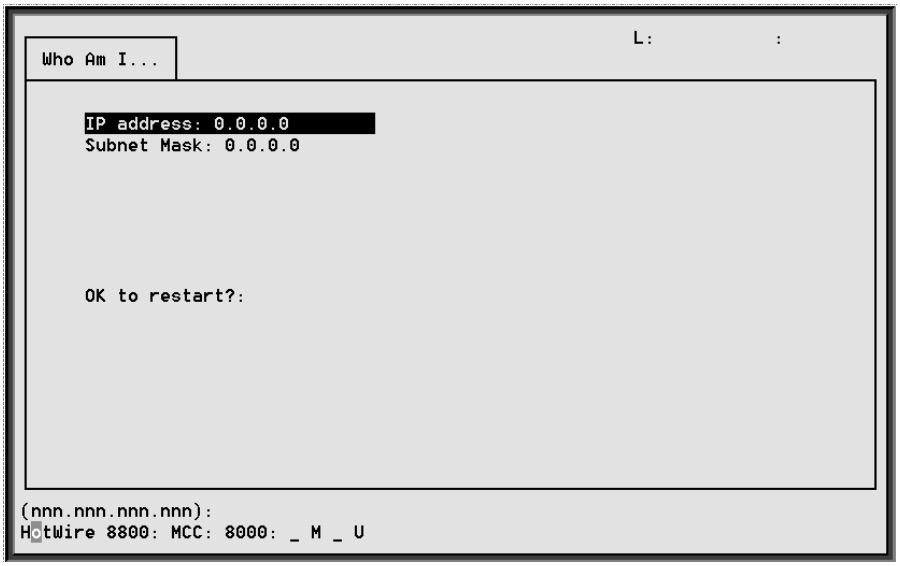
After powering on the system for the first time, set the management IP address and subnet mask of the MCC card. This is a mandatory step and must be completed before proceeding to Chapter 4, *Configuring the HotWire DSLAM*.

▶ Procedure

To set the management IP address and subnet mask from the console terminal:

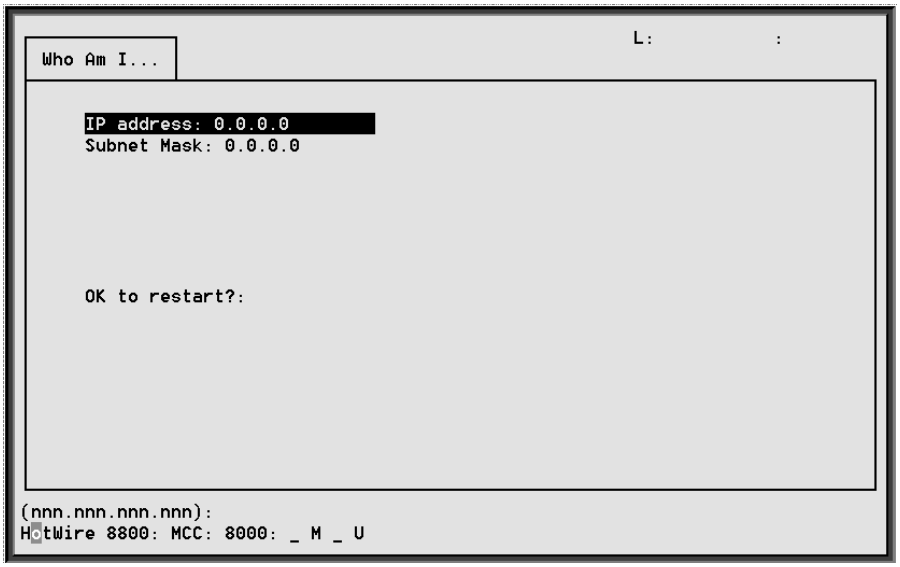
1. Power up the chassis.

   After the self-test completes, the Who Am I screen appears.



2. From the Who Am I screen, enter the management domain IP address of the MCC card and press the Return key. For example, if the IP address of the MCC card is **198.152.110.1**, type this value at the `(nnn.nnn.nnn.nnn):` prompt on the Input Line at the bottom of the screen.

   The system automatically calculates the subnet mask based on the IP address you enter.

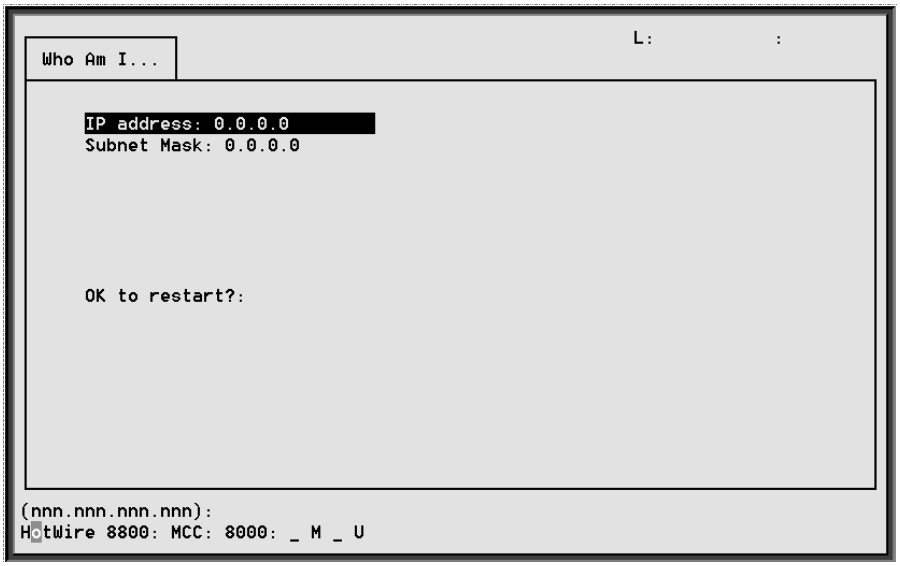


3. Do one of the following at the `(nnn.nnn.nnn.nnn):` prompt:

   — To accept the subnet mask, press Return.

   — To enter a different subnet mask, enter a new subnet mask and press Return.

   The system highlights the `OK to restart?:` prompt.



4. Type **y** at the `yes/no:` prompt to restart the card or **n** to decline the restart.

   If you type **y**, the card restarts. The system displays the HotWire Chassis Main Menu.

   NOTE:

   At this point, the MCC card can accept a Telnet session to be used for remote configuration.

Additional Setup Instructions

This section describes additional setup instructions you should perform. On the Chassis Information screen, you can enter pertinent chassis information, such as the chassis name, name of person responsible for the system, and physical location of the chassis.

Chassis Information Screen

▶ Procedure

1. Choose Chassis Info from the HotWire Chassis Main Menu to enter or display chassis configuration information.

   The following table describes the information you should enter on the Chassis Information screen. This information is used in the general section of the SNMP MIB II.

Field	Input	Description
Chassis Name	16 alphanumeric characters	Name for the equipment
Chassis Contact	32 alphanumeric characters	Name and phone number of individual responsible for the equipment
Chassis Location	16 alphanumeric characters	Physical location of the equipment
Bay Number	16 alphanumeric characters	Floor and/or bay number of the equipment
Chassis Number	16 alphanumeric characters	Chassis serial number (located on the lower right side of chassis)

2. When you have made the appropriate changes to the screen, a message `Configuration has been modified. Save (yes/no)?` appears. Enter **yes** to save changes and press Return to go back to the HotWire Chassis Main Menu.

What's Next?

Now you are ready to configure your HotWire DSLAM. Refer to Chapter 4, *Configuring the HotWire DSLAM*, for instructions on how to configure the mandatory minimum configurations, and Chapter 5, *MCC Card Configuration*, and Chapter 6, *DSL Card Configuration*, for additional configuration instructions when customizing your application.

After you have configured your system, you can monitor and troubleshoot potential problems on the system. Refer to Chapter 7, *Monitoring the HotWire DSLAM*, and Chapter 8, *Diagnostics and Troubleshooting*, for more information.

Configuring the HotWire DSLAM

4

Overview

The HotWire DSLAM enables you to configure and manage the HotWire MCC and DSL cards. This chapter describes the basic card configuration instructions.

Port Naming Convention

The following is the naming convention used for the HotWire DSLAM interfaces:

NOTE:

Interfaces are sometimes referred to as ports. The term *ports*, however, usually is reserved for referring to the physical layer attributes of an interface.

- **e1a** — Interface name of the DSLAM system 10BaseT interface on the MCC and DSL cards.
- **s1b** — Interface name of the MCC and DSL card's interface to the DSLAM system backplane bus.
- **s1c**, **s1d**, **s1e**, and **s1f** — Interface names of the four DSL ports on a DSL card.

NOTE:

These names are used throughout the remainder of this guide to reference the HotWire DSLAM interfaces. These are also the names used in the HotWire DSLAM software when configuring the HotWire DSLAM system.

Configuring MCC Cards, DSL Cards, and RTUs

Use the procedures **in the following order** to configure the MCC and DSL cards for the basic setup for terminal management and user data connectivity.

NOTE:

It is assumed that you have read the *HotWire DSLAM for 8540 and 8546 DSL Cards Network Configuration Guide* and have assigned service and management domain IP addresses for all devices (MCC, DSL, and RTUs). For your convenience, Appendix A of the *Network Configuration Guide* contains worksheets to record your configuration settings.

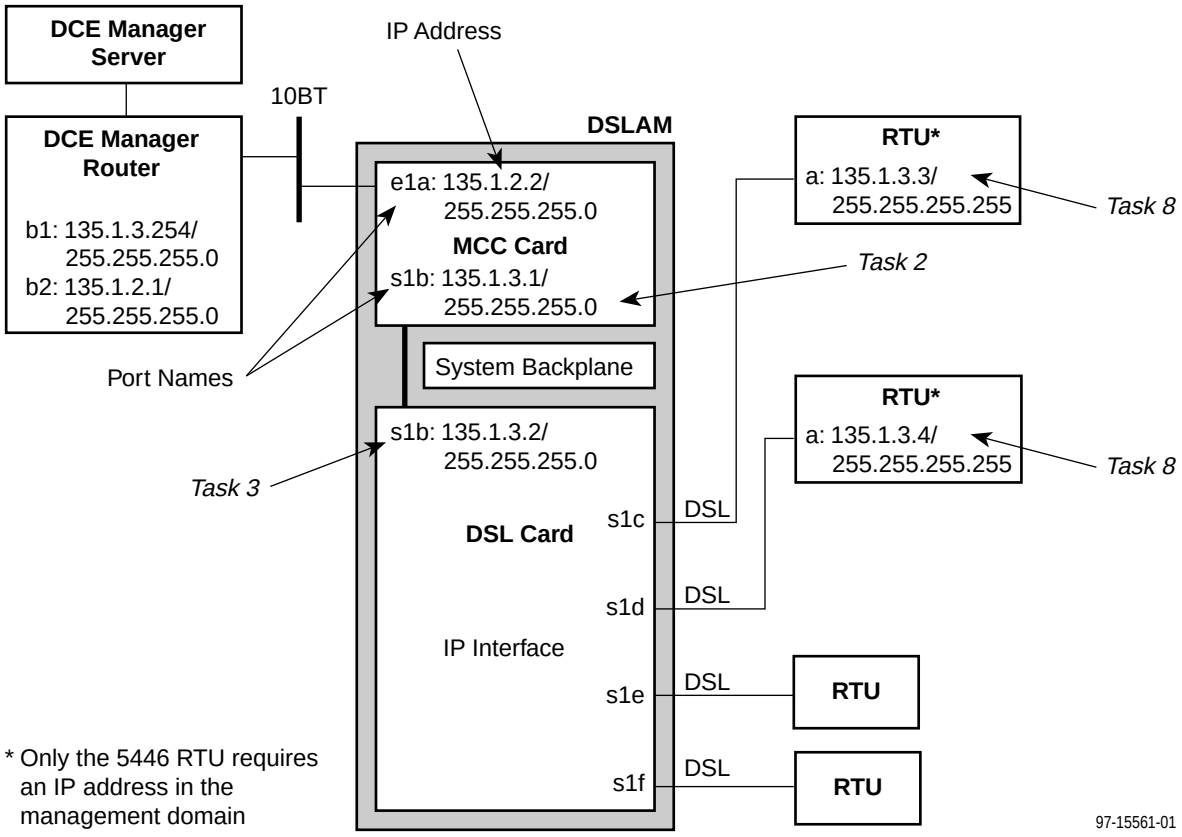
The following tables list the basic steps you need to configure the MCC cards, DSL cards, and RTUs.

For the Management Domain, perform task . . .	On the . . .	See . . .
1. Configure time and date.	MCC	*Setting Time and Date Screen*, page 4-6.
2. Assign the IP address to the backplane on the MCC card.	MCC	*Assigning IP Addresses to the Backplane on the MCC Card*, page 4-7.
3. Assign the IP addresses to the DSL cards.	MCC	*Assigning IP Addresses to the DSL Cards on the MCC Card*, page 4-8.
4. Create SNMP Community Strings and Authentication Failure Trap.	MCC	*Creating SNMP Community Strings and Authentication Failure Trap*, page 4-9.
5. Create default route.	MCC	*Creating the Default Route*, page 4-10.
6. Reset the MCC card.	MCC	*Resetting the MCC Card*, page 4-11.
7. Select a DSL card to configure.	DSL	*Selecting a DSL Card to Configure*, page 4-11.
8. Configure 5446 RTU IP host address for the 8546 DSL card. (Not applicable to 8540 DSL card.)	DSL	*Configuring 5446 RTU IP Host Addresses on the 8546 DSL Card*, page 4-12.

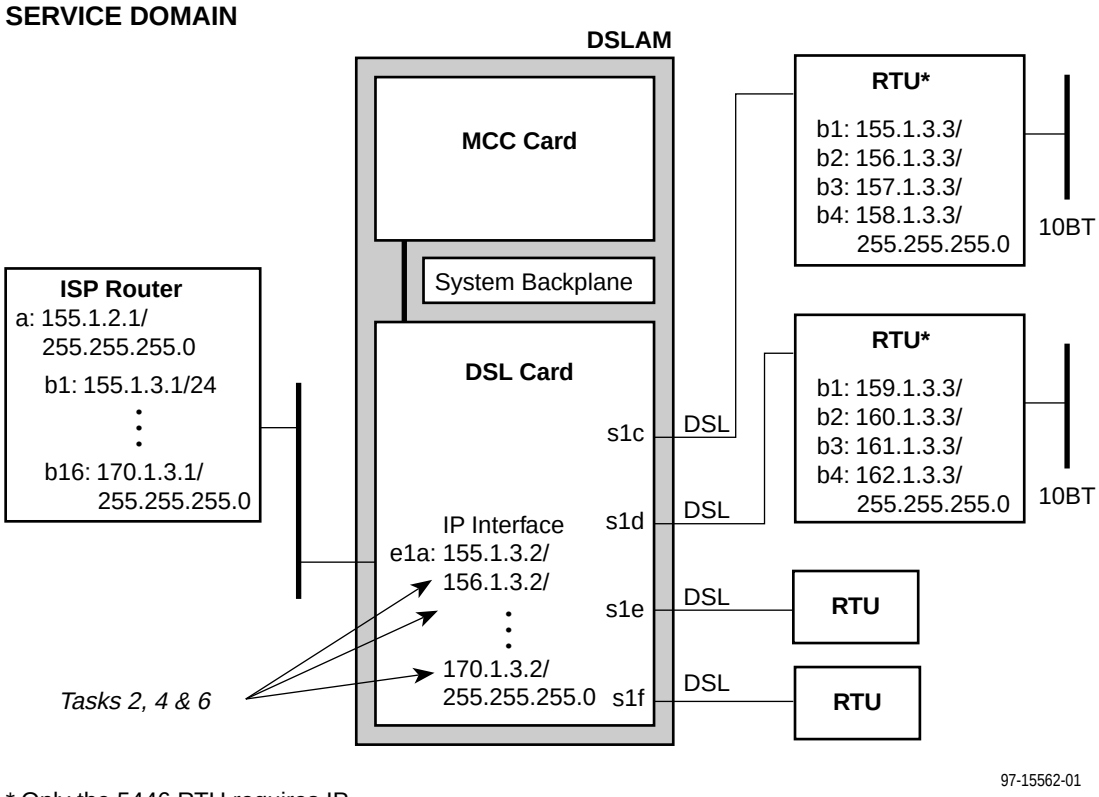
For each Service Domain, perform task . . .	On the . . .	See . . .
1. Configure a static route to the NMS.	DSL	*Configuring a Static Route to the Network Management System on each DSL Card*, page 4-13.
2. Assign IP addresses to the DSL card LAN.	DSL	*Assigning IP Addresses to the DSL Card LAN*, page 4-14.
3. Reset the DSL card.	DSL	*Resetting the DSL Card*, page 4-15.
4. Configure static routes to end users on each DSL card.	DSL	*Configuring Static Routes to End Users on each DSL Card*, page 4-16.
5. Create DHCP Relay Agent.	DSL	*Creating DHCP Relay Agent*, page 4-17.
6. Create default route or source route on DSL.	DSL	*Creating Default Route or Source Route on the DSL*, page 4-18.

The following illustrates the management domain components that must be configured and examples of the various naming conventions.

MANAGEMENT DOMAIN



The following illustrates the service domain components that must be configured and examples of the various naming conventions.



* Only the 5446 RTU requires IP addresses in the service domain

Setting Time and Date Screen

When you select Time/Date from the Card Status menu, the Time/Date screen is displayed. From this screen, you can configure the local time and date on the card.

▶ Procedure

To set the time and date on the MCC card:

1. Select Card Selection (**B**) from the HotWire Chassis Main Menu.
2. At the `Goto Card (MCC or DSLnn)`: prompt, enter **MCC** or **M**.
3. Select *Configuration* → *Card Status* → *Time/Date* (**A-A-C**).
4. Enter values for the following fields and press Return after each entry:

Field	Description	Input
Local Time/Date	Current local time and date.	*hh.mm (*am or pm*)* *mm/dd/yy* format
Client Network Time Protocol (NTP) Mode	General time protocol (Broadcast) or specific time protocol with address (Unicast).	Broadcast or Unicast (Default = broadcast)
NTP Server*	IP address of the NTP server.	*nnn.nnn.nnn.nnn* format
Synchronized(hrs)	How often the system should go out looking for the time and date to synchronize the system time and date.	1–24
* While this field is optional, it is recommended that a value be entered to ensure the time of the DSLAM stays in synch with “real time.”		

NOTE:

At system boot time, the time on the DSL card automatically syncs with the MCC card. Therefore, it is usually not necessary to use this screen on the DSL. If there are active DHCP-leased routes on the card, changing the local time is not recommended.

5. Press Ctrl-z to return to the *Configuration* → *Card Status* menu.

Assigning IP Addresses to the Backplane on the MCC Card

Use this procedure to create a separate and distinct network or subnetwork for the 8546 DSL cards and 5446 RTUs.

▶ Procedure

To assign IP addresss to the backplane:

1. Select *Configuration* → *Interfaces* → *IP Network* (**A-C-B**).
2. Enter values for the following basic fields and press Return after each entry:

Field	Description	Input
IP Interface	Name of the interface.	s1b (backplane)
Base IP Addr	IP address of the management domain.	*nnn.nnn.nnn.nnn* format
Base Subnet Mask	Associated subnet mask of the base IP address.	*nnn.nnn.nnn.nnn* format
Peer IP Address	IP address used to indicate directly connected systems.	*nnn.nnn.nnn.nnn* format *
Route to Peer	Routing method to use to get to peer (i.e., host or net).	*Net*
* Enter the network/subnetwork portion of the Base IP address, with 0 for the host portion so that the Peer is the entire subnet.		

In addition, the following fields appear on the screen. These fields can be used to customize your application.

Field	Description	Input
Input Filter	Prevents packets from entering the DSL card through a specified interface.	Blank to disable.
Output Filter	Prevents packets from going out of the DSL card through a specified interface.	Blank to disable.

3. Press Ctrl-z to return to the *Configuration* → *Interfaces* menu.

Assigning IP Addresses to the DSL Cards on the MCC Card

Use this procedure to define addresses within the management domain. These are automatically assigned to the DSL cards when they are inserted in the chassis.

▶ Procedure

To assign IP addresses to the DSL cards:

1. Select *Configuration* → *DSL Cards* → *Set IP Address* (**A-G-A**).
2. Enter values for the following fields and press Return after each entry:

Field	Description	Input
DSL Card Subnet Mask	Subnet mask for the backplane(s1b) management subnet.	*nnn.nnn.nnn.nnn* format
IP Address (for each DSL card)	Management domain IP address for each DSL card in the system.	*nnn.nnn.nnn.nnn* format. (Subnet is predetermined – you can enter the host number.)

NOTE:

You must have assigned IP addresses to the backplane on the IP Network screen for s1b before performing this procedure.

3. Press Ctrl-z to return to the *Configuration* → *DSL Cards* menu.

Creating SNMP Community Strings and Authentication Failure Trap

Use this procedure to configure SNMP community strings and enable the Authentication Failure trap mechanism. For additional security, ensure that source validation is enabled. (See Appendix C, *Checklist for Setting Up SNMP Features*.)

▶ Procedure

To create SNMP community strings and authentication failure trap:

1. Select *Configuration* → *SNMP* → *Communities/Traps* (**A-F-D**).
2. Enter values for the following fields and press Return after each entry:

Field	Description	Input
Authentication Failure Trap	Determines whether to send a trap when a SNMP request community string does not match or when the password for a telnet session is incorrect.	Enable/Disable
Community Name	SNMP community string name.	Up to four unique community names per screen
Access	Permission that is granted for each community.	RO = Read Only RW = Read/Write NA = No Access
IP address and port	NMS system host IP address	*nnn.nnn.nnn.nnn* format
Input Number	Number of port.	Default = 162

3. Confirm the save and press Ctrl-z to return to the *Configuration* → *SNMP* menu.

Creating the Default Route

Use this procedure to create the default route to the management domain next hop router. This default route will be used to forward management domain traffic from the MCC card.

▶ Procedure

To create the default route:

1. Select *Configuration* → *IP Router*→ *Static_Routes* (**A-E-A**).
2. Press Return on the Item 0 field to add a new record.
3. Enter values for the following fields and press Return after each entry:

Field	Description	Input
Host/Net	Destination of the route.	*0.0.0.0* to indicate the default route
Subnet Mask	Associated subnet mask for the specified destination IP address.	*nnn.nnn.nnn.nnn* format
Next Hop	IP address of the next hop device for the specified destination.	*nnn.nnn.nnn.nnn* format
Pref (Preference)	Measure of how preferable one route is to another, if you have two routes going to the same destination. (The lower the number, the more preferable the route.) This route is compared to other routes for the same destination address.	*1*

4. Confirm the save and press Ctrl-z to return to the *Configuration* → *IP Router* menu.

Resetting the MCC Card

After configuring the MCC card, reset the MCC card to install the configuration settings.

▶ Procedure

To reset the HotWire Chassis:

1. Select *Configuration* → *Card Status*→*Card Reset* (**A-A-F**).
2. Enter yes (**y**) to verify MCC reset.

   NOTE:

   When you enter yes, all data connectivity is interrupted.
3. Wait for the MCC card to reboot.
4. Press Return.
5. The Operator Login screen is displayed.
6. Enter login information.

Selecting a DSL Card to Configure

All DSL cards that are present in the chassis and have had backplane addresses assigned to them should appear on the Card Status screen. However, if one or more do not appear, go to the MCC card, select *Configuration* → *DSL Cards*→*Reset Slot* and reset the DSL card.

▶ Procedure

To select a specific DSL card to configure:

1. From the HotWire Chassis Main Menu, select Card Selection (**B**).
2. Enter DSL*nn* or *nn*, where *nn* is the number of the DSL card you want to configure, and press Return.

   The HotWire DSL menu is displayed.
3. Select Configuration and press Return.

   The Configuration Menu is displayed.

Configuring 5446 RTU IP Host Addresses on the 8546 DSL Card

Use this procedure to assign an IP address within the management subnet to each 5446 RTU interoperating with an 8546 DSL card.

▶ Procedure

To configure IP host addresses on the DSL card:

1. Select *Configuration* → *Interfaces*→ *IP Network* (**A-C-B**).
2. Enter values for the following basic fields and press Return after each entry:

Field	Description	Input
IP Interface	Name of the interface.	s1c (8546 DSL interface)
Peer IP Address	IP address associated with the other end of the link; i.e., the 5446 RTU.	*nnn.nnn.nnn.nnn* format *
Route to Peer	Routing method to use to get to peer (i.e., host or net).	*Host*
* The subnet mask can be changed for the corresponding 5446 RTU. Refer to Appendix F, *5446 RTU Setup*.		

NOTE:

The DSL interface is “unnumbered,” meaning it requires no IP address. (This field is read only.)

The following fields also appear on the screen. These fields can be used to customize your application.

Field	Description	Input
Input Filter	Prevents packets from entering the DSL card through a specified interface.	Blank to disable.
Output Filter	Prevents packets from going out of the DSL card through a specified interface.	Blank to disable.

3. Repeat the above procedure for interfaces s1d, s1e, and s1f (8546 DSL Ports 2, 3, and 4, respectively).
4. Press Ctrl-z to return to the *Configuration* → *Interfaces* menu.

Configuring a Static Route to an NMS on each DSL Card

Use this procedure to enable the management traffic from the 8546 DSL cards or 5446 RTUs to be routed back through the MCC.

▶ Procedure

To configure a static route to an NMS on each DSL card:

1. Select *Configuration* → *IP Router* → *Static_Routes* (**A-E-A**).
2. Press Return on the Item 0 field to add a new record.
3. Enter values for the following fields and press Return after each entry:

Field	Description	Input
Host/Net	Destination of the route to the NMS.	*0.0.0.0* to indicate the default route
Subnet Mask	Associated subnet mask for the specified destination IP address to the NMS.	*nnn.nnn.nnn.nnn* format
Next Hop	IP address of the next hop device for the specified destination to the NMS.	*nnn.nnn.nnn.nnn* format
Pref (Preference)	Measure of how preferable one route is to another, if you have two routes going to the same destination. (The lower the number, the more preferable the route.) This route is compared to other routes for the same destination address.	*1*

4. Confirm the save and press Ctrl-z to return to the *Configuration* → *IP Router* menu.

Assigning IP Addresses to the DSL Card LAN

Use this procedure to give DSL cards a LAN Interface IP address in each Network Service Provider (NSP) domain supported by those cards.

▶ Procedure

To assign IP addresses to the DSL Card LAN:

1. Select *Configuration* →*Interfaces* →*IP Network* (**A-C-B**).
2. Enter values for the following fields and press Return after each entry:

Field	Description	Input
IP Interface	Name of the interface.	*e1a* (Ethernet port)
IP Address (for each 8540 and 8546 DSL card)	IP address for each DSL card in the system. This address must be different that the management domain IP address.	*nnn.nnn.nnn.nnn* format. (Subnet is predetermined – you can enter the host number.)
Subnet Mask	Associated subnet mask for the specified destination IP address.	*nnn.nnn.nnn.nnn* format
Route to Peer (Field does not appear on *e1a* and Model 8540.)	Routing method used to get to peer (i.e., host or net).	*Net*
* Enter the network/subnetwork portion of the Base IP address, with 0 for the host portion so that the Peer is the entire subnet.		

In addition, the following fields also appear on the screen. These fields can be used to customize your application.

Field	Description	Input
Input Filter	Prevents packets from entering the DSL card through a specified interface.	Blank to disable.
Output Filter	Prevents packets from going out of the DSL card through a specified interface.	Blank to disable.

3. Press Ctrl-z to return to the *Configuration* →*Interfaces* menu.

Resetting the DSL Card

After configuring all of the service domain IP addresses on a DSL card (IP address has been added or changed), reset the card to enable the new configuration changes.

▶ Procedure

To reset the DSL Card:

1. Select *Configuration* → *Card Status* → *Card Reset* (**A-A-F**).
2. Enter DSL*nn*, where *nn* is the slot number for the DSL card you just configured.
3. Enter **Y** at the prompt to confirm.

   NOTE:

   When you enter Y, all data connectivity is interrupted.

4. If you have entered yes, verify that the LEDs on the DSL card go through the reset sequence once, and then a second time after approximately 10 seconds (BOOTP).

Configuring Static Routes to End Users on each DSL Card

Use this procedure to enable the management traffic from the 8546 DSL cards to the 5446 RTU and attached end-user systems. Use SNMP or the IP Injection Tool to download the needed enterprise MIBs and to configure static routes and service domain routes to end users attached to each 5446 RTU. Refer to Appendix F, *5446 RTU Setup*.

NOTE:

Each time you create a static route for an end-user system behind an RTU, you should also create a corresponding source-based input filter rule. See Chapter 5, *IP Address Allocation,* Chapter 6, *IP Routing, and* Chapter 7, *IP Filtering*, of the *HotWire DSLAM for 8540 and 8546 DSL Cards Network Configuration Guide*.

▶ Procedure

To configure a static route to End Users:

1. Select *Configuration* → *IP Router*→*Static_Routes* (**A-E-A**).
2. Press Return on the Item 0 field to add a new record.
3. Enter values for the following fields and press Return after each entry:

Field	Description	Input
Host/Net	Destination of the route.	*0.0.0.0* to indicate the default route
Subnet Mask	Associated subnet mask for the specified destination IP address.	*nnn.nnn.nnn.nnn* format On Model 8540, subnet mask must be 255.255.255.255.
Next Hop (on Model 8546)	IP address of the next hop device for the specified destination.	*nnn.nnn.nnn.nnn* format
Next Hop (on Model 8540)	DSL port name for next hop.	Port name s1c, s1d, s1e, or s1f.
Pref (Preference)	Measure of how preferable one route is to another, if you have two routes going to the same destination.	The lower the number, the more preferable the route.
S/D (Source/Destination)	Source or destination route type.	Default = Dst
PA (Proxy ARP)	Router answers ARP requests intended for another machine.	Default = No

4. Confirm the save and press Ctrl-z to return to the *Configuration* → *IP Router* menu.

Configuring DHCP Relay Agent (dynamic addressing)

Use this procedure to provide dynamic Service Domain IP address allocation to the end-user systems attached to the DSL RTUs.

▶ Procedure

To configure relay agent:

1. Make certain that the Gateway address used in relaying DHCP requests is configured as an *e1a* address (**A-C-B**).
2. Select *Configuration → DHCP Relay → Domain Names* (**A-G-A**).
3. Enter values for the following field and press Return after each entry:

Field	Description	Input
Domain Names	ISP domain names.	32 maximum characters.

NOTE:

Unless your client supports the domain names field, you will not be able to have service selection. By default, each port can be assigned one service provider.

The Interface IP address is read only and is required to key in the corresponding domain name.

4. Select *Configuration → DHCP Relay → Servers 1–8 or 9–16* (**A-G-B** or **C**).
5. Enter values for the following field and press Return after each entry:

Field	Description	Input
DHCP Server	DHCP server IP address.	*nnn.nnn.nnn.nnn* format.
Authen Server (optional)	Authentication server IP address for this domain.	*nnn.nnn.nnn.nnn* format.
RADIUS Secret (optional)	RADIUS encryption value.	Up to 16 numeric characters.
Authen Type	Type of authentication you want performed.	**N** = none (No authentication to be performed.) **R** = RADIUS (Forward a message to a RADIUS server.) **T** = XTACACS (Forward a message to a XTACACS server.)
Authentication Wait TIme (optional)	Authentication time out.	Default = 5 seconds.
Number of Authentication attempts	Authentication attempts.	Default = 2 seconds.
Dynamic access control security	Security control flag.	**E** = Enable **D** = Disable.
Port (1–4) Default DHCP Domain Index	Which domain's DHCP service will be used.	0 = no default.

Creating Default Route or Source Route on the DSL

Use this procedure to create a default route or source route for each DSL card (upstream direction). You can create up to 16 default or source routes per DSL card.

▶ Procedure

To create default routes or source routes on the DSL:

1. Select *Configuration* → *IP Router* → *Static_Routes* (**A-E-A**).
2. Press Return on the Item 0 field to add a new record.
3. Enter values for the following fields and press Return after each entry.

Field	Description	Input
Host/Net	Destination of the route.	*0.0.0.0* to indicate the default route
Subnet Mask	Associated subnet mask for the specified destination IP address.	*nnn.nnn.nnn.nnn* format
Next Hop	IP address of the next hop device for the specified destination.	*nnn.nnn.nnn.nnn* format
Pref (Preference)	Measure of how preferable one route is to another, if you have two routes going to the same destination. (The lower the number, the more preferable the route.) This route is compared to other routes for the same destination address.	*1*
S/D (Source/Destination)	Source or destination route type.	Default = Dst
PA (Proxy ARP)	Router answers ARP requests intended for another machine.	Default = No

4. Confirm the save and press Ctrl-z to return to the *Configuration* → *IP Router* menu.

MCC Card Configuration

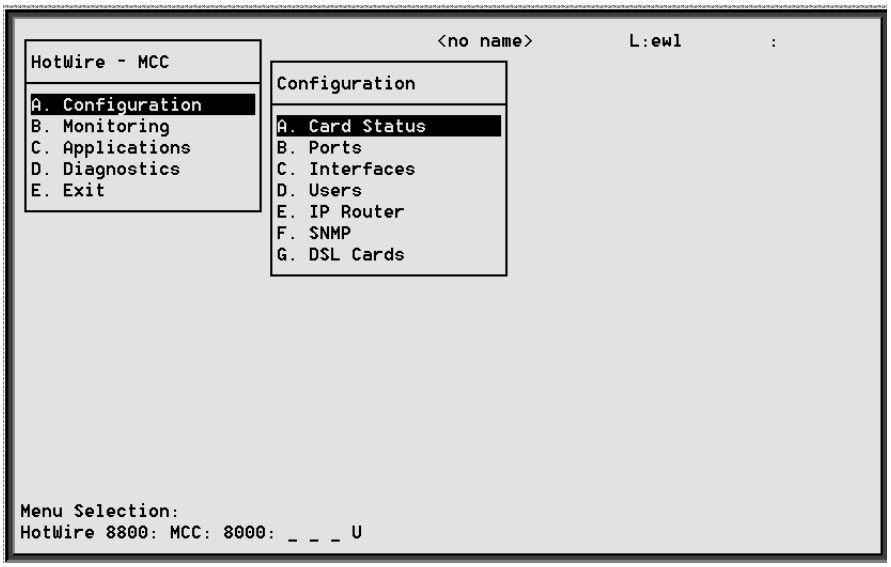
5

Overview

This chapter describes the configuration options on the MCC card. Use these options to customize your applications.

MCC Configuration Card Status Screens

Use the system information submenu of the Card Status screens to configure basic MCC card-level information.



NOTE:

Only a user who logs onto the HotWire DSLAM with Administrative permission can configure the MCC card.

▶ Procedure

To configure card information, DNS setup, time/date, clear NVRAM, upload or download configuration set, download new firmware, or reset card:

1. Follow this menu sequence:

   Configuration → *Card Status* (**A-A**)

2. The Card Status menu appears. Enter the desired value on each selected screen and field as shown in Table 5-1 and press Return.

Table 5-1. Card Status Menu Options (1 of 3)

Card Info (System Information)	**A-A-A**
Gives the user the ability to configure basic card-level information.	
System Name – 16 alphanumeric characters. Name assigned to the card.	
System Contact – 32 alphanumeric characters. Name or number of party responsible for card.	
System Location – 16 alphanumeric characters. Location assigned to the system.	
Router ID – (This field is read only.) Diagnostic Domain IP address assigned to card.	
Router Subnet Mask – (This field is read only.) *nnn.nnn.nnn.nnn* format.	
Local Control Terminal Port Mode – Standard/Extended (Default = Standard). Standard is for USA keyboards; Extended is for European keyboards.	
Remote Control Terminal Port Mode – Standard/Extended (Default = Standard). Standard is for USA keyboards; Extended is for European keyboards.	
Telnet daemon tcp port – 0–65536 (Default = 23). If you change this field, you need to do a card reset.	
Alarm on loss of Redundant Power – Enter Y if carrier has redundant power and you want local and remote indications of the loss of one power source.	
DNS Setup (Configure DNS)	**A-A-B**
Gives the user the ability to configure the access to DNS servers from which name to IP address translation requests are made.	
DNS Servers – Three entry fields in *nnn.nnn.nnn.nnn* format. Enter the primary Domain Name System Server address.	
Default Domain Name – 40 characters. Domain used for queries that are not fully qualified. For example, if the default domain name = paradyne.com and a telnet is attempted to reach a system called gemini, the card would query the DNS server for gemini.paradyne.com.	
Time to wait for response (**secs**) – 1– 15 seconds (Default = 5). Enter the time to wait for a response.	
Number of times to retry server – 1–3 times (Default = 2). Enter the number of times to retry the server.	

Table 5-1. Card Status Menu Options (2 of 3)

Time/Date	**A-A-C**
Gives the user the ability to configure the local time and date on the DSL card with network time and to synchronize the DSLAM's clock via a Network Time Protocol (NTP) server. **Local Time/Date** – Enter the time in *hh.mm* format (am or pm). Enter the date in *mm/dd/yy* format. **Client NTP Mode** – Broadcast/Unicast (Default = Broadcast). Select the Client Network Time Protocol Mode. **NTP Server** – *nnn.nnn.nnn.nnn* format. Enter the NTP Server IP address. **Synchronized(hrs)** – 1–24 (Default = 1). Enter the hours between synchronization.	
NVRAM Clear Screen (Clear NVRAM)	**A-A-D**
Gives the user the ability to clear out the Non-Volatile RAM (NVRAM) in order to reuse the card or to reconfigure the current card. CAUTION: If you select yes on this screen, you will permanently remove most of the configuration information you have stored on this card and all IP addresses and routing tables will have to be re-entered. The system will perform a reset and return to the factory configuration.	
NVRAM Config Loader	**A-A-E**
Gives the user the ability to upload or download a copy of the card's binary configuration data to or from a Trivial File Transfer Protocol (TFTP) server. **Configuration File Name** – The file name may be a regular path name expression of directory names separated by a forward slash (/) ending with the file name. The total path name length must be less than 40 characters. If the TFTP server is hosted by a DOS machine, then directory and file names must follow the 8.3 naming convention imposed by DOS. **DOS Machine** If your server is hosted by a DOS machine, you must name the file to be uploaded using the DOS convention eight-character length. The system will automatically upload the configuration file and create directories and file names as needed. **UNIX Machine** If your server is hosted by a UNIX machine, the configuration file you name **will not** be created on the UNIX system by the TFTP server. It is **critical** that you work with your system administrator to plan the naming conventions for directories, filenames, and permissions so that anyone using the system has read and write permissions. (This is a UNIX system security feature.) NOTE: This must be done before you can upload files to a UNIX server. **TFTP Server IP Address** – *nnn.nnn.nnn.nnn* format. **TFTP Transfer Direction** – Upload/Download (Default = Upload). Select Upload to store a copy of the card's configuration on the server. Select Download to have the file server send a copy of the stored configuration file to the card. **Start Transfer** – Yes/No (Default = No). **Packets Sent** – Number of packets sent in download. **Bytes Sent** – Number of bytes sent in download. **Bytes Received** – Number of bytes received in download. **Transfer Status** – Status of the upload or download transfer. NOTE: After a download, the card must be reset for the new configuration to take effect.	

Table 5-1. Card Status Menu Options (3 of 3)

Card Reset (Reset System)	**A-A-F**
Gives the user the ability to reset the card. This resets all counters and if a new configuration or software version has been downloaded, the new code will then become active. **Reset Card** – Enter Yes to reset card. NOTE: This action disrupts the data flow for at least 10 seconds.	
Download Code (Download Code and Apply Download)	**A-A-G**
Gives the user the ability to download a new version of code and apply the downloaded code. For further information on this feature, see Appendix C, *Download Code and Apply Download*.	
Download Code	**A**
This screen is similar to the NVRAM Config Loader screen. **Image File Name** – The file name may be a regular pathname expression of directory names separated by a forward slash (/) ending with the file name. The total pathname length must be less than 40 characters. If the TFTP server is hosted by a DOS machine, then directory and file names must follow the 8.3 naming convention imposed by DOS. **TFTP Server IP Address** – *nnn.nnn.nnn.nnn* format. **Start Transfer** – Yes/No (Default = No). **Packets Sent** – Number of packets sent in download. **Packets Received** – Number of packets received in download. **Bytes Sent** – Number of bytes sent in download. **Bytes Received** – Number of bytes received in download. **Transfer Status** – Status of the download transfer. Once the download is complete, press Ctrl-z to exit back to the Download Code submenu and select Apply Download.	
Apply Download	**B**
This selection applies the downloaded code and drops all connections by performing a device reset. This screen is used to overlay the previously downloaded image for the card. If you select yes at the **Reset System** prompt, the system goes through a system restart and interrupts service on the card. For further information on this feature, see Appendix C, *Download Code and Apply Download*. NOTE: If you have not previously downloaded code, then you will not be able to access this selection.	

MCC Configuration Ports Screens (Reserved for Future Use)

NOTE:

There are no configurable ports on the MCC at this time.

MCC Configuration Interfaces Screens

Use the system information submenu of the Interfaces screens to configure basic interface information.

▶ Procedure

To configure general interfaces, IP networks, and control interfaces:

1. Follow this menu sequence:

   Configuration → *Interfaces* (**A-C**)

2. The Interfaces menu appears. Enter the desired value on each selected screen and field as shown in Table 5-2 and press Return.

Table 5-2. Interfaces Menu Options (1 of 2)

General (Interfaces)	**A-C-A**
Gives the user the ability to configure basic information about a given interface.	
Interface Name – s1b = backplane that connects all the cards, e1a = Ethernet port.	
Type – Static.	
Protocol – Type of protocol for an interface.	
Port List – Name of the port associated with this interface.	
MTU (max) (Maximum Transmission Unit) – 64–64000 (Default = 1500). For the Model 8540, the MTU (max) is 1500, with the range being 61–1500.	
NOTE: The above MTU values are the only values you may enter. Do not change the MTU of s1b from the default of 1500. Make certain that if you change from the default value, the numbers are appropriate to your network. Do a card reset or reset the interface.	

Table 5-2. Interfaces Menu Options (2 of 2)

IP Network	**A-C-B**
Gives the user the ability to configure up to 16 IP addresses for the LAN port. However, under normal conditions, only one IP address in the management domain need be assigned. **IP Interface** – 15 characters. s1b = backplane that connects all cards; e1a = Ethernet port. **Base IP Addr** – *nnn.nnn.nnn.nnn* format. **Base Subnet Mask** – *nnn.nnn.nnn.nnn* format. **IP Addr** – *nnn.nnn.nnn.nnn* format. (You may enter up to 16 addresses.) Only appears if e1a is the IP interface name. **Subnet Mask** – *nnn.nnn.nnn.nnn* format. (You may enter up to 16 addresses.) Only appears if e1a is the IP interface name. **Input Filter** – Optional. **Output Filter** – Optional. **Peer IP Address** – *nnn.nnn.nnn.nnn* format. Only appears if s1b is the interface name. **Route to Peer** – Net. Only appears if s1b is the interface name. NOTE: If you have made any changes to this screen, you must do a card reset or restart the appropriate interface (e1a or s1b). For changes to the s1b interface, the peer IP address for each of the DSL ports (s1c, s1d, s1e, s1f) on each DSL card must be changed and saved. In addition, the DSL card must be reset.	
Control (Control Interface)	**A-C-C**
Gives the user the ability to restart, stop, and monitor (up, down, or testing) the current state of an interface. This screen is populated depending on your entry in the Command and Interface Name fields. For example, if you select Monitor mode and enter s1b for the Interface name, the following information is displayed: Type, State, Link Protocol, IP State, Uptime, Inactive, Connect Time, Port, Local IP Addr, and Peer IP Addr.	

MCC Configuration Users Screens

Use the system information submenu of the Users screens to configure login accounts for local terminal and telnet sessions.

▶ Procedure

1. Follow this menu sequence:

   Configuration → *Users* (**A-D**)

2. The Users menu appears. Enter the desired value on each selected screen and field as shown in Table 5-3 and press Return.

Table 5-3. Users Menu Options

Users (Configure Account)	**A-D-A**
Gives the user the ability to add, edit, or delete a user from a system account and to edit user passwords and privileges. Up to 10 active users can be supported. User accounts provide security for the DSLAM by requiring that anyone who is trying to log onto the system has a valid password to gain access. User accounts on the MCC provide security to users accessing the system from the VT100-compatible terminal interface and via Telnet over the management domain LAN. If no accounts are set up, then no login or password is required to gain entry to the system via the terminal interface or telnet. It is recommended that user accounts also be set up for each DSL card, even if you do not intend to telnet directly to the DSL cards, so that no unauthorized telnet sessions can be made. Each card will support up to 10 user accounts with either Operator (read only) or Administrator (read/write) permissions. If you configure an account on the MCC card, you have privileges on both the MCC and DSL cards. If you configure an account on the DSL card, you only have privileges for that specific DSL card and only via a Telnet session. **Action** – Add/Edit/Delete. **Login ID** – Enter your Login ID. **Password** – Enter the password associated with the login ID. **Repeat Password** – Re-enter the password. **Privilege** – Operator/Administrator. Enter Operator for read-only access; enter Administrator for complete system access. NOTE: Use Ctrl-v to see a list of all user accounts at the Login ID prompt.	

MCC Configuration IP Router Screens

Use the system information submenu of the IP Router screens to configure static routes to protocols and filters.

▶ Procedure

To configure static routes, martian networks, and IP router filters:

1. Follow this menu sequence:

   Configuration → *IP Router* (**A-E**)

2. The IP Router menu appears. Enter the desired value on each selected screen and field as shown in Table 5-4 and press Return.

Table 5-4. IP Router Menu Options (1 of 4)

Static Routes	**A-E-A**
Gives the user the ability to add or delete static routes in the system. You can add up to 32 static routes. **Item** – Press Return on 0 field to add entry. **Host/Net** – *nnn.nnn.nnn.nnn* format or space to delete entry. This field is read only for dynamic routes. **Subnet Mask** – Associated subnet mask for the specified destination IP address. This field is read only for dynamic routes. **Next Hop** – *nnn.nnn.nnn.nnn* format. This field is read only for dynamic routes. **Pref**– Measure of how preferable one route is to another, if you have two routes going to the same destination. (The lower the number, the more preferable.) This route is compared to others for the same address. This field is read only for dynamic routes. **S/D** (Source/Destination) – Source or destination IP address of the packet. This field is read only for dynamic routes. **PA** (Proxy ARP) – Router answers ARP requests intended for another machine. This field is read only for dynamic routes. NOTE: When you define a source route, the Proxy ARP field is no longer selectable.	
Martian Networks	**A-E-B**
Gives the user the ability to enter addresses that the system recognizes as invalid. **Item** – Press Return on 0 field to add entry. **Martian Net ID** – *nnn.nnn.nnn.nnn* format or space to delete entry. Enter IP address of unwanted source. **Martian Net Mask** – *nnn.nnn.nnn.nnn* format. Enter IP mask of unwanted source. NOTE: The system is shipped with default martian networks. It is recommended that you do not remove entries. If you have made changes to this screen, you must do a card reset.	

Table 5-4. IP Router Menu Options (2 of 4)

Filter Table	**A-E-C**
Displays an overview of the various filters that are in the system. The FIlter Table screen displays the following information: **Line** – Sequential number of line. **Filter Name** – Name of the IP filter. **# of Static Rules** – Number of static routes in filter. **# of Dynamic Rules** – Number of dynamic routes in filters. **Reference Count** – Number of active interfaces using the filter. **Default Action** – Default action for the filter. On the bottom of this screen, at the `Goto Line Number (0 to Add, #to Edit, -# to Delete)` prompt: ■ Select `0` to add a new filter to existing filters. ■ Select `#` to edit existing filters. ■ Select `-#` to delete a filter. The Add or Edit selection takes you to the IP Filter Configuration screen. When you exit that screen, you return to the Filter Table screen.	

Table 5-4. IP Router Menu Options (3 of 4)

IP Router Filters (IP Filter Configuration)	A-E-C
Gives the user the ability to build name sets of filter rules. A filter is a rule (or set of rules) that is applied to a specific interface to indicate whether a packet can be forwarded or discarded. You can add, edit, or delete router filter rules within a named set. View filter names by pressing Ctrl-v. A filter works by successively applying the rules to the information obtained from the packet header until a match is found. The filter then performs the action specified by the rule on that packet, which can be forwarded, discarded, or both. Rules apply to the source and destination ports going to the end-user system. You may have up to 33 rules per filter, but the greater number of rules, the lesser the performance of the router filter. On the MCC card, a maximum of two filters can be configured. For additional information on IP Router filters, see Chapter 7, *IP Filtering*, of the *HotWire DSLAM for 8540 and 8546 DSL Cards Network Configuration Guide*. **Action** – Add/Delete/Edit. **Filter Name** – Up to 16 characters (optional). **Default Filter Action** – Discard (Packet)/Forward (Packet). **Rule #** – Up to 33 rules can be configured for each filter. This number is automatically assigned. **# of Rules** – Number of rules that apply to this port. **Source Address** – *nnn.nnn.nnn.nnn* format. **Source Address Mask** – *nnn.nnn.nnn.nnn* format. If you specify a source subnet mask of 0.0.0.0, the system skips the source address comparison. **Source Port No** – 0–65536 (Default = 0). If the source port number is 0, the system filters ICMP packets in addition to the packet types defined in the rule. **Comparison Type** – Ignore – Do not do a comparison. To do a comparison on the port number specified in the packet and the rule, specify one of the following: Ignore – Ignore ports. EQ – Equal to, NEQ – Not Equal To, GT – Greater than, LT – Less than, In_Range – Within the specified range, Out_Range – Outside of the specified range. **Destination Address** – *nnn.nnn.nnn.nnn* format. **Destination Address Mask** – *nnn.nnn.nnn.nnn* format. If you specify a destination subnet mask of 0.0.0.0, the system skips the destination address comparison. **Destination Port No** – 0–65536 (Default = 0). If the source port number is 0, the system filters ICMP packets in addition to the packet types defined in the rule. **Comparison Type** – Ignore – Ignore ports, EQ – Equal to, NEQ – Not Equal To, GT – Greater than, LT – Less than, In_Range – Maximum source port, Out_Range – Minimum source port. **Filter Action** – Discard (Packet)/Forward (Packet). **Rule Type** – Static/Dynamic (Default = Static). **Delete Rule** – Yes/No. **Go to Rule Number** – Default = 0.	

Table 5-4. IP Router Menu Options (4 of 4)

ARP (Parameters, Add Entry, and Delete Entry)	**A-E-D (A-E-A to A-E-C)**

Select:

Parameters (A)

Gives the user the ability to configure general Address Resolution Protocol (ARP) cache parameters.

Complete Entry Timeout (minutes) – 1–200,000 (Default = 20).

Incomplete Entry Timeout (minutes) – 1–200,000 (Default = 20).

NOTE: If you have made changes to this screen, you must do a card reset.

Add Entry (Add ARP Entry) (B)

Gives the user the ability to add entries into the ARP cache.

IP Address/Host Name – *nnn.nnn.nnn.nnn* format.

MAC Address – *xx-xx-xx-xx-xx-xx* format.

Trailers – Yes/No (Default = No).

Proxy – Yes/No (Default = No).

PERM – Yes/No (Default = No). If you select yes for Perm and no to proxy, the ARP entry will be saved in NVRAM (up to 32 entries; 8 for the MCC). These are loaded when the card reboots.

Add Entry? – Enter Yes to add an entry or exit.

Add Another Entry? – Enter Yes to add another entry.

Delete Entry (Delete ARP Entry) (C)

Gives the user the ability to delete entries line by line in the ARP cache. The screen displays columns for Line, IP Address, Ethernet Address, Min, and Delete.

Select the line you want to delete, select Yes and press Return.

NOTE: For the Add and Delete ARP Entry screens, any information entered is not stored in the NV memory and will be lost when you reset the card.

Host Table (IP Host Table)	**A-E-E**

Gives the user the ability to define mappings between IP addresses and host names. The host table can be used to hold the host name to IP address translation for telnet sessions out from the card. An alternative to populating this table is to define a DNS server (see **A-A-B**).

Enter the IP Address and Host Name in *nnn.nnn.nnn.nnn* format and press Return after each entry.

NOTE: You have to confirm the save for any changes to take effect**.**

MCC Configuration SNMP Screens

Use the system information submenu of the SNMP screens to configure SNMP security, logical entities, community names, and trap addresses.

▶ Procedure

To configure SNMP security, SNMP Logical entities, and SNMP Communities/Traps:

1. Follow this menu sequence:

   Configuration → *SNMP* (**A-F**)

2. The SNMP appears. Enter the desired value on each selected screen and field as shown in Table 5-5 and press Return.

Table 5-5. SNMP Menu Options (1 of 2)

Security (SNMP Security) **A-F-A**
Gives the user the ability to configure allowable NMS IP addresses and to configure SNMP agent. Although SNMP community strings (if they are changed from the defaults) provide a measure of security for unauthorized managers, enabling IP address security and entering the IP address of up to five authorized SNMP managers provides a much higher level of security. When IP address security is enabled, the source address of any SNMP message addressed to any of the card's IP addresses (in either the management or service domain) will be checked against the authorized list and will be dropped if there is no match. **IP Address Security** – Enable/Disable (Default = Disable). ■ Enabling allows DSLAM to accept SNMP messages from SNMP managers whose IP source addresses have been entered in the IP Address field. NOTE: If enabled with no IP address specified or with all addresses set to No Access (NA) permission, then there is no SNMP connectivity to the MCC card. ■ Disabling stops IP address checking and allows the card to respond to a SNMP query from any source with a proper community string. **IP Address** – *nnn.nnn.nnn.nnn* format. Enter up to five IP source addresses of NMS managers. **Access** – ReadOnly(ro)/ReadWrite(rw)/NoAccess(na). Permission to be granted to each NMS manager.
Logical Entities (SNMP Logical Entities) **A-F-B**
This screen displays default system information contained in the logical table of the Entity MIB. Only the Community Name fields can be edited; others are read only. ■ **I** (Index) column shows the index number of DSL cards 1 through 18. ■ **T** (Type) column shows "D" for DSL cards. ■ **Read Only Comm** and **Read Write Comm** show the community strings of the DSL cards present in that slot.
Logical Entities 2 (SNMP Logical Entities 2) **A-F-C**
Continuation of previous screen.

Table 5-5. SNMP Menu Options (2 of 2)

Communities/Traps (SNMP Communities/Traps)	**A-F-D**
Gives the user the ability to enable the Authentication Failure Trap Mechanism, stores SNMP Community string names for the DSL card, and stores NMS host IP addresses to which the DSLAM sends trap messages. It also lets the user configure four communities with three trap destinations each. This can be for a total of up to 12 destinations. **Authentication Failure Trap** – Enable to send a trap when a SNMP request community string does not match or when the password for a Telnet session is incorrect. **Community Name** – 32 characters, up to four unique entries per screen. Default names are public (ro), mcc (rw), nms (rw), nms-2 (ro). **Access** – ReadOnly(ro)/ReadWrite(rw)/NoAccess(na), up to four entries per screen. **IP Address** – *nnn.nnn.nnn.nnn* format. Enter NMS system host address. **Input Number (port)** – *nnn* format. Enter NMS system port number. **Send Traps** – Set to E to Enable traps to be sent to this address. Set to D to disable.	

MCC DSL Cards Screen

Use the system information submenu of the DSL Cards screen to set IP addresses and reset the DSL cards.

▶ Procedure

To Configure DSL IP addresses and Reset DSL Slot:

1. Follow this menu sequence:

   Configuration → *DSL Cards* (**A-G**)

2. The DSL Cards menu appears. Enter the desired value on each selected on each selected screen and field as shown in Table 5-6 and press Return.

Table 5-6. DSL Options

Set IP Address (Configure DSL IP Addr) **A-G-A**
You must assign up to 18 IP addresses in the management domain, one for each slot in the DSLAM that has a DSL card. These are addresses for the s1b backplane interface on each DSL card and will be automatically assigned to the DSL card when it is inserted in a slot. All IP addresses must be on the same Management Domain Subnet as the MCC's IP address (entered on the MCC's IP Network screen **A-C-B**). **DSL Card Subnet Mask** – *nnn.nnn.nnn.nnn* format. **Slot** – Slot number of the DSL card. **IP Address** – *nnn.nnn.nnn.nnn* format. (Subnet is predetermined – you can enter the host number.) NOTE: If you have made changes to this screen, you must do a card reset or restart the s1b interface. Also, do not assign the same subnets as those used for the e1a (Ethernet) service domains.
Reset Slot (Reset DSL Slot) **A-G-B**
Gives the user the ability to perform a reset of a DSL card in any DSLAM slot. This reset should be performed if there is a card in a slot but it does not appear on the DSLAM card selection screen. After entering the card number, selecting the command that will be sent (ForceBootP or reset), and confirming the reset, the MCC sends a reset signal via the backplane to the selected card. Your choices on this screen allow you to ForceBootP (a nondisruptive reset), Reset (a minor disruption of less than 30 seconds), or Clear NVRAM (resets card and restores factory default settings). **DSL Card/Slot #** – Slot number of the DSL card. **Command** – ForceBootP/Reset. ForceBootP will only work for certain cards (e.g., with T1 and E1 connections). **Clear NVRAM also** – Yes/No.***** NOTE: If a DSL card has been reset but still does not appear on the screen, its configuration may have been corrupted and the card should be reset again, this time answering yes at the Clear NVRAM prompt. If the card then appears on the screen, it will have to be reconfigured. If the card does not appear on the screen, it should probably be replaced.
***** If you select yes on this screen, you will permanently remove most of the configuration information you have stored on this card and all IP addresses and routing tables will have to be reentered. The system will perform a reset and return to the factory settings.

DSL Card Configuration

6

Overview

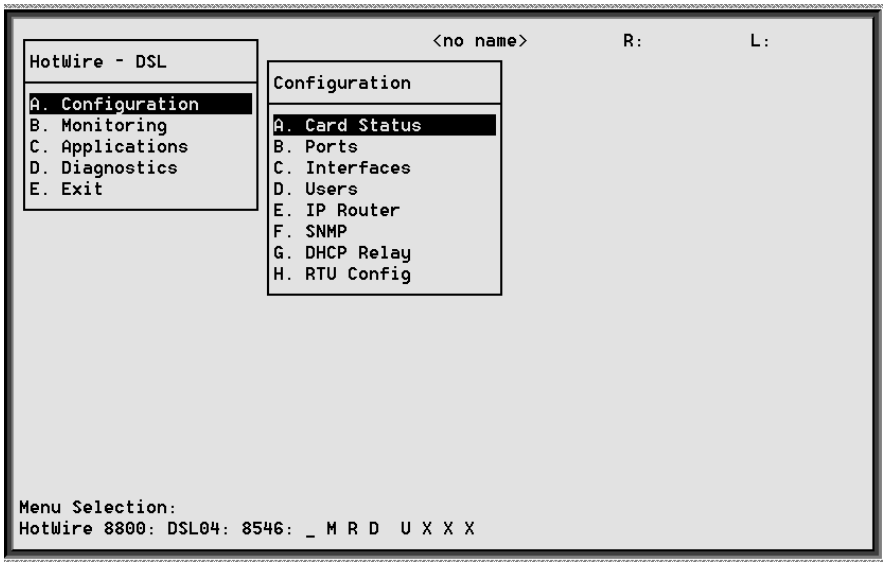
This chapter describes the non-mandatory configuration options on the DSL card. Use these options to customize your applications.

NOTE:

Certain parameters such as speeds are dependent on the settings on the RTU Configuration screen. Go to *Configuration* → *RTU Config* (**A-H**) and select your RTU type for each port before any additional configuration activities.

DSL Configuration Card Status Screens

Use the system information submenu of the Card Status screens to configure basic DSL card-level information.



NOTE:

Only a user who logs on to the HotWire DSLAM with Administrative permission can configure the DSL card.

▶ Procedure

To configure card information, DNS setup, time/date, clear NVRAM, upload or download configuration set, download new firmware, or reset card:

1. Follow this menu sequence:

   Configuration → *Card Status* (**A-A**)

2. The Card Status menu appears. Enter the desired value on each selected screen and field as shown in Table 6-1 and press Return.

Table 6-1. Card Status Options (1 of 4)

Card Info (System Information)	**A-A-A**
Gives the user the ability to configure basic card-level information. **System Name** – 16 alphanumeric characters. Name assigned to the card. **System Contact** – 32 alphanumeric characters. Name or number of party responsible for card. **System Location** – 16 alphanumeric characters. Location assigned to the card. **Router ID** – *nnn.nnn.nnn.nnn* format. (This field is read only.) Diagnostic Domain IP address assigned to card by the MCC. **Router Subnet Mask** – *nnn.nnn.nnn.nnn* format. (This field is read only.) **Local Control Terminal Port Mode** – Standard/Extended (Default = Standard). Standard is for USA keyboards; Extended is for European keyboards. **Remote Control Terminal Port Mode** – Standard/Extended (Default = Standard). Standard is for USA keyboards; Extended is for European keyboards. **Telnet daemon tcp port** – 0–65536 (Default = 23). If you change this field, you need to do a card reset.	
DNS Setup (Configure DNS)	**A-A-B**
Gives the user the ability to configure the access to DNS servers from which name to IP address translation requests are made. **DNS Servers** – Three entry fields in *nnn.nnn.nnn.nnn* format. Enter the primary Domain Name System Server address. **Default Domain Name** – 40 characters. Domain used for queries that are not fully qualified. For example, if the default domain name = paradyne.com and a telnet is attempted to reach a system called gemini, the card would query the DNS server for gemini.paradyne.com. **Time to wait for response** – 1–15 seconds (Default = 5). Enter the time to wait for a response. **Number of times to retry server** – 1–3 times (Default = 2). Enter the number of times to retry the server.	

Table 6-1. Card Status Options (2 of 4)

Time/Date	**A-A-C**
Gives the user the ability to configure the local time and date on the DSL card with network time and to synchronize the DSLAM's clock via a Network Time Protocol (NTP) server. **Local Time/Date** – Enter the time in *hh.mm* format (am or pm). Enter the date in *mm/dd/yy* format. **Client NTP Mode** – Broadcast/Unicast (Default = Broadcast). Select the Client Network Time Protocol (NTP) Mode. **NTP Server** – *nnn.nnn.nnn.nnn* format. Enter the NTP Server IP address. **Synchronized(hrs)** – 1–24 (Default = 1). Enter the hours between synchronization. NOTE: At system boot time, the time on the DSL cards automatically synchronizes with the MCC card. Therefore it is usually not necessary to use this screen on the DSL card.	
NVRAM Clear Screen (Clear NVRAM)	**A-A-D**
Gives the user the ability to clear out the Non-Volatile RAM (NVRAM) in order to reuse the card or to reconfigure the current card. CAUTION: If you select yes on this screen, you will permanently remove most of the configuration information you have stored on this card and all IP addresses and routing tables will have to be re-entered. The system will perform a reset and return to the factory configuration.	

Table 6-1. Card Status Options (3 of 4)

NVRAM Config Loader	**A-A-E**
Gives the user the ability to upload or download a copy of the card's binary configuration data to or from a Trivial File Transfer Protocol (TFTP) server. **Configuration File Name** –The file name may be a regular path name expression of directory names separated by a forward slash (/) ending with the file name. The total path name length must be less than 40 characters. If the TFTP server is hosted by a DOS machine, then directory and file names must follow the 8.3 naming convention imposed by DOS. **DOS Machine** If your server is hosted by a DOS machine, you must name the file to be uploaded using the DOS convention eight-character length. The system will automatically upload the configuration file and create directories and file names as needed. **UNIX Machine** If your server is hosted by a UNIX machine, the configuration file you name **will not** be created on the UNIX system by the TFTP server. It is **critical** that you work with your system administrator to plan the naming conventions for directories, filenames, and permissions so that anyone using the system has read and write permissions. (This is a UNIX system security feature.) NOTE: This must be done before you can upload files to a UNIX server. **TFTP Server IP Address** – *nnn.nnn.nnn.nnn* format. **TFTP Transfer Direction** – Upload/Download (Default = Upload). Select Upload to store a copy of the card's configuration on the server. Select Download to have the file server send a copy of the stored configuration file to the card. **Start Transfer** – Yes/No (Default = No). **Packets Sent** – Number of packets sent in download. **Bytes Sent** – Number of bytes sent in download. **Bytes Received** – Number of bytes received in download. **Transfer Status** – Status of the upload or download transfer. NOTE: After a download, the card must be reset for the new configuration to take effect.	
Card Reset (Reset System)	**A-A-F**
Gives the user the ability to reset the card. This resets all counters and if a new configuration or software version has been downloaded, the new code will then become active. NOTE: This action disrupts the data flow for at least 30 seconds.	

Table 6-1. Card Status Menu Options (4 of 4)

Download Code (Download Code and Apply Download)	**A-A-G**
Gives the user the ability to download a new version of code and apply the downloaded code. For further information on this feature, see Appendix C, *Download and Apply Download*.	
Download Code	**A**
This screen is similar to the NVRAM Config Loader screen. **Image File Name** – The file name may be a regular pathname expression of directory names separated by a forward slash (/) ending with the file name. The total pathname length must be less than 40 characters. If the TFTP server is hosted by a DOS machine, then directory and file names must follow the 8.3 naming convention imposed by DOS. **TFTP Server IP Address** – *nnn.nnn.nnn.nnn* format. **Start Transfer** – Yes/No (Default = No). **Packets Sent** – Number of packets sent in download. **Packets Received** – Number of packets received in download. **Bytes Sent** – Number of bytes sent in download. **Bytes Received** – Number of bytes received in download. **Transfer Status** – Status of the download transfer. Once the download is complete, press Ctrl-z to exit back to the Download Code submenu and select Apply Download.	
Apply Download	**B**
This selection applies the downloaded code and drops all connections by performing a device reset. This screen is used to overlay the previously downloaded image for the card. If you select yes at the Reset System prompt, the system goes through a system restart and interrupts service on the card. For further information on this feature, see Appendix C, *Download and Apply Download*. NOTE: If you have not previously downloaded code, then you will not be able to access this selection.	

DSL Configuration Ports Screens

Use the system information submenu of the Ports screens to display the DSL Ports screen.

▶ Procedure

To configure DSL ports:

1. Follow this menu sequence:

   Configuration → *Ports* (**A-B**)

2. The Ports menu appears. Enter the desired value on each selected screen and field and press Return.

Table 6-2. Ports Options (1 of 2)

Ethernet Port	**A-B-A**
Gives the user the ability to configure the Ethernet Port. **Port Name** – Enter the port name (up to 7 characters). **Full Duplex** – Enable/Disable. (Default = Disable) **Function** – Edit/Reset. Select Reset to have changes become active.	
DSL Ports (DSL Parameters)	**A-B-B**
Gives the user the ability to configure the operational and alarm parameters of the DSL ports. Each DSL port is configured separately. **Action** – Edit/Reset. Edit to configure the DSL ports, Reset to reset the port and make changes active. **Port #** – Enter port 1 to 4. (Default = 0) **Port Desc** – 40 characters (User Name, telephone number, circuit id of DSL loop, etc.). **Tx Power Attenuation** – 0db, –3db, –6db. Enter the rate that allows you to reduce the transmit power by: –3 or –6 db. (Default = 0db) **Startup Margin** – The Startup Margin field is used to determine the quality of the connection of the upstream link on system startup. It is used in conjunction with the adaptive speed fields to determine the initial line speeds of the DSL link. The value is between –3 and 9. In Adaptive Mode, if the margin falls below SM, the DSL link will be restarted at a slower speed. If the calculated margin of the next speed is greater than SM by 3db, the speed will increase. Enter –3 to 9. (Default = 3)	

Table 6-2. Ports Options (2 of 2)

DSL Ports (DSL Parameters) (Continued)	A-B-B
Behavior – Fixed/Adaptive (Default = Adaptive). In fixed rate mode, the DSL will operate at the specified up and down speed. In rate adaptive mode, the rates will not exceed the maximum speed and traps are sent when the links drop below the minimum, as the transmission characteristics of the loop change. **RTU Type** – Model number of endpoint. For Model 8540, selections are 5170/5171/5246/5216 (Default = 5216). For Model 8546, selections are 5446r1/5446r2/5546 (Default = 5446r2). **Fixed: Down Speed*** – 7168/6272/5120/4480/3200/2688/2560/2240/1920/1600/1280/960/640 (Default = 2560). Enter the fixed down speed. (Not all speeds are available for all RTUs.) **Fixed: Up Speed** – 1088/952/816/680/544/408/272/91 (Default = 1088). Enter the fixed up speed. **Adaptive: Max Dn Speed*** – 7168/6272/5120/4480/3200/2688/2560/2240/1920/1600/1280/960/640 (Default = 2560). Enter the maximum down speed. (Not all speeds are available for all RTUs.) **Adaptive: Min Dn Speed*** – 7168/6272/5120/4480/3200/2688/2560/2240/1920/1600/1280/960/640 (Default = 640). Enter the minimum down speed. (Not all speeds are available for all RTUs.) **Adaptive: Max Up Speed*** – 1088/952/816/680/544/408/272/91 (Default = 1088). Enter the maximum up speed. **Adaptive: Min Up Speed** – 1088/952/816/680/544/408/272/91 (Default = 272). Enter the minimum up speed. **Margin Threshold:** – Sends a trap message if the margin on either end falls below a selected value. Enter a value for the margin threshold trap (–5 to +10 db) (Default = +3). Enter D to disable trap. **Link Down Ct:** – Sends a trap message if the number of DSL link down events in 15 minutes exceeds the selected value. Enter a value for the Link Down Count Trap (0 to 1000). Enter D to disable trap. **Error Rate (secs)** – Sends a trap message if the 10 second average of the upstream block error rate exceeds the threshold value. (Default = 1.00–E–03) Enter a value for the threshold (two to 10 = negative exponent of error rate.) The default of five approximates the bit error rate of 10^{-8}, if the block length = 128 bytes. To disable the trap, enter d. Traps received because this threshold was crossed provide an indication of conditions that cause short duration bursty errors. Because the block error rate is only averaged over 10 seconds, the precision of this measure is not as good as the hourly block error measure. Therefore, this threshold should not be set to detect a higher error rate than the hourly threshold. **Error Rate (hr)** – Sends a trap message if the 1 hour average of the upstream block error rate exceeds the selected value. (Default = 1.00–E–04) Enter a value for the threshold (two to 10 = negative exponent of error rate.) The default of six approximates the bit error rate of 10^{-9}, if the block length = 128 bytes. To disable the trap, enter d. Bit error rate can be estimated and correlated with the bit error rate predicted by the upstream margin if you know what your average block size is in the upstream direction. (A margin of 6dB corresponds to a bit error rate of 10^{-7}.) NOTE: If you have made changes to this screen, select Reset in the Action field to make the changes active.	
* If you select a downstream speed of 2688 or higher, your upstream speed selection is limited to 1088/952/680/408.	

DSL Configuration Interfaces Screens

Use the system information submenu of the Interfaces screens to configure basic interface information.

▶ Procedure

To configure interface names and MTU settings, IP addresses on the ethernet port, PPP settings on the DSL ports, or restart, stop, or monitor an interface:

1. Follow this menu sequence:

   Configuration → *Interfaces* (**A-C**)

2. The Interfaces menu appears. Enter the desired value on each selected screen and field as shown in Table 6-3 and press Return.

Table 6-3. Interfaces Options (1 of 3)

General (Interfaces)	**A-C-A**
Gives the user the ability to view basic card interface information or to configure Maximum Transfer Units (MTUs). **Interface Name** – 15 characters. s1b = backplane that connects all the cards; e1a = ethernet port; s1c, s1d, s1e and s1f = DSL interface. Depending on your selection in this field, the following pre-populated fields appear: **Type** – Static or dynamic. **Protocol** – HDLC, PPP, or Ether. For the 8540, the protocol is Ether-HDLC. **Port List** – Name of the port associated with this interface. **MTU (max)** – 64–64000 (Default = 1500). For the 8540, the MTU (max) is 1500, with the range being 61–1500. NOTE: The above MTU values are the only values you may enter. Do not change the MTU of s1b from the default of 1500. Make certain that if you change from the default value, the new numbers are appropriate to your network. Do a card reset or reset the Ethernet interface.	

Table 6-3. Interfaces Options (2 of 3)

IP Network	**A-C-B**
Gives the user the ability to configure up to 16 IP addresses for a port. Configure one IP address for each service domain on the DSL card. **IP Interface** – 15 characters. s1b = backplane; e1a = ethernet port; s1c, s1d, s1e, and s1f = DSL ports. **Base IP Addr** – *nnn.nnn.nnn.nnn* format. (This field is read only.) **Base Subnet Mask** – *nnn.nnn.nnn.nnn* format. (This field is read only.) **IP Addr** – *nnn.nnn.nnn.nnn* format. (You may enter up to 16 addresses for LANs.) Only appears if e1a is the IP interface name. **Subnet Mask** – *nnn.nnn.nnn.nnn* format. (You may enter one for each address above.) Only appears if e1a is the IP interface name. **Input Filter** – Optional. **Output Filter** – Optional. **Peer IP Address*** – *nnn.nnn.nnn.nnn* format. **Route to Peer*** – Net or Host. Must be Net for s1b. NOTE: If you have made any changes to this screen, you must do a card reset or restart the Ethernet interface.	
Control (Control Interface)	**A-C-C**
Gives the user the ability to restart, stop, and monitor (up, down, or testing) the current state of an interface. This screen is populated depending on your entry in the Command and Interface Name fields. For example, if you select Monitor mode and enter s1b for the Interface name, the following information is displayed: Type, State, Link Protocol, IP State, Uptime, Inactive, Connect Time, Port, Local IP Addr, and Peer IP Addr.	
* Field does not appear if the card is an 8540 or if e1a is the IP interface name.	

Table 6-3. Interfaces Options (3 of 3)

PPP	**A-C-D**
Gives the user the ability to configure parameters for the PPP links used for the DSL connections. For the 8540, there is no PPP submenu. **Interface Name** – s1c, s1d, s1e, or s1f. **Restart Timer** – 1–10000 in seconds (Default = 3). **Max Terminates** – (Default = 2). **Max Configures** – Maximum number of PPP links (Default = 10). **Max Naks** – Maximum number of negative acknowledgments before PPP link goes down (Default = 10). **Negotiate Options** The following values should not be changed: **MRU:** no **ACCM:** no **MAGIC**: no **Quality:** no **PFC:** no **ACFC:** no **Option Values** **Local MRU (max)** – 64–64000 bytes (Default = 1500) **ACCM:** Default = FFFFFFFF **LQR Freq:** Default = 10 **Link Options** **Trace:** on/off/raw/decode (Default = off). This field is for field service use only and should not be turned on. **Echo Probe:** yes/no (Default = no) **Option Values** **Echo Freq:** Default = 10 **Echo Policy:** Default = 5 NOTE: While most of the fields on this screen are pre-populated, the values can be changed.	

DSL Configuration Users Screens

Use the system information submenu of the Users screens to configure login accounts for telnet sessions directly to the DSL cards.

▶ Procedure

1. Follow this menu sequence:

   Configuration → *Users* (**A-D**)

2. The Users menu appears. Enter the desired value on each selected screen and field as shown in Table 6-4 and press Return.

Table 6-4. Users Options

Users (Configure Account)	**A-D-A**
Gives the user the ability to add, edit, or delete a user from a system account and to edit user passwords and privileges. Up to 10 active users can be supported. User accounts provide security for the DSLAM by requiring that anyone who is trying to log onto the system has a valid password to gain access. User accounts on the MCC provide security to users accessing the system from the VT100-compatible terminal interface and via Telnet over the management domain LAN. If no accounts are set up, then no login or password is required to gain entry to the system via the terminal interface or telnet. It is recommended that user accounts also be set up for each DSL card, even if you do not intend to telnet directly to the DSL cards, so that no unauthorized telnet sessions can be made. Each card will support up to 10 user accounts with either Operator (read only) or Administrator (read/write) permissions. If you configure an account on the MCC card, you have privileges on both the MCC and DSL cards. If you configure an account on the DSL card, you only have privileges for that specific DSL card and only via a Telnet session. **Action** – Add/Edit/Delete. **Login ID** – Enter your login ID. **Password** – Enter the password associated with the login ID. **Repeat Password** – Re-enter your password. **Privilege** – Operator/Administrator. Enter Operator for read-only access; enter Administrator for complete system access. NOTE: Use Ctrl-v to see a list of all user accounts at the login ID prompt.	

DSL Configuration IP Router Screens

Use the system information submenu of the IP Router screens to configure static routes to protocols and filters.

▶ Procedure

To configure static routes, martian networks, and IP router filters:

1. Follow this menu sequence:

   Configuration → *IP Router* (**A-E**)

2. The IP Router menu appears. Enter the desired value on each selected screen and field as shown in Table 6-5 and press Return.

Table 6-5. IP Router Options (1 of 4)

Static Routes	**A-E-A**
Gives the user the ability to add or delete static routes in the system. For the management domain, static routes must be provided to the MCC and the RTUs. For the service domain, static routes must be provided upstream to the next hop route and downstream to those hosts that require static routes. **Item** – Press Return on 0 field to add entry. **Host/Net** – *nnn.nnn.nnn.nnn* format or space to delete entry. This field is read only for dynamic routes. **Subnet Mask** – Associated subnet mask for the specified destination IP address. On Model 8540, 255.255.255.255 is the subnet mask for routes to the RTUs. This field is read only for dynamic routes. **Next Hop** – *nnn.nnn.nnn.nnn* format. On Model 8540, the next hop is DSL port name s1c, s1d, s1e, or s1f. This field is read only for dynamic routes. **Pref** – Measure of how preferable one route is to another, if you have two routes going to the same destination. (The lower the number, the more preferable.) This route is compared to others for the same address. This field is read only for dynamic routes. **S/D** (Source/Destination) – Source or destination IP address of the packet. This field is read only for dynamic routes. **PA** (Proxy ARP) – Router answers ARP requests intended for another machine. This field is read only for dynamic routes. NOTE: When you define a source route, the Proxy ARP field is no longer selectable.	
Martian Networks	**A-E-B**
Gives the user the ability to configure addresses that the system recognizes as invalid. **Item** – Press Return on 0 field to add entry. **Martian Net ID** – *nnn.nnn.nnn.nnn* format or space to delete entry. Enter IP address of unwanted source. **Martian Net Mask** – *nnn.nnn.nnn.nnn* format. Enter IP mask of unwanted source. NOTE: The system is shipped with default martian networks. It is recommended that you do not remove entries. If you have made changes to this screen, you must do a card reset.	

Table 6-5. IP Router Options (2 of 4)

Filter Table	**A-E-C**
Displays an overview of the various filters that are in the system. The FIlter Table screen displays the following information: **Line** – Sequential number of line. **Filter Name** – Name of the IP filter. **# of Static Rules** – Number of static routes in filter. **# of Dynamic Rules** – Number of dynamic routes in filters. **Reference Count** – Number of active interfaces using the filter. **Default Action** – Default action for the filter. On the bottom of this screen, at the `Goto Line Number (0 to Add, #to Edit, -# to Delete) prompt:` ■ Select `0` to add a new filter to existing filters. ■ Select `#` to edit existing filters. ■ Select `-#` to delete a filter. The Add or Edit selection takes you to the IP Filter Configuration screen. When you exit that screen, you return to the Filter Table screen.	

Table 6-5. IP Router Options (3 of 4)

IP Router Filters (IP Filter Configuration)	A-E-C
Gives the user the ability to build name sets of filter rules. A filter is a rule (or set of rules) that is applied to a specific interface to indicate whether a packet can be forwarded or discarded. You can add, edit, or delete router filter rules within a named set. A filter works by successively applying the rules to the information obtained from the packet header until a match is found. The filter then performs the action specified by the rule on that packet, which can be forwarded, discarded, or both. Rules apply to the source and destination ports going to the end-user system. You may have up to 33 rules per filter, but the greater number of rules, the lesser the performance of the router filter. On the DSL card, a maximum of 8 filters can be configured. For additional information on IP Router filters, see Chapter 7, *IP Filtering*, of the *HotWire DSLAM for 8540 and 8546 DSL Cards Network Configuration Guide*. **Action** – Add/Delete/Edit. **Filter Name** – Up to 16 characters (optional). **Default Filter Action** – Discard (Packet)/Forward (Packet). **Rule #** – Up to 33 rules can be configured for each filter. This number is automatically assigned. **# of Rules** – Number of rules that apply to this port. **Source Address** – *nnn.nnn.nnn.nnn* format. This field is read only for dynamic filers. **Source Address Mask** – *nnn.nnn.nnn.nnn* format. If you specify a source subnet mask of 0.0.0.0, the system skips the source address comparison. This field is read only for dynamic filters. **Source Port No** – 0–65536 (Default = 0). If the source port number is 0, the system filters ICMP packets in addition to the packet types defined in the rule. This field is read only for dynamic filters. **Comparison Type** – Ignore – Do not do a comparison. To do a comparison on the port number specified in the packet and the rule, specify one of the following: EQ – Equal to, NEQ – Not Equal To, GT – Greater than, LT – Less than, In_Range – Within the specified range, Out_Range – Outside of the specified range. This field is read only for dynamic filters. **Destination Address** – *nnn.nnn.nnn.nnn* format. This field is read only for dynamic filters. **Destination Address Mask** – *nnn.nnn.nnn.nnn* format. If you specify a destination subnet mask of 0.0.0.0, the system skips the destination address comparison. This field is read only for dynamic filters. **Destination Port No.** – 0–65536 (Default = 0). If the source port number is 0, the system filters ICMP packets in addition to the packet types defined in the rule. This field is read only for dynamic filters. **Comparison Type** – Ignore – Ignore ports, EQ – Equal to, NEQ – Not Equal To, GT – Greater than, LT – Less than, In_Range – Maximum source port, Out_Range – Minimum source port. This field is read only for dynamic filters. **Filter Action** – Discard (Packet)/Forward (Packet). This field is read only for dynamic filters. **Rule Type** – Static/Dynamic (Default = Static). This field is read only for dynamic filters. **Delete Rule** – Yes/No. **Go to Next Rule** – Yes/No.	

Table 6-5. IP Router Options (4 of 4)

ARP (Parameters, Add Entry, and Delete Entry)	**A-E-D (A-E-A to A-E-C)**
Select: **Parameters (A)** Gives the user the ability to configure general Address Resolution Protocol (ARP) cache parameters. **Complete Entry Timeout (minutes)** – 1–200000 (Default = 20). **Incomplete Entry Timeout (minutes)** – 1–200000 (Default = 20). NOTE: If you have made changes to this screen, you must do a card reset. **Add Entry (Add ARP Entry) (B)** Gives the user the ability to add entries into the ARP cache. **IP Address/Host Name** – *nnn.nnn.nnn.nnn* format. **MAC Address** – *xx-xx-xx-xx-xx-xx* format. **Trailers** – Yes/No (Default = No). **Proxy** – Yes/No (Default = No). **Perm** – Yes/No (Default = No). If you select yes for Perm and no to proxy, the ARP entry will be saved in NVRAM (up to 32 entries). These are loaded when the card reboots. **Add Entry** – Enter Yes to add an entry or exit. **Add Another Entry** – Enter Yes to add another entry. **Delete ARP Entry (Delete ARP Entry)(C)** Gives the user the ability to delete entries line by line in the ARP cache. The screen displays columns for Line, IP Address, Ethernet Address, Min, and Delete. Select the line you want to delete, select Yes/No, and press Return. NOTE: For the Add and Delete ARP Entry screens, any information entered is not stored in the NV memory and will be lost when you reset the card.	
Host Table (IP Host Table)	**A-E-E**
Gives the user the ability to define mappings between IP addresses and host names. The host table can be used to hold the host name to IP address translation for telnet sessions out from the card. An alternative to populating this table is to define a DNS server (see **A-A-B**). Enter the IP Address and Host Name in *nnn.nnn.nnn.nnn* format and press Return after each entry. NOTE: You have to confirm the save for any changes to take effect	

DSL Configuration SNMP Screens

Use the system information submenu of the SNMP screens to configure SNMP security, logical entities, community names, and trap addresses.

▶ Procedure

1. Follow this menu sequence:

   Configuration → *SNMP* (**A-F**)

2. The SNMP menu appears. Enter the desired values on the selected screen and field as shown in Table 6-6 and press Return.

Table 6-6. SNMP Options (1 of 2)

Security (SNMP Security) **A-F-A**
Gives the user the ability to configure allowable NMS IP addresses and to configure SNMP agent. Although SNMP community strings (if they are changed from the defaults) provide a measure of security for unauthorized managers, enabling IP address security and entering the IP address of up to five authorized SNMP managers provides a much higher level of security. When IP address security is enabled, the source address of any SNMP message addressed to any of the card's IP addresses (in either the management or service domain) will be checked against the authorized list and will be dropped if there is no match. **IP Address Security** – Enable/Disable (Default = Disable). ■ Enabling allows DSLAM to accept SNMP messages from SNMP managers whose IP source addresses have been entered in IP Address field. NOTE: If enabled with no IP address specified or with all addresses set to No Access (NA) permission, then there is no SNMP connectivity to the DSL card. ■ Disabling stops this IP address checking and allows the card to respond to a SNMP query from any source. **IP Address** – *nnn.nnn.nnn.nnn* format. Enter up to five IP source addresses of NMS managers. **Access** – ReadOnly(ro)/ReadWrite(rw)/NoAccess(na). Permission to be granted to each NMS manager. The following applies to additional SNMP security measures for a 5446 RTU: **Endpoint Cookie** – Security string for endpoint. Enter up to eight alphanumeric characters (Default = nosets). Once endpoint security is enabled, none of the SNMP managers can do SNMP sets on the RTUs. SNMP gets, however, can be done. **SNMP Sets at RTU on Port (port 1-4)** – Four SNMP security features to enable or disable SNMP sets for a specific endpoint.
Logical Entities (SNMP Logical Entities) **A-F-B**
This screen displays information contained in the logical table of the Entity MIB. Only the Community Name field can be edited; others are read only. ■ **I** (Index) column shows the index number of DSL ports two to five. ■ **T** (Type) column shows "Remote." ■ **Read Write Comm** shows the community strings of the RTU attached to this port. It is used when the DSLAM downloads configuration data to the RTU in a future release.

Table 6-6. SNMP Options (2 of 2)

Communities/Traps (SNMP Communities/Traps)	**A-F-C**
Gives the user the ability to enable the Authentication Failure Trap Mechanism, stores SNMP Community string names for the DSL card, and stores NMS host IP addresses to which the DSLAM sends trap messages. NOTE: All traps from the DSL card go to the MCC before being forwarded to NMS. It also lets the user configure four communities with three trap destinations each. This can be for a total of up to 12 destinations. **Authentication Failure Trap** – Enable to send a trap when a SNMP request community string does not match or when the password for a Telnet session is incorrect. **Community Name** – 32 characters, up to four unique entries per screen. Default names are public (ro), mcc (rw), nms (rw), nms-2 (ro). **Access** – ReadOnly(ro)/ReadWrite(rw)/NoAccess(na), up to four entries per screen. **IP Address** – *nnn.nnn.nnn.nnn* format. Enter NMS system host address. **Input Number (port)** – *nnn* format. Enter NMS system port number. **Send Traps** – Set to E to enable. Set to D to disable.	

DSL Configuration DHCP Relay Screens

Use the system information sub-menu of the DHCP screens to configure ISP names and DHCP Authentication servers.

▶ Procedure

1. Follow this menu sequence:

   Configuration → *DHCP Relay* (**A-G**)

2. The DHCP Relay menu appears. Enter the desired value on the selected screen and field as shown in Table 6-7 and press Return.

Table 6-7. DHCP Relay Options

Domain Names	**A-G-A**
This screen is used for creating the DHCP Relay agent. The gateway address is used in relaying DHCP requests is configured as an e1a address on the IP Network screen (**A-C-B**). The interface IP address will be inserted into the Gateway Address field of all DHCP requests before relaying to the associated DHCP server. The first column, Interface IP Address, is read only. The second column, ISP Domain Names, is where you enter the corresponding domain name.	
Servers 1–8 and Servers 9–16	**A-G-B or C**
Select: **Servers 1–8 (B)** Gives the user the ability to configure the DHCP and Authentication Server IP addresses for 16 ISP domain names. On these screens, the first 10 characters of the previously configured domain name are displayed in the first column. Based on the domain name, you can configure the DHCP server or the corresponding authentication server. **Authentication wait time** – Default = 3 second(s). Length of time the system waits for a response before timing out. **Number of Authentication attempts** – Default = 2. Number of attempts to the authentication server. **Dynamic access control security** – Default = enable. **Port 1 Default DHCP Domain index (0–16, 0 for none)** – Default = 0 **Port 2 Default DHCP Domain index (0–16, 0 for none)** – Default = 0 **Port 3 Default DHCP Domain index (0–16, 0 for none)** – Default = 0 **Port 4 Default DHCP Domain index (0–16, 0 for none)** – Default = 0 **Servers 9–16 (C)** **Domain Names –** ISP domain name. **DHCP Server** – IP addresses in *nnn.nnn.nnn.nnn* format. Server that uses DHCP to allocate network addresses and delivers configuration parameters to dynamically configured hosts. **Authtn. Server** – IP addresses in *nnn.nnn.nnn.nnn* format. Server that is used to to confirm an end-user system's access location. **RADIUS Secret** – Key used to encrypt the RADIUS message sent to the server. If you have selected RADIUS as your authentication type, this field must be populated. **Authtn. Type** – XTACACS, RADIUS, or None. (Default = none.) Type of authentication server that is being used.	

DSL Configuration RTU Screens

Use the system information sub-menu of the RTU screens to configure RTU information.

▶ Procedure

1. Follow this menu sequence:

   Configuration → *RTU Config.* (**A-H**)

2. The RTU Information menu appears. Enter the desired value on the selected screen and field as shown in Table 6-8 and press Return.

Table 6-8. RTU Information

RTU Information	**A-H-A**
Displays RTU information such as RTU type, system, location, and contact, model number, serial number, version of firmware, and version of hardware.	
Port # – Enter the RTU port number.	
RTU Type – Model number of endpoint. For Model 8540, possible endpoints are 5170/5171/5246/5216. For Model 8546, possible endpoints are 5446r1/5446r2/5546 .	
System Name – Name assigned to the card.	
System Contact – Name or number of the person responsible for the card.	
System Location – Physical location of the system.	
Model Num – Model number of card. (This field only appears on Model 8540 and is read only.)	
Serial Num – Serial number of card. (This field only appears on Model 8540 and is read only.)	
Firmware Rev. – Version of firmware. (This field only appears on Model 8540 and is read only.)	
Hardware Rev. – Version of hardware. (This field only appears on Model 8540 and is read only.)	

Monitoring the HotWire DSLAM

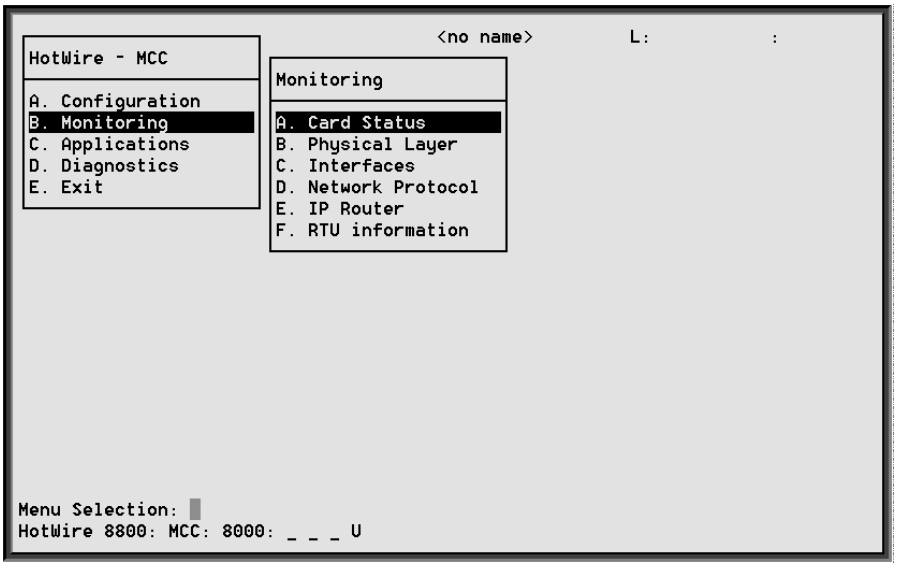
7

Overview

The HotWire DSLAM lets you to monitor the activity of the HotWire MCC and DSL cards. When you select Monitoring from the HotWire MCC or DSL Main Menu, a menu tree of selections on history and error logs, performance statistics, card status, and physical and logical interface status information is presented.

Most of the Monitoring screens are read only; that is, the information displayed is to help you gather pertinent information and isolate potential problem areas. For diagnostic tools and hardware and software troubleshooting techniques, see Chapter 8, *Diagnostics and Troubleshooting*.

MCC Monitoring Menu Tree



MCC Monitoring Card Status Screens

Use the system information submenu of the Card Status screens to display read-only system information.

▶ Procedure

To view general card information, login history, and the syslog:

1. Follow this menu sequence:

   Monitoring → *Card Status* (**B-A**)

2. The Card Status menu appears. Select the submenu option as shown in Table 7-1 and press Return.

Table 7-1. Card Status Options (1 of 2)

Card Info (General Card Information)	**B-A-A**
Displays card information such as system name, location and contact, system up time, available buffers, instruction ram size, buffer ram size, fast data ram size, card type, model and serial number, firmware, and hardware release number.	
System Name – Name assigned to the card.	
System Location – Physical location of the system.	
System Contact – Name or number of the person responsible for the card.	
System Up Time – Length of time the system has been running.	
Available Buffers – Number of buffers not in use.	
Instruction Ram Size – Size of the Instruction Ram.	
Buffer Ram Size – Size of the Buffer Ram.	
Fast Data Ram Size – Total and Available Fast Data Ram.	
Card Type – Type of card (MCC, DSL).	
Model Num – Model number of card.	
Serial Num – Serial number of card.	
Firmware – Version of firmware.	
Hardware Rev – Version of hardware.	
Login History	**B-A-B**
Displays a list of information of the 10 most recent logins.	
Most recent login – Time of the most recent login.	
User – User ID.	
Remote – Local or Remote Connection.	
Least Recent Login – Time of the least recent login.	
Number of unsuccessful Console logins – Number of console logins that were incorrect.	
Number of unsuccessful Telnet logins – Number of Telnet logins that were unsuccessful.	

Table 7-1. Card Status Options (2 of 2)

Syslog	B-A-C
Displays a timestamp sequential list of operational type errors (such as invalid IP addresses) by date and error. There is one logged error per line in a downward scrolling list.	

MCC Monitoring Physical Layer Screens

Use the system information submenu of the Physical Layer screens to display read-only system information about physical ports.

▶ Procedure

To view the active ports list, Ethernet statistics, and HDLC bus statistics:

1. Follow this menu sequence:

   Monitoring → *Physical Layer* (**B-B**)

2. The Physical Layer menu appears. Select the submenu option as shown in Table 7-2 and press Return.

Table 7-2. Physical Layer Options (1 of 2)

Active List (Active Ports List)	B-B-A
Displays a list of the current status of all the active ports (e1a =Ethernet, s1b = backplane) in the card, such as the port number, port name, port type, MAC address, and status of the port (in use or disconnected). **Num** – Number of the port. **Name** – Name of the port. **Description** – Type of port. **MAC Address** – MAC address of the active port. (Internal dummy address is used for non-Ethernet ports.) **Status** – In-use or disconnected.	

Table 7-2. Physical Layer Options (2 of 2)

Ether Statistics (Ethernet Statistics)	**B-B-B**
Displays a list of the Ethernet statistics of the LAN port (e1a) such as port name, LAN address, bytes (running account of how many bytes have been received since last reset), packets (running account of how many packets have been received since last reset) and errors received and transmitted, number of disconnects, number of fast restarts, number of endless and startless packets, and amount of babble. You may enter Ctrl-r at any time to reset counters. **Port** – Name of port (e1a). **Initialized Ethernet Ports** – e1a (there is only one Ethernet port on the card). **LAN Address** – LAN (or MAC) address of the Ethernet port. **Bytes received** – Number of bytes received by the Ethernet port. **Packets received** – Number of packets received by the Ethernet port and what type (multicasts, broadcasts, flooded, filtered, discarded). **Errors** – Number of errors received by the Ethernet port and what type (overruns, bad CRC, framing, jumbo-gram, overflow, buffer). **Bytes transmitted** – Number of bytes transmitted by the Ethernet port. **Packets transmitted** – Number of packets transmitted by the Ethernet port and what type (multicasts, broadcasts, flooded, local origin, queued). **Errors** – Number of errors transmitted by the Ethernet port and what type (collisions, M/L/E, deferrals, carrier loss, underflow, buffer). M = multi collision frames – not counted this release and always set to 0. L= late collisions – collision detected often; at least 64 bytes have been transmitted. E = excessive collisions – port tried to send a packet 15 times without success. **Disconnects** – Number of disconnects on the Ethernet port and what type (disable, MAU drop, Xmit fail). **Fast restarts** – Number of fast restarts and what type (RX off, TX off, Mem err). **Endless Pkt** – Number of endless packets received on the Ethernet port. **Startless Pkt** – Number of startless packets received on the Ethernet port. **Babble** – Number of garbled packets received due to crosstalk.	
HDLC Bus Stats (HDLC Bus Statistics)	**B-B-C**
Displays a list of of the HDLC backplane port statistics for the s1b port (backplane), bytes received and transmitted, packets received and transmitted, and errors received and transmitted. (If a high number of errors have been received, the card may have to be reset.) You may enter Ctrl-r at any time to reset counters. **Port name** – Port name (s1b). **Bytes received** – Number of bytes received on the backplane port. **Bytes transmitted** – Number of bytes transmitted on the backplane port. **Packets received** – Number of packets received on the backplane port. **Packets transmitted** – Number of packets transmitted on the backplane port. **Errors** – Number of other receive errors. **Lost** – Number of packets not transmitted due to internal congestion.	

MCC Monitoring Interfaces Screens

Use the system information submenu of the Interfaces screens to display read-only system information about interfaces.

▶ Procedure

To view the active interfaces list, and interface status list:

1. Follow this menu sequence:

   Monitoring → *Interfaces* (**B-C**)

2. The Interfaces menu appears. Select the submenu option as shown in Table 7-3 and press Return.

Table 7-3. Interfaces Options

Active List (Active Interfaces List)	**B-C-A**
Displays a list of the current status of all of the active interfaces in the card. **If** – Number of the interface. **Name** – Name of the interface. **Type** – Interface type (static). **Link** – Name of the protocol on the interface. **State** – Current state of the interface. **LL-state** – Not applicable. **Port** – Port linked to this interface. The only information that changes on this screen is the state (active or port-wait) column.	
Status (Interface Status)	**B-C-B**
Displays a list of additional information, after a specific interface (port) has been selected, such as interface name, interface protocol, interface port, user name, interface type, number of restarts and link-downs, interface state, and the interface timeout inactivity. **Ifname** – Enter the name of the desired interface (e1a, s1b). **Protocol** – Type of protocol for the entered interface name. **Port** – Port linked to this interface. **Restarts** – Number of times the interface has been restarted. **User** – NA or none. **Type** – Static. **Link-downs** – Number of times the link has gone down. **State** – Active or prtwait (port-wait). **Inactivity T/O** – Number of times the interface has timed out.	

MCC Network Protocol Screens

Use the system submenu information of the Network Protocol screens to display read-only system information.

▶ Procedure

To view socket statistics, UDP statistics, TCP statistics, IP statistics, ICMP statistics, SNMP statistics, and HDLC statistics:

1. Follow this menu sequence:

   Monitoring → *Network Protocol* (**B-D**)

2. The Network Protocol menu appears. Select the submenu option as shown in Table 7-4 and press Return.

Table 7-4. Network Protocol Options (1 of 6)

Socket Statistics	**B-D-A**
Displays information on the active sockets such as socket name, socket family, socket type (stream or datagram), input bytes and output bytes, and PDU and byte drops. Enter the socket name from the active socket list to view information on the application assigned to the specified socket number. **Start Socket** – Enter the socket number to start the active socket list. **Active Socket List** – This is the heading information for the following fields. It lists all the information about the currently selected socket. In addition, the lower right-hand corner of the screen displays a Socket Statistics window with detailed information about the selected destination. **Socket** – Socket number. **Socket name** – Internal name of the socket. **Family** – Family of this socket (DARPA Internet). **Type** – Socket type (stream or datagram). **Local** – Port number on this card. **Remote** – Port number on remote card. **State** – Current state of the socket. **Input Bytes** – Bytes waiting in the socket for the owning application to process (will go to 0 when processed by the application). **Send Bytes** – Bytes waiting to be sent out to the remote machine. **PDU Drops** – Incoming packets dropped (usually due to a lack of space). **Byte Drops** – Outgoing packets dropped (usually due to a lack of space).	

Table 7-4. Network Protocol Options (2 of 6)

UDP Statistics	B-D-B
Displays information on UDP statistics such as input packets, output packets, packets with checksum errors, bad length packets, and other information on all interfaces. The counters increment in real time and you may enter Ctrl-r at any time to reset the counters. **Output Packets** – Number of UDP packets sent out of the card. **Input Packets** – Number of UDP packets coming into the card. **No receive port** – Number of UDP packets coming into the card that had no receive port waiting for this packet. **Unchecksummed** – Number of UDP packets coming into the card that had no checksum. **Header Error** – Number of UDP packets coming into card that had an error with the packet header. **Incorrect Checksum** – Number of UDP packets coming into the card that had a bad checksum. **Bad length** – Number of UDP packets coming into the card that are an illegal length (too short). **Other Error** – Number of UDP packets coming into the card that had an error, but not one of the above.	

Table 7-4. Network Protocol Options (3 of 6)

TCP Data Stats (TCP Statistics)	B-D-C
Displays a summary of the TCP data activity (packets and bytes transmitted and received) on all interfaces on the card. The left column is for received data and the right column is for transmitted data. The counters increment in real time and you may enter Ctrl-r at any time to reset the counters. *Left column:* **Packets Received** – Number of TCP packets received by the card. **Acks** – Number of acknowledgements received for transmitted packets. (Also shows the number of bytes that were acknowledged as received by the remote system.) **Duplicate Acks** – Number of duplicate acks received. **Acks For Unsent Data** – Number of acks received for data that has not been sent yet. **Pkts/Bytes Received in Sequence** – Number of packets/bytes correctly received in sequence for data that had to be split in multiple TCP packets. **Dupl Pkts/Bytes** – Number of duplicate packets/bytes received. **Pkts/Bytes W. Some Dup. Data** – Number of packets/bytes with some duplicated data. (Duplicated data is discarded by TCP.) **Pkts Rcvd out-of-order** – Packets received out of order. **Pkts of data after window** – Packets of data received after our receive window is full. **Window Probes** – Packets received looking for space in our receive window. **Window Update Pkts** – Packets received from the remote system advertising a new window size. **Pkts Rcv After Close** – Packets received after the TCP connection is shut down. **Discarded for Bad Checksum** – Packets that were discarded because the checksum failed. **Discarded for Bad Header Offset Fields** – Packets discarded because the TCP header was corrupted. **Discarded because Packet Too Short** – Packets discarded because the packet was too short (not a complete TCP header). *Right column:* **Packets Sent** – Number of TCP packets sent by the card. **Data Pkts/Bytes** – Number of the sent packets that were data packets instead of TCP control packets. **Retransmit Pkts/Bytes** – Number of packets/bytes that had to be transmitted. **Ack Only Packets** – Number of sent packets that contained only an ack of a received packet and no additional data. **URG only** – Number of packets that contained only an Urgent flag and no data. **Window Probe Pkts** – Number of packets that were window probes. **Window Update** – Number of packets that were advertising our new window size. **Control Pkts** – Number of control packets sent (SYN, FIN, or RST flag).	

Table 7-4. Network Protocol Options (4 of 6)

TCP Connection Statistics	**B-D-C**
Displays a summary of the TCP connection activity on all interfaces on the card. **Connection Requests** – Number of TCP connections initiated by a process on this card. **Connection Accepts** – Number of TCP connections accepted by this card. **Connections Established** – Number of connections established. **Connections closed/dropped** – Number of connections closed (normally) including those dropped. **Embryonic Connections Closed** – Number of connections dropped before data transfer. **Segments Updated RTT** – Number of packets that updated the Round Trip Time and the total number of times TCP attempted to update the RTT. **Retransmit Timeouts** – Number of times a packet had to be transmitted because it was not ack-ed and the number of times a connection was dropped because a packet could not be transmitted. **Persist Timeout** – Number of times the TCP persistence timer went off and sent a probe to the remote system. **Keepalive Timeouts** – Number of times a TCP keepalive request timed out. **Keepalive probes sent** – Number of TCP keepalive probes sent. **Conn Dropped by Keepalive** – Number of connections dropped because the keepalive timer failed to get any responses.	
IP Statistics	**B-D-D**
Displays a summary of the IP activity on all interfaces on the card. **Total Pkts Rev** – Total number of IP packets received by this card, with errors broken down on the right of the screen. **Fragments Rev** – Number of packet fragments received, with dropped fragments on the right of the screen. **Frag on Transmit** – Number of packets that were fragmented on transmit and the number of fragments that were created by those packets. **Packets Forwarded** – Number of packets that were forwarded to another system. **Packets Not Forwardable** – Number of packets that could not be forwarded. (Usually due to packet errors or routing problems.) **Packet Redirects sent** – Number of redirect messages sent to other systems because they sent a packet that should not be sent to this card. **Network Broadcasts Received** – Number of network broadcasts received for local networks. **Network Broadcasts Forwarded** – Number of network broadcasts for local networks sent. **Network Broadcasts partially processed** – Number of network broadcasts dropped due to an error.	

Table 7-4. Network Protocol Options (5 of 6)

ICMP Statistics (ICMP Packet Statistics)	**B-D-E**
Displays a summary of the ICMP activity on all interfaces of the card such as echo replies, source quench messages, and information requests with their output, input, and status. The columns show input and output packet counts. Note that the Status column is only applicable for “routing redirect.” The counters increment in real time and you may enter Ctrl-r at any time to reset the counters.	
SNMP Statistics	**B-D-F**
Displays information on SNMP statistics such as number of set packets, number of get requests, and parsing errors. When you press Return, the SNMP Authentication Statistics screen is displayed, giving you additional Community Administration information. The counters increment in real time and you may enter Ctrl-r at any time to reset the counters. **In Packets** – Total number of SNMP Protocol Data Units (PDUs) received by the agent. **Get Requests** – Total number of SNMP Get Request PDUs accepted and processed by the SNMP agent. **Get Next Requests** – Total number of SNMP Get Next PDUs accepted and processed by the SNMP agent. **Total Requested Variables** – Total number of Management Information Base (MIB) retrieved successfully by the SNMP agent as a result of receiving valid SNMP Get Request and Get Next PDUs. **Set Requests** – Total number of SNMP Set Requests PDUs accepted and processed by the SNMP agent. **Total Set Variables** – Total number of MIB objects modified successfully by the SNMP agent as a result of receiving valid SNMP Set Requests PDUs. **ASN.1** – Total number of ASN.1 or BER errors encountered when decoding received SNMP messages. **Out Packets** – Total number of SNMP PDU responses sent by the agent. **Out Too Big Errors** – Total Number of SNMP PDUs generated by the SNMP agent for which the value of error status field is too big. **Out No Such Names** – Total number of SNMP PDUs generated by the SNMP agent for which the value of error status field is “no such name.” **Out Bad Values** – Total number of SNMP PDUs generated by the SNMP agent for which the value of the error status field is bad value. **Out General Errors** – Total number of SNMP PDUs generated by the SNMP agent for which the value of error status is Gen Err. **Read-only Errors** – Total number of SNMP PDUs delivered by the SNMP agent for which the value of the error status field is read-only. **Out Get Response** – Total number of Get-Response PDUs sent out by the SNMP agent. **Out Traps** – Total number of SNMP Traps PDUs generated by the SNMP agent. **SNMP Status** – Indicates the state of the SNMP Agent. The first byte = error code, the second byte = sub-routine code.	

Table 7-4. Network Protocol Options (6 of 6)

SNMP Authentication Statistics	**B-D-F**
The SNMP Authentication Statistics screen displays the following information: **Community Administration** – Number of SNMP PDUs with community based authentication. **Bad Versions** – Total number of SNMP messages delivered to the SNMP agent for an unsupported SNMP version. **Bad Community Name** – Total number of SNMP messages delivered to the SNMP agent that used an SNMP community name not known to the entity. **Bad Community Use** – Total number of SNMP messages delivered to the SNMP agent that represent an SNMP operation not allowed by the SNMP community named in the message.	
HDLC Stats (HDLC Statistics)	**B-D-G**
Displays information on High-Level Data Link Control statistics for the backplane bus such as number of octets and frames transmitted, packet receive errors, and framing errors. The counters increment in real time and you may enter Ctrl-r at any time to reset the counters. **Interface Name** – Interface Name (s1b). **Totals Summary** – This is the heading information for the following fields. There will not be entries in this field. **Octets Transmitted and Received** – Number of octets (8 bit bytes) transmitted and received. **Frames Transmitted and Received** – Number of frames (groups of data bits) transmitted and received. **Alloc Failures on Send** – Number of packets not transmitted because there was no memory available to build the packet. **Output Errors** – Number of other transmit errors (i.e., bad HDLC address).	

MCC IP Router Screens

Use the system information submenu of the IP Router screens to display read-only system information.

▶ Procedure

To view routing and ARP tables:

1. Follow this menu sequence:

   Monitoring → *IP Router* (**B-E**)

2. The IP Router menu appears. Select the submenu option as shown in Table 7-5 and press Return.

Table 7-5. IP Router Menu Options (1 of 3)

Routing Table	**B-E-A**
Displays information and statistics stored in the routing table. Note that routes will appear only for interfaces that are up. The information and statistics are listed by route and destination number. To display information for a specific destination, enter the destination IP address at the `[Destination # or <RET>]:` prompt.	
The Routing Table displays the following columns of information: **Routing Table Screen** # – Displays the entry number in the routing table. Use this number to specify which entry you want to display more information. **Destination** – Specifies the destination (or source) IP address of the packet. **Subnet Mask** – Indicates the associated subnet mask for the specified destination IP address. **Routes** – Number of routes for Destination. **Flags** – Identifies the type of route: host, sub (subnetwork), or net (network).	

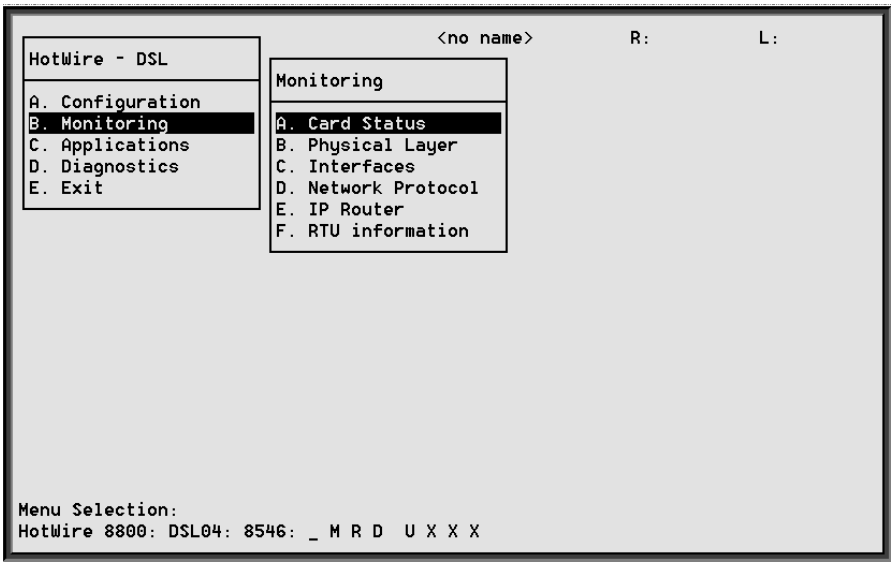
Table 7-5. IP Router Menu Options (2 of 3)

Routing Information Window In addition, the lower right-hand corner of the screen displays a Route Information window with detailed information about the selected destination. **Route #** – Displays the number of the route for the given destination. If more than one route exists for the given destination, you may view subsequent routes by entering the routing entry number at the `[Route # or <RET>]:` prompt. **Next Hop** – Indicates the IP address of the next hop device for the specified destination. Protocol – Displays the type of routing protocol by which the route was learned (i.e., static or direct). **Preference** – Specifies the assigned preference number to this route. If more than one route exists for the given destination, this number is compared to the preference number of the other routes. The route with the lowest preference number is the preferred route. The value of 0 indicates the highest preference. The greater the number, the lower the preference. **Flags** – Indicates if a route is a Host and if the next hop is valid. **Interface** – Displays the name of the interface associated with the destination address. **State** – Indicates the various state information about the route including Permanent, Deleted, SRC, Host, Net, Subn. **Metric** – Not applicable. **Age** – Displays the length of time in seconds that a non-permanent route has been active. **Revision #** – Not applicable. **Max Age** – Displays the maximum length of time in seconds before a non-permanent route has been active. **Ref Count –** Number of internal references for this route. Displays the working routing table. Routes will appear only for interfaces that are up. Details for the selected destinations are shown in the lower right corner. You may select a different destination by entering a number at the “Destination #” prompt. If more than one route exists for the given destination, you may view subsequent routes by entering the number at the “Route #” prompt.
ARP Table **B-E-B**
Displays the current Address Resolution Protocol (ARP) cache. Permanent entries show an age of 0. **Line** – Sequential number of line. **IP Address** – Internet Protocol Address. **Ethernet Address** – Ethernet address associated with the IP address. (An incomplete can be shown in this column for some internal entries such as the backplane.) **Min** – Number of minutes since this entry was last used. **Interface** – The interface on which this ARP request was answered. **Flags** – Various flags associated with this entry. PERM = permanent, PUB = publish this entry (respond for other hosts), PROX = proxy ARP (card will proxy ARP for this IP address).

Table 7-5. IP Router Menu Options (3 of 3)

Filter Table	B-E-C
Displays the various filters that have been configured.	
The FIlter Table screen displays the following information:	
Line – Sequential number of line.	
Filter Name – Name of the IP filter.	
# of Static Rules – Number of static routes in filter.	
# of Dynamic Rules – Number of dynamic routes in filters.	
Reference Count – Number of active interfaces using the filter.	
Default Action – Default action for the filter.	

DSL Monitoring Menu Tree



DSL Monitoring Card Status Screens

Use the system information submenu of the Card Status screens to display read-only system information.

▶ Procedure

To view general card information, login history, and the syslog:

1. Follow this menu sequence:

   Monitoring → *Card Status* (**B-A**)

2. The Card Status menu appears. Select the submenu option as shown in Table 7-6 and press Return.

Table 7-6. Card Status Options

Card Info (General Card Information)	**B-A-A**
Displays card information such as system name, location and contact, system up time, available buffers, instruction ram size, buffer ram size, fast data ram size, card type, model and serial number, and firmware, CAP, and hardware release number. **System Name** – Name assigned to the card. **System Location** – Physical location of the system. **System Contact** – Name or number of the person responsible for the card. **System Up Time** – Length of time the system has been running. **Available Buffers** – Number of Buffers not in use. **Instruction Ram Size** – Size of the Instruction Ram. **Buffer Ram Size** – Size of the Buffer Ram. **Fast Data Ram Size** – Total and Available Fast Data Ram. **Card Type** – Type of Card (MCC, DSL). **Model Num** – Model number of card. **Serial Num** – Serial number of card. **Firmware** – Version of firmware. **CAP Firmware** – Firmware for DSL chipset. **Hardware Rev** – Version of hardware.	
Login History	**B-A-B**
Displays a list of information of the 10 most recent logins. **Most recent login** – Time of the most recent login. **User** – User ID. **Local/Remote** – Local or Remote Connection. **Least Recent Login** – Time of the least recent login. **Number of unsuccessful Console logins** – Number of console logins that were incorrect in the last 10 attempts**.** **Number of unsuccessful Telnet logins** – Number of Telnet logins that were incorrect in the last 10 attempts.	
Syslog	**B-A-C**
Displays a timestamp sequential list of operational type errors (such as invalid IP addresses) by date and error. There is one logged error per line in a downward scrolling list. There is a 17 error entry maximum.	

DSL Monitoring Physical Layer Screens

Use the system information submenu of the Physical Layer screens to display read-only system information about physical ports.

▶ Procedure

To view the active ports list, Ethernet statistics, and HDLC bus statistics:

1. Follow this menu sequence:

   Monitoring → *Physical Layer* (**B-B**)

2. The Physical Layer menu appears. Select the submenu option as shown in Table 7-7 and press Return.

Table 7-7. Physical Layer Options (1 of 5)

Active List (Active Ports List)	**B-B-A**
Displays a list of the current status of all the active ports (e1a = Ethernet; s1b = backplane; s1c, s1d, s1e, and s1f = DSL cards) in the card such as the port number, port name, port type, MAC address, and status of the port (in use or disconnected). **Num** – Number of the port. **Name** – Name of the port. **Description** – Type of port. **MAC Address** – MAC address of the active port. (Internal dummy address used for non-Ethernet ports.) **Status** – Active or disconnected.	

Table 7-7. Physical Layer Options (2 of 5)

Ether Statistics (Ethernet Statistics)	B-B-B
Displays a list of the Ethernet statistics of the LAN port (e1a) such as port name, LAN address, bytes (running account of how many bytes have been received since last reset), packets (running account of how many packets have been received since last reset) and errors received and transmitted, number of disconnects, number of fast restarts, number of endless and startless packets, and amount of babble. You may enter Ctrl-r at any time to reset counters. **Port** – Type of port (e1a). **Initialized Ethernet Ports** – e1a (There is only one other net port on the card). **LAN Address** – LAN (or MAC) address of the Ethernet port. **Bytes received** – Number of bytes received by the Ethernet port. **Bytes transmitted** – Number of bytes transmitted by the Ethernet port. **Packets received** – Number of packets transmitted by the Ethernet port and what type (multicasts, broadcasts, flooded, local origin, queued). – Multicast – Single packets copied to a specific subset of network addresses. – Broadcasts – Messages sent to all network destinations. – Flooded – Information received, then sent out to each of the interfaces. – Filtered – Processes or devices that screen incoming information. – Discarded – Packets discarded. **Errors** – Number of errors transmitted by the Ethernet port and what type (collisions, M/L/E, deferrals, carrier loss, underflow, buffer). M = multi-collision frames – not counted this release and always set to 0. L = late collisions – collision detected often; at least 64 bytes have been transmitted. E = excessive collisions – port tried to send a packet 15 times without success. – Overruns – No buffer space. – Bad CRC – Cyclic Redundancy Check. – Framing – Receiver improperly interprets set of bits within frame. – Jumbo gram – Ethernet packet too long. – Overflow – Part of traffic that is not carried. – Buffer – No buffer space. **Bytes transmitted** – Number of bytes transmitted on the Ethernet port. **Fast restarts** – Number of fast restarts and what type (RX off, TX off, Mem err). **Endless Pkt** – Number of endless packets received on the Ethernet port. **Startless Pkt** – Number of startless packets received on the Ethernet port. **Babble** – Number of garbled packets received due to crosstalk.	

Table 7-7. Physical Layer Options (3 of 5)

Ether Statistics (Ethernet Statistics) (continued)	**B-B-B**
Packets transmitted – Number of packets transmitted by the Ethernet port and what type (multicasts, broadcasts, flooded, local origin, queued) – Multicast – Single packets copied to a specific subset of network addresses. – Broadcast – Messages sent to all network destinations. – Flooded – Information received, then sent out to each of the interfaces. – Local origin – Locally transmitted packet; e.g. Ping. – Queued – Packets waiting to be processed. **Errors** – Number of errors transmitted by the Ethernet port and what type (collisions, M/L/E, deferrals, carrier loss, underflow, buffer) – M = multi-collision frames – not counted this release and always set to 0. – L = late collisions – collision detected often; at least 64 bytes have been transmitted. – E = excessive collisions – port tried to send a packet 15 times without success. **Disconnects** – Number of disconnects on the Ethernet port and what type (disable, MAU drop, Xmit fail). – Disable – Transmit error, timed out. – MAU drop – Transceivers dropped. – Xmit fail Transmit fail	
HDLC Bus Stats (HDLC Bus Statistics)	**B-B-C**
Displays a list of of the HDLC backplane port statistics for the s1b port (backplane), bytes received and transmitted, packets received and transmitted, and errors received and transmitted. (If a high number of errors have been received, the card may have to be reset.) You may enter Ctrl-r at any time to reset counters. **Port name** – Port name (s1b). **Bytes received** – Number of bytes received on the backplane port. **Bytes transmitted** – Number of bytes transmitted on the backplane port. **Packets received** – Number of packets received on the backplane port. **Packets transmitted** – Number of packets transmitted on the backplane port. **Errors** – Number of other receive errors. **Lost** – Number of packets not transmitted due to internal congestion.	

Table 7-7. Physical Layer Options (4 of 5)

DSL Link Perf (DSL Link Performance Summary)	**B-B-D**
Displays a summary of the link performance for each of the DSL ports. Enter port number one to four to see the fields for current 15-minute period (real time count of events during the past 0 to 15 minutes), previous 15-minute period (data updated every 15 minutes), previous one hour period (data updated every hour), and 24-hour period (data is updated every hour). Error Rate Definition: **Dn Margin** – Measure of the noise margin on the specified port in the downstream direction. **Up Margin** – Measure of the noise margin on the specified port in the upstream direction. **DnErrRate**– This statistic is not available for this release and an NA appears for each time period. **UpErrRate**– Block error rate in upstream direction. Error rate = bad blocks/good blocks and is expressed as A x 10^{-B}. **DnAttEst** – Measure of the downstream transmission loss on the DSL line. **UpAttEst** – Measure of the upstream transmission loss on the DSL line.	
DSL Perf Stats (DSL Performance Stats)	**B-B-E**
Displays the link performance for each of the DSL ports. Tells you the number of times the link has been down and the elapsed time the link has been up. Enter port number one to four to see the fields for current 15-minute period (real time count of events during the past 0 to 15 minutes), previous 15-minute period (data updated every 15 minutes), previous one hour period (data updated every hour), and 24-hour period (data updated every hour). **15min Valid** – Number of 15 minutes intervals in which downstream performance data, which is measured by the 5446 RTU, has been received across the DSL link from the RTU. **pkt rcv up** – Number of upstream packets received. **pkt snt up** – Number of upstream packets sent. **pkt rcv dn** – Number of downstream packets received. **pkt snt dn** – Number of downstream packets sent. **pkt lost dn** – Number of downstream packets lost. **Link dn count** – Number of times the DSL link has gone down. **elp lnk up** – Count in seconds of the elapsed time the link has been up. **elp time** – Count in seconds of the elapsed time since the DSL card was last reset. **Pct link up** – Percentage of time the link has been up in the past 24 hours. **k octs sent dn** – How many thousands of octets have been sent to the RTU. **k octs rcv dn** – How many thousands of octets have been received by the RTU. **k octs sent up** – How many thousands of octets have been sent upstream from the RTU. **k octs rcv up** – How many thousands of octets have been received upstream from the RTU.	

Table 7-7. Physical Layer Options (5 of 5)

DSL Error Stats	**B-B-F**
Displays the error performance (margin) rates for each of the DSL ports after selecting a specific DSL port number. Margin is a measure of performance. Enter port number one to four to see the fields for current 15-minute period (real time count of events during the past 0 to 15 minutes), previous 15-minute period (data updated every 15 minutes), previous one hour period (data updated every hour), and 24-hour period (data bucket updated every hour). A margin of 0 db equals an expected bit error rate of 10^{-7}. (The higher the margins, the fewer the errors.) You may enter Ctrl-r at any time to reset counters. Error Rate Definition: **dn margin** – Measure of the noise margin on the specified port in the downstream direction. **up margin** – Measure of the noise margin on the specified port in the upstream direction. **dn err rate** – This statistic is not available for this release and an NA appears for each time period. **up err rate** – Block error rate in upstream direction. Error rate = bad blocks/good blocks and is expressed as A x 10^{-B}. **dn err secs** (**dn err mins for Model 8540**) – Count of the number of down error seconds with at least one block error. **up err secs** – (**up err mins for Model 8540**) – Count of the number of up error seconds with at least one block error. **dn svr err sec** – This statistic is not available for this release and an NA appears for each time period. **up svr err sec** – Count of the number of seconds with at least 800 block errors.	
DSL Xmit Status (DSL Transmit Stats)	**B-B-G**
Displays the transmit and receive statistics for each of the DSL ports after selecting a specific DSL port number. Enter port number one to four to see the fields for current 15-minute period (real time count of events during the past 0 to 15 minutes), previous 15-minute period (data updated every 15 minutes), previous one hour period (data updated every hour), and 24-hour period (data updated every hour). You may enter Ctrl-r at any time to reset counters. **dn xmit pwr** – Measure of the power level of the downstream signal sent to the RTU (in db). **up xmit pwr** – Measure of the power level of the upstream signal sent to the RTU (in db). **dn rx gain** – Measure of how much amplification was applied to the signal received at the RTU. **up rx gain** – Measure of how much amplification was applied to the signal received at the DSLAM port. **dn att est** – Measure of the downstream transmission loss on the DSL line. **up att est** – Measure of the upstream transmission loss on the DSL line.	

DSL Monitoring Interfaces Screens

Use the system submenu information of the Interfaces screens to display read-only system information about interfaces.

▶ Procedure

To view the active interfaces list, and interface status list:

1. Follow this menu sequence:

   Monitoring → *Interfaces* (**B-C**)

2. The Interfaces menu appears. Select the submenu option as shown in Table 7-8 and press Return.

Table 7-8. Interfaces Options

Active List (Active Interfaces List)	**B-C-A**
Displays a list of the current status of all of the active interfaces in the card. **If** – Number of the interface. **Name** – Name of the interface. **Type** – Interface type (static). **Link** – Name of the protocol on the interface. **State** – Current state of the interface. **ll-state** – Not applicable. **Port** – Port linked to this interface. The only information that changes on this screen is the state (active or port-wait) column.	
Status (Interface Status)	**B-C-B**
Displays a list of additional information, after a specific interface (port) has been selected, such as interface name, interface protocol, interface port, user name, interface type, number of restarts and link-downs, interface state, and the interface timeout inactivity. **Ifname** – Enter the name of the desired interface (s1a, e1b). **Protocol** – Type of protocol for the entered interface name. **Port** – Port linked to this interface. **Restarts** – Number of times interface has been restarted. **User** – NA or none. **Type** – Static. **Link-downs** – Number of times the link has gone down. **State** – Active or prtwait. **Inactivity T/O** – Number of times the interface has timed out.	

DSL Network Protocol Screens

Use the system submenu information of the Network Protocol screens to display read-only system information.

▶ Procedure

To view socket statistics, UDCP statistics, TCP data and connection statistics, IP statistics, ICMP statistics, SNMP statistics, and HDLC statistics:

1. Follow this menu sequence:

   Monitoring → *Network Protocol* (**B-D**)

2. The Network Protocol menu appears. Select the submenu option as shown in Table 7-9 and press Return.

Table 7-9. Network Protocol Options (1 of 7)

Socket Statistics	**B-D-A**
Displays information on the active sockets such as socket name, socket family, socket type (stream or datagram), input bytes and output bytes, and PDU and byte drops. Enter the socket name from the active socket list to view information on the application assigned to the specified socket number.	
Start Socket – Enter the socket number to start the active socket list.	
Active Socket List – This is the heading information for the following fields. It lists all the information about the currently selected socket.	
In addition, the lower right-hand corner of the screen displays a Socket Statistics window with detailed information about the selected destination. The Socket Statistics window displays the following information:	
Socket – Socket number.	
Socket name – Internal name of the socket.	
Family – Family of this socket (DARPA Internet).	
Type – Socket type (stream or datagram).	
Local – Port number on this card.	
Remote – Port number on remote card.	
State – Current state of the socket.	
Input Bytes – Bytes waiting in the socket for the owning application to process (will go to 0 when processed by the application).	
Send Bytes – Bytes waiting to be sent out to the remote machine.	
PDU Drops – Incoming packets dropped (usually due to a lack of space).	
Byte Drops – Outgoing packets dropped (usually due to a lack of space).	

Table 7-9. Network Protocol Options (2 of 7)

UDP Statistics	B-D-B
Displays information on UDP statistics such as input packets, output packets, packets with checksum errors, bad length packets, and other information on all interfaces. The counters increment in real time and you may enter Ctrl-r at any time to reset the counters. **Output Packets** – Number of UDP packets sent out of the card. **Input Packets** – Number of UDP packets coming into the card. **No receive port** – Number of UDP packets coming into the card that had no receive port waiting for this packet. **Unchecksummed** – Number of UDP packets coming into the card that had no checksum. **Header Error** – Number of UDP packets coming into card that had an error with the packet header. **Incorrect Checksum** – Number of UDP packets coming into the card that had a bad checksum. **Bad length** – Number of UDP packets coming into the card that are an illegal length (too short). **Other Error** – Number of UDP packets coming into the card that had an error, but not one of the above.	

Table 7-9. Network Protocol Options (3 of 7)

TCP Data Stats (TCP Data Statistics)	B-D-C

Displays a summary of the TCP data activity (packets and bytes transmitted and received) on all interfaces on the card. The left column is for received data and the right column is for transmitted data.

The counters increment in real time and you may enter Ctrl-r at any time to reset the counters.

Left column:

Packets Received – Number of TCP packets received by the card.

Acks – Number of acknowledgements received for transmitted packets. (Also shows the number of bytes that were acknowledged as received by the remote system.)

Duplicate Acks – Number of duplicate acks received.

Acks For Unsent Data – Number of acks received for data that has not been sent yet.

Pkts/Bytes Received in Sequence – Number of packets/bytes correctly received in sequence for data that had to be split in multiple TCP packets.

Dupl Pkts/Bytes – Number of duplicate packets/bytes received.

Pkts/Bytes W. Some Dup. Data – Number of packets/bytes with some duplicated data. (Duplicated data is discarded by TCP.)

Pkts rcvd out-of-order – Packets received out of order.

Pkts of data after window – Packets of data received after our receive window is full.

Window Probes – Packets received looking for space in our receive window.

Window Update Pkts – Packets received from the remote system advertising a new window size.

Pkts Rcv After Close – Packets received after the (our) TCP connection is shut down.

Discarded for Bad Checksum – Packets that were discarded because the checksum failed.

Discarded for Bad Header Offset Fields – Packets discarded because the TCP header was corrupted.

Discarded because Packet Too Short – Packets discarded because the packet was too short (not a complete TCP header).

Right column:

Packets sent – Number of TCP packets sent by the card.

Data Pkts Retransmit – Number of the sent packets that were data packets instead of TCP control packets.

Retransmit Pkts/Bytes – Number of packets/bytes that had to be transmitted.

Ack Only Packets – Number of sent packets that contained only an ack of a received packet and no additional data.

URG only – Number of packets that contained only an Urgent flag and no data.

Window Probe Pkts – Number of packets that were window probes.

Window Update – Number of packets that were advertising our new window size.

Control Pkts – Number of control packets sent (SYN, FIN, or RST flag).

Table 7-9. Network Protocol Options (4 of 7)

TCP Connection Statistics	**B-D-C**
Displays a summary of the TCP connection activity on all interfaces on the card. **Connection Requests** – Number of TCP connections initiated by a process on this card. **Connection Accepts** – Number of TCP connections accepted by this card. **Connections Established** – Number of connections established. **Connections closed/dropped** – Number of connections closed (normally) including those dropped. **Embryonic Connections Closed** – Number of connections dropped before data transfer. **Segments Updated RTT** – Number of packets that updated the Round Trip Time and the total number of times TCP attempted to update the RTT. **Retransmit Timeouts** – Number of times a packet had to be transmitted because it was not ack-ed and the number of times a connection was dropped because a packet could not be transmitted. **Persist Timeout** – Number of times the TCP persistence timer went off and sent a probe to the remote system. **Keepalive Timeouts** – Number of times a TCP keepalive request timed out. **Keepalive probes sent** – Number of TCP keepalive probes sent. **Conn Dropped by Keepalive** – Number of connections dropped because the keepalive timer failed to get any responses.	
IP Statistics	**B-D-D**
Displays a summary of the IP activity on all interfaces on the card. **Total Pkts Rev** – Total number of IP packets received by this card, with errors broken down on the right of the screen. **Fragments Rev** – Number of packet fragments received, with dropped fragments on the right of the screen. **Frag on Transmit** – Number of packets that were fragmented on transmit and the number of fragments that were created by those packets. **Packets Forwarded** – Number of packets that were forwarded to another system. **Packets Not Forwardable** – Number of packets that could not be forwarded. (Usually due to packet errors or routing problems.) **Packet Redirects sent** – Number of redirect messages sent to other systems because they sent a packet that should not be sent to this card. **Network Broadcasts Received** – Number of network broadcasts received for local networks. **Network Broadcasts Forwarded** – Number of network broadcasts for local networks sent. **Network Broadcasts partially processed** – Number of network broadcasts dropped due to an error.	

Table 7-9. Network Protocol Options (5 of 7)

ICMP Statistics (ICMP Packet Statistics)	**B-D-E**
Displays a summary of the ICMP activity on all interfaces of the card such as echo replies, source quench messages, and information requests with their output, input, and status. The columns show input and output packet counts. Note that the Status column is only applicable for “routing redirect.” The counters increment in real time and you may enter Ctrl-r at any time to reset the counters.	
SNMP Statistics	**B-D-F**
Displays information on SNMP statistics such as number of set packets, number of get requests, and parsing errors. When you press Return, the SNMP Authentication Statistics screen is displayed, giving you additional Community Administration information. The counters increment in real time and you may enter Ctrl-r at any time to reset the counters. **In Packets** – Total number of SNMP Protocol Data Units (PDUs) received by the agent. **Get Requests** – Total number of SNMP Get Request PDUs accepted and processed by the SNMP agent. **Get Next Requests** – Total number of SNMP Get Next PDUs accepted and processed by the SNMP agent. **Total Requested Variables** – Total number of Management Information Base (MIB) retrieved successfully by the SNMP agent as a result of receiving valid SNMP Get Request and Get Next PDUs. **Set Requests** – Total number of SNMP Set Requests PDUs accepted and processed by the SNMP agent. **Total Set Variables** – Total number of MIB objects modified successfully by the SNMP agent as a result of receiving valid SNMP Set Requests PDUs. **ASN.1** – Total number of ASN.1 or BER errors encountered when decoding received SNMP messages. **Out Packets** – Total number of SNMP PDU responses sent by the agent. **Out Too Big Errors** – Total Number of SNMP PDUs generated by the SNMP agent for which the value of error status field is too big. **Out No Such Names** – Total number of SNMP PDUs generated by the SNMP agent for which the value of error status field is “no such name.” **Out Bad Values** – Total number of SNMP PDUs generated by the SNMP agent for which the value of the error status field is bad value. **Out General Errors** – Total number of SNMP PDUs generated by the SNMP agent for which the value of error status is Gen Err. **Read-only Errors** – Total number of SNMP PDUs delivered by the SNMP agent for which the value of the error status field is read-only. **Out Get Response** – Total number of Get-Response PDUs sent out by the SNMP agent. **Out Traps** – Total number of SNMP Traps PDUs generated by the SNMP agent. **SNMP Status** – Indicates the state of the SNMP Agent. The first byte = error code, the second byte = sub-routine code.	

Table 7-9. Network Protocol Options (6 of 7)

SNMP Authentication Statistics (continuation of previous screen)	**B-D-F**
The SNMP Authentication Statistics screen displays the following information: **Community Administration** – Number of SNMP PDUs with community based authentication. **Bad Versions** – Total number of SNMP messages delivered to the SNMP agent for an unsupported SNMP version. **Bad Community Name** – Total number of SNMP messages delivered to the SNMP agent that used an SNMP community name not known to the entity. **Bad Community Use** – Total number of SNMP messages delivered to the SNMP agent that represent an SNMP operation not allowed by the SNMP community named in the message.	
HDLC Statistics (HDLC Statistics)	**B-D-G**
Displays information on High-Level Data Link Control statistics for the backplane bus such as number of octets and frames transmitted, packet receive errors, and framing errors. The counters increment in real time and you may enter Ctrl-r at any time to reset the counters. **Interface Name** – Interface Name (s1b). **Totals Summary** – This is the heading information for the following fields. There will not be entries in this field. **Octets Transmitted and Received** – Number of octets (8 bit bytes) transmitted and received. **Frames Transmitted and Received** – Number of frames (groups of data bits) transmitted and received. **Alloc Failures on Send** – Number of packets not transmitted because there was no memory available to build the packet. **Output Errors** – Number of other transmit errors (i.e., bad HDLC address). This field does not appear on Model 8540.	

Table 7-9. Network Protocol Options (7 of 7)

PPP Stats (General)	**B-D-H (A)**
Displays a summary of the PPP activity on a selected interface on the card. **Interface Name** – Enter the name of the desired DSLinterface (s1c, s1d, s1e, s1f). **Link Phase** – Current phase/state of this link (Init, Link Control). **Octets Transmitted** – Number of octets (8 bit bytes) transmitted. **Frames Transmitted** – Number of frames (groups of data bits) transmitted. **Octets Received** – Number of octets received. **Frames received** – Number of frames received. **Alloc failures on send** – Number of packets not transmitted because there was no memory available to build the packet. **Unknown Pkts Received** – Packet with unknown received. **Bad Checksum Packets Received** – Packet with a bad checksum received. **Frame Errors Received** – Packet received with bad framing. **Other Pkt Errors Received**– Packet received with an error not listed above. **Alloc failures Received** – Card was unable to allocate enough memory to receive the packet.	
LCP Stats (PPP)	**B-D-H (B)**
Displays a summary of the Link Control Protocol (LCP) activity on a selected interface on the card. The screen is divided into two parts – the left side is for the local end of the link; the right half is for the remote end of the link. **Interface name** – Enter the name of the desired interface (s1c, s1d, s1e, s1f). **Link Phase** – Current phase/state of this link (Init, Link Control, Opened). **Async Bit Map** – Coding used to embed PPP control characters in the data section of the packet. **Authentication** – Authentication type required for the connect to be accepted (usually none). **Magic number** – Unique number associated with this end of the link, used to ensure the link is not a loopback.	
IPCP General Stats (PPP)	**B-D-H (C)**
Displays a summary of the IP Control Protocol (IPCP) activity on a selected interface on the card. The screen is divided into two parts – the left side is for the local end of the link; the right half is for the remote end of the link. **Interface name** – Enter the name of the desired interface (s1c, s1d, s1e, s1f). **Link Phase** – Current phase/state of this link (Init, Link Control, Opened). **LCP Configuration** – Configuration of the link control protocol. **State** – State of the IP link (Initial, Opened, Closed). **IP Address** – IP address assigned to this end of the link.	

DSL IP Router Screens

Use the system submenu information of the IP Router screens to display read-only system information.

▶ Procedure

To view routing and ARP tables:

1. Follow this menu sequence:

   Monitoring → *IP Router* (**B-E**)

2. The IP Router menu appears. Select the submenu option as shown in Table 7-10 and press Return.

Table 7-10. IP Router Options (1 of 3)

Routing Table	**B-E-A**
Displays information and statistics stored in the IP routing table. Note that routes will appear only for interfaces that are up. The information and statistics are listed by route and destination number. To display information for a specific destination, enter the destination IP address at the `[Destination # or <RET>]:` prompt.	
Routing Table Screen The Routing Table displays the following columns of information: # – Displays the entry number in the routing table. Use this number to specify which entry you want to display more information. **Destination** – Specifies the destination (or source) IP address of the packet. **Subnet Mask** – Indicates the associated subnet mask for the specified destination IP address. **Routes** – Number of routes for Destination. **Flags** – Identifies the type of route: host, sub (subnetwork), or net (network).	

Table 7-10. IP Router Options (2 of 3)

Routing Table (continued)	**B-E-A**
Routing Information Window In addition, the lower right-hand corner of the screen displays a Route Information window with detailed information about the selected destination. The Route Information window displays the following information: **Route #** – Displays the number of the route for the given destination. If more than one route exists for the given destination, you may view subsequent routes by entering the routing entry number at the `[Route # or <RET>]:` prompt. **Next Hop** – Indicates the IP address of the next hop device for the specified destination. **Protocol** – Displays the type of routing protocol by which the route was learned (i.e., static or direct). **Preference** – Specifies how the routes are sorted. The lower the number, the higher the priority. However, if a static route is created with a preference of 0, the route will be given a preference of 50. **Flags** – Indicates if a route is a Host and if the next hop is valid. **Interface** – Displays the name of the interface associated with the destination address. **State** – Indicates the various state information about the route including Permanent, Deleted, SRC, Host, Net, Subn. **Metric** – Not applicable. **Age** – Displays the length of time in seconds that a non-permanent route has been active. **Revision #** – Number of changes to the routing table prior to the creation of this route, with the change that includes this route also added in. For example, if the revision number is 89, then this route was created with the 89th change to the routing table. **Max Age** – Displays the maximum length of time in seconds before a non-permanent route has been active. **Ref Count** – Number of times this route has been used to route a packet since the last reboot.	
ARP Table	**B-E-B**
Displays the current Address Resolution Protocol (ARP) cache. Permanent entries show PERM PUB PROX. (See **Flags**.) **Line** – Sequential number of line. **IP Address** – Internet Protocol Address. **Ethernet Address** – Ethernet address associated with the IP address. (An incomplete can be shown in this column for some internal entries such as the backplane.) **Min** – Number of minutes since this entry was last used. **Interface** – The interface on which this ARP request was answered. **Flags** – Various flags associated with this entry. PERM = permanent, PUB = publish this entry (respond for other hosts), PROX = proxy ARP (card will proxy ARP for this IP address).	

Table 7-10. IP Router Options (3 of 3)

Filter Table	B-E-C
Displays the various filters that have been configured. The Filter Table screen displays the following information: **Line** – Sequential number of line. **Filter Name** – Name of the IP filter. **# of Static Rules** – Number of static routes in filter. **# of Dynamic Rules** – Number of dynamic routes in filters. **Reference Count** – Number of active interfaces using the filter. **Default Action** – Default action for the filter.	

DSL Configuration RTU Screens

Use the system information sub-menu of the RTU screens to display read-only RTU information.

▶ Procedure

1. Follow this menu sequence:

   Monitoring → *RTU Config.* (**B-F**)

2. The RTU Information menu appears. Select the submenu option as shown in Table 7-11 and press Return.

Table 7-11. RTU Information

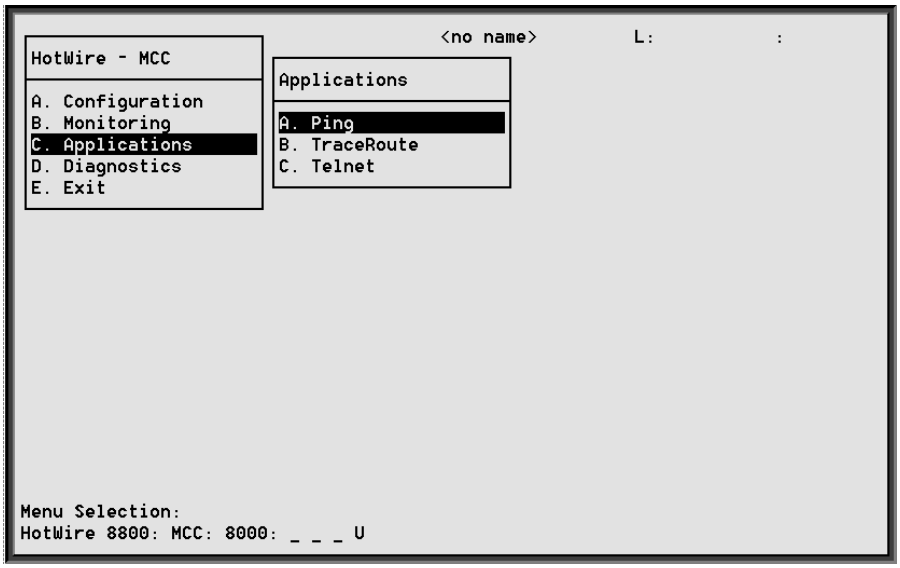
RTU Information	B-F-A
Displays RTU information such as RTU type, system, location, and contact, model number, serial number, version of firmware, and version of hardware.	
Port # – Enter the RTU port number.	
RTU Type – Model number of endpoint. For Model 8540, possible endpoints are 5170/5171/5246/5216. For Model 8546, possible endpoints are 5446r1/5446r2/5586).	
System Name – Name assigned to the card.	
System Contact – Name of number of the person responsible for the card.	
System Location – Physical location of the system.	
Model Num – Model number of card. (This field only appears on Model 8540 and is read only.)	
Serial Num – Serial number of card. (This field only appears on Model 8540 and is read only.)	
Firmware Rev. – Version of firmware. (This field only appears on Model 8540 and is read only.)	
Hardware Rev. – Version of hardware. (This field only appears on Model 8540 and is read only.)	

Diagnostics and Troubleshooting

8

Applications Screens

Use the Applications submenu to perform a Ping, TraceRoute, or Telnet (MCC only) to a remote host or client.



▶ Procedure

To use the Ping, Trace Route, and Telnet functions:

1. Follow these menu sequences:

   Applications → *Ping* (**C-A**)

   Applications → *TraceRoute* (**C-B**)

   Applications → *Telnet* (**C-C**)

2. Select Applications from the HotWire MCC or DSL main menu.

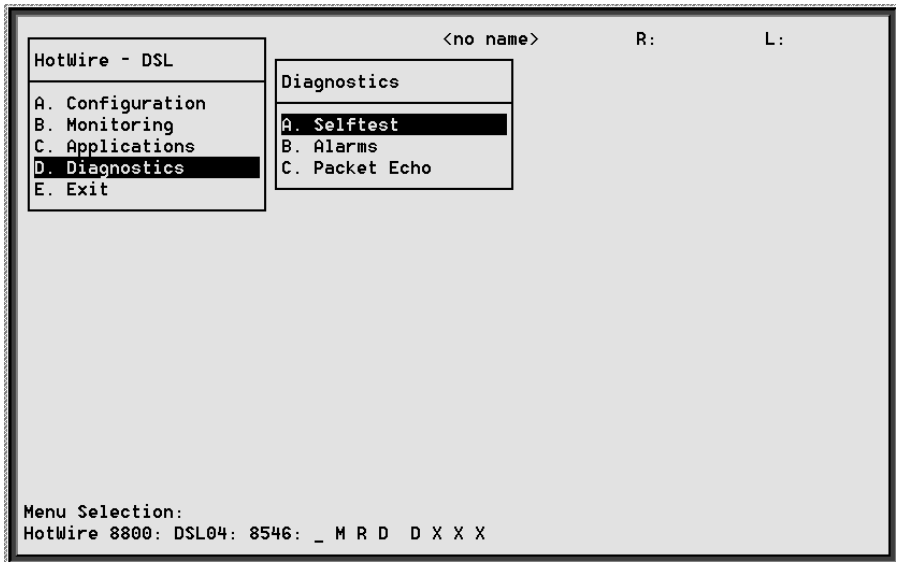
3. The Applications menu appears. Select the submenu option and enter the desired value on each screen and field as shown on Table 8-1 and press Return.

Table 8-1. Applications Options

Ping (MCC and DSL)	**C-A**
Gives the user the ability to conduct a non-disruptive packet test between the MCC or DSL card and any IP-aware device with network connectivity. Downstream devices include HotWire RTUs and user host computers; upstream devices include Network Access and Service Provider routers, switches, and Network Management System (NMS) stations. **IP Address** – *nnn.nnn.nnn.nnn* format. **Packet** – 12–1600 bytes (Default = 64). **Timeout** (wait time for return packet before next try) – 1–30 seconds (Default = 5). The results of this test include packets sent, received, and a scrolling list of timeouts, along with the minimum, maximum, and average round trip times of the packets. NOTE: The test will continue until you exit the screen.	
TraceRoute	**C-B**
Displays trace routing information to destinations of up to 64 hops away from the DSL card. **Destination IP Address** – IP hostname or address in *nnn.nnn.nnn.nnn* format. **Packet size** – Length of the packet in bytes.12–1600 bytes (Default = 38). **MaxHops** – Maximum number of hops for tracerouting. **Timeout** – Maximum time (in seconds) that the system should wait before assuming that the packet was lost. 1–30 seconds (Default = 5). After the above information is entered, a results screen is displayed. Results include a list of reporting hops, each with a hop number and IP address.	
Telnet (MCC Card only)	**C-C**
Gives the user the ability to connect with a remote host. Enter the host name or the Internet Protocol address for the destination to which you wish to connect. NOTE: To enter the host name, either the DNS server or the Host Table must be configured.	

Diagnostic Screens

Use the Diagnostics submenu to perform self-tests or view alarm status.



▶ Procedure

To view selftest, card alarm, and packet test information:

1. Follow these menu sequences:

   Diagnostics → *Selftest* (**D-A**)

   Diagnostics → *Alarms* (**D-B**)

   Diagnostics → *Packet Echo Test* (**D-C**)

2. The Diagnostics menu appears. Select the submenu option and enter the desired value on each screen and field as shown in Table 8-2 and press Return.

Table 8-2. Diagnostics Options

Selftest	**D-A**
Displays the results of the last disruptive selftest of the DSL card. This selftest is only performed on power up of the system or a reset of the card. Each subsystem (processors, memory, and interfaces) reports pass or fail. If all subsystems pass, the card has passed selftest. If a subsystem fails, reset or replace the card. You can determine when the selftest occurred by reading the elapsed time since the last reset on the card.	
Alarms (Card Alarms)	**D-B**
Displays all active card alarm conditions. Major alarms include Selftest failure, Processor failure (sanity timer), and DSL or Ethernet port failures. Minor alarms include Config Error (configuration has been corrupted) and threshold exceed for DSL margin, Error Rate, or Link Down events.	
Packet Echo Test	**D-C**
Gives the user the ability to conduct a non-disruptive packet test between the DSL card and HotWire RTU endpoint. Test packets are sent to the RTU at 10 percent of the line rate and echoed back to this card, where they are counted and checked for errors. You do not have to specify the IP address of the RTU. The running time of the test can be specified (15 to 900 seconds), and the test will continue until the specified time has elapsed or the test is stopped. Results include packets sent, valid packets received, errored packets received, errored seconds, and elapsed time of the test. NOTE: Only one port can be entered at a time.	

Troubleshooting

The status of each card in the HotWire DSLAM is indicated on the Card Selection screen (see Chapter 2, *HotWire Menus and Screens*). Choose Card Selection from the HotWire Chassis Main Menu.

The status of each DSL card is indicated by codes being displayed in any of eight positions to the right of the card selected. For example, if you select DSL card in Slot 4, the following may be displayed:

```
4: MODEL #  _ M R D  U X X X
Pos:          1 2 3 4  5 6 7 8
```

This display indicates that there is a Major Alarm on the DSL card in Slot 4, and that, while Ethernet and DSL Ports 1 and 2 are up, DSL Ports 3 and 4 are disabled.

The following table explains the codes by position.

Position	Display	Description
	<card type>	MCC
1	T (Test mode)	Card currently in test mode
2	M (Major alarm)	Major alarm present on card
3	R (Minor alarm)	Minor alarm present on card
4	e (Ethernet)	Status of Ethernet link (U=UP, D=Down, or X=Disabled)
5	d1 (DSL)#	Status of DSL card Port 1 (U=UP, D=Down, or X=Disabled, or H=Handshaking)
6	d2 (DSL)#	Status of DSL card Port 2 (U=UP, D=Down, or X=Disabled, or H=Handshaking)
7	d3 (DSL)#	Status of DSL card Port 3 (U=UP, D=Down, or X=Disabled, or H=Handshaking)
8	d4 (DSL)#	Status of DSL card Port 4 (U=UP, D=Down, or X=Disabled, or H=Handshaking)
9	w1 (WAN)*#	Status of WAN link (U=Up, D=Down, L=Loopback)
–	w2 (WAN)*#	Status of WAN link Port 2 (U=Up, D=Down, L=Loopback)
–	w3 (WAN)*#	Status of WAN link Port 3 (U=Up, D=Down, L=Loopback)
–	w4 (WAN)*#	Status of WAN link Port 4 (U=Up, D=Down, L=Loopback)
* Not applicable for 8540 or 8546 DSLAM RADSL circuit cards of MCC cards. # Not used for MCC cards.		

Checking Alarms

If the Card Selection screen indicates that a Major or Minor Alarm is on a card, follow the menu sequence *Diagnostics* → *Alarms* (**D**-**B**) to determine the cause of the alarm.

> **NOTE:**
>
> If a DSL card does not appear on the Card Selection screen because the MCC card can no longer communicate with it, the MCC card will generate a major alarm. You should go to the MCC's *Monitor* → *Card Status* → *Syslog* (**A-A-C**) and view the event on its system log.

Major Alarms

Use Table 8-3 to determine the appropriate action to take for each Major Alarm.

Table 8-3. Major Alarms (1 of 2)

Failure Type	Action
Selftest failure:	1. Check the Selftest Results display by following the menu sequence: *Diagnostics* → *Selftest.* 2. Do another Selftest (Reset) and check results. – If the results are normal, the problem was transient. Log the results. – If the results are the same as the first selftest, the card should be replaced. If only one port on a DSL card is bad, that port can be disabled. You may continue to use the card until it is convenient to replace it.
Processor failure (Sanity timer):	1. Check the Selftest Results display by following the menu sequence: *Diagnostics* → *Selftest.* 2. Do another Selftest (Reset) and check results. – If the results are normal, the problem was transient. Log the results. – If the results are the same as the first selftest, the card should be replaced.

Table 8-3. Major Alarms (2 of 2)

Failure Type	Action
Ethernet port failure	1. Check cable connections to the DSLAM. – If cables are terminated properly, go to Step 2. – If cables are not terminated properly, terminate them correctly. 2. Check cable connections to the Hub or Ethernet switch. – If cables are terminated properly, go to Step 3. – If cables are not terminated properly, terminate them correctly. 3. Check the Activity/Status LED at the Ethernet Hub or Switch. – If Activity/Status LED does not indicate a problem, go to Step 4. – If Activity/Status LED indicates a problem, take appropriate action. 4. Disconnect the Ethernet cable and replace it with a working cable from a spare port on the Hub. – If the replacement cable works, the original is bad and should be permanently replaced. – If the replacement cable does not work, reconnect the original cable and go to Step 5. 5. Move the DSL card and cable to another (spare) slot. – If this solves the problem, the connector or interface panel connections for the original slot are bad. Schedule maintenance for the chassis and try to use the spare slot temporarily. – If this does not solve the problem, the DSL card is probably bad and should be replaced.
DSL port failure	1. Check the Selftest Results display by following the menu sequence: *Diagnostics* → *Selftest.* 2. Do another Selftest (Reset) and check results. – If the results are normal, the problem was transient. Log the results. – If the results are the same as the first selftest, the card should be replaced. If only one port on a DSL card is bad, that port can be disabled. You may continue to use the card until it is convenient to replace it.
DSL card not responding (LEDs on card are out or MCC is showing an alarm.)	1. Check to see if the lights are out on the card. – Plug the card into an empty slot to see if it responds. If not, the card is bad and needs to be replaced. – If the card responds in a different slot, the slot connector may be bad. Call your service representative. 2. Check to see if the lights are on, but not responding. – Pull the card out and plug it in again. – Reset the card from the MCC or DSL Main Menu. – Go to the MCC Main Menu and clear NVRAM. – Replace the card.

Minor Alarms

Use Table 8-4 to determine the appropriate action to take for each Minor Alarm.

Table 8-4. Minor Alarms (1 of 2)

Failure Type	Action
Config Error:	1. Check the Selftest Results display by following the menu sequence: *Diagnostics → Selftest.* 2. Do another Selftest (Reset) and check results. – If the results are normal, the problem was transient. Log the results. – If Selftest results still show configuration corruption, there is a card problem. The card's non-volatile RAM should be erased and the configuration reentered. Perform a configuration download. – If the configuration has not been saved, use reset and erase NVRAM to force the card to the factory default. Enter the basic default route to the MCC and reconfigure the card manually.
NOTE: The following are minor alarms where thresholds have been exceeded and are primarily indications of degraded quality on the DSL loop. They are not necessarily related to problems with the DSL card.	
Margin Threshold (A trap message sent if margin falls below selected value.)	■ If DSL speed is set to a Fixed Rate, you may choose to lower the speed in the direction indicated by the threshold alarm (Fixed Up Speed or Fixed Down Speed) to get a better Margin and improved error performance. ■ If DSL speed is set to Rate Adaptive and the Margin Threshold is > 0, then this alarm is a warning that the loop has degraded. The actual bit rate should still be above 10^{-7}. This condition may be temporary due to high temperature or humidity/rain, or it may be permanent due to high noise from additional digital circuits installed in the same cable bundle. ■ If DSL speed is set to Rate Adaptive and the Margin Threshold is < 0, then this alarm is a warning that the loop has seriously degraded. The actual bit rate may be below 10^{-7}. This condition may be temporary or permanent. However, if it persists, the loop may have to be reengineered for better performance by performing one of the following: – Remove bridge taps – Change cable gauge on a cable section – Run new cable – Remove other noise-generating digital circuits from the cable bundle

Failure Type	Action
Error Rate Threshold (A trap message sent if the Block Error Rate averaged over a period of time exceeds the selected value.)	■ If the Error Rate Threshold is < 10^{-4}, then this alarm is a warning that the loop has degraded. The actual bit rate should still be above 10^{-7}. This condition may be temporary due to high temperature or humidity/rain. It may be permanent due to high noise from additional digital circuits installed in the same cable bundle. ■ If the Error Rate Threshold is >10^{-4}, then this alarm is a warning that the loop has degraded. The actual bit rate may be below 10^{-7}. This condition may be temporary or permanent. However, if it persists, the loop may have to be reengineered for better performance by performing one of the following: – Remove bridge taps – Change cable gauge on a cable section – Run new cable – Remove other noise-generating digital circuits from the cable bundle
Link Down Threshold (A trap message sent if the number of DSL link down events in 15 minutes exceeds the selected value.)	■ If the threshold is set low (1–4), and the link is currently down, then there may be a loop or RTU problem. Check both. – Verify that the RTU is powered up, is connected to the loop, and has passed its Selftest. – Check the loop for continuity ■ If the threshold is set low (1–4), and the link is currently up, then an event had occurred to temporarily knock out the connection. Log the event and continue normal operation. ■ If the threshold is set high (> 4), and the link is currently down, then check the Margin statistics over the past hour and day. If the numbers are low, there may be a situation where the DSL modems cannot train. This condition may be temporary or permanent. However, if it persists, the loop may have to be reengineered for better performance by performing one of the following: – Remove bridge taps – Change cable gauge on a cable section – Run new cable – Remove other noise-generating digital circuits from the cable bundle ■ If the threshold is set high (> 4) and the link is currently up, then there may be a loose connection in the loop plant, or the loop is barely usable. Check the Margin. If the Margin is normal, there may be a loose connection. If the Margin is low, try reducing the speed of the DSL port.

Network Problems

Review the following symptoms and possible solutions to help in solving any problems you may encounter on the HotWire DSLAM.

PROBLEM: Intranetworking communication problems.

ACTION:

1. Verify that the internetworking network cables meet IEEE standards for local Ethernet networks.
2. Check cable connections to DSLAM and other devices in the network.
3. Determine whether or not your system is the only one in the network with a problem.

PROBLEM: Cannot PING or Telnet after entering IP address.

ACTION:

1. Restart the interface (see *Configuration* → *Interfaces* (**A-C**) in Chapter 6).
2. Reset or power cycle before the IP address changes take effect.
3. Check to see if you entered the correct IP address (see *Who Am I* screen in Chapter 3).
4. Check to see that the IP address is unique and matches the class of the subnet. (For example, if using a Class B address, make sure the first two numbers match.)
5. Check to see that the sub-net mask is set correctly. If in doubt, leave the default sub-net mask (see *Who Am I* screen in Chapter 3).
6. Check to see that the IP next-hop address matches that of the router (if communicating through IP router) (see *Configuration* → *IP Route*r (**A-E**) in Chapter 5).
7. Verify that your address, port, or IP protocol is not being filtered from the port or bridge. (Turn off the filters if you are not sure.)
8. Check to see that the port in question is forwarding traffic.
9. Check received packets (see *Monitoring* → *Network Protocol* (**B-D**) in Chapter 7).

Slow Performance

PROBLEM: Performance is slow.

ACTION:

1. Verify that there are enough buffers on the System Info screen (see *Monitoring* → *Card Status* (**B-A**) in Chapter 7).
2. Check the Ethernet Statistics screen for excessive Cycle Redundancy Check (CRC) errors (see *Monitoring* → *Physical Layer* (**B-B**) in Chapter 7).

Excessive Collisions

PROBLEM: Excessive collisions on an Ethernet port.

ACTION:

1. Determine if your network is too large or long (single Ethernet cable or end-to-end cable).
2. Check to see if there are too many repeaters.
3. Check to see if there are too many users on a single Ethernet.

No SNMP Connection Established

PROBLEM: Cannot establish an SNMP session/connection.

ACTION:

1. Try to ping the MCC card and/or DSL card from the management system.
2. If you cannot, check to see that you have entered an IP address and subnet mask (see *Who Am I* screen in Chapter 3).
3. If there is an IP address, then check the routing tables in the MCC card and DSL card.
4. Check to see if the community string is correct.
5. If IP Address Security is enabled, check to see that Network Management's IP address has been entered correctly in the MCC card's and DSL card's permission list and that it has proper access.
6. Check to see if you have properly configured the SNMP parameters (see *Monitoring* → *Network Protocol* (**B-D**) in Chapter 7, especially *SNMP Security: Configuration* → *SNMP* (**A-F**) in Chapter 6).

Filters Not Working

PROBLEM: Filters are not working properly.

ACTION:

1. Check to see that filters have been configured properly (see *Configuration* → *Interfaces* (**A-C**) in Chapters 5 and 6).
2. Check to see if there is a conflict with the order of the filter tests. They should perform in the following order: Port-to-Port (PTOP), Host-to-Port (HTOP), Host-to-Host (HTOH), Protocol Type (PROTOCOL), Bit Filtering.

IP Routing Problems

PROBLEM: Stations cannot communicate through the router.

Incorrect IP address.

Incorrect Subnet Mask

ACTION:

1. Check to see that IP addresses have been configured correctly (see *Who Am I* screen in Chapter 3, and *Configuration* → *Interfaces* (**A-C**) in Chapters 5 and 6).
2. Go to: *Configuration* → *Interface* → *Control* (**A-C-C)** and monitor the state of the system for e1a Bridge Up (forwarding).

No PPP Traffic

PROBLEM: PPP circuit is forwarding no traffic.

ACTION:

1. Verify that the DSL link is up.
2. Go to: *Configuration* → *Interface* → *Control* **(A-C-C**) and monitor the state of the system.
3. If the IP state is up and the local and peer IP addresses are displayed, IPCP is completed.
4. If the IP state is missing from the screen, check that the port has an IP address assigned.
5. If the IP state is missing from the screen, check that the port has an IP address assigned.

No Response at Start Up

PROBLEM: DSL cards do not respond at start-up after rebooting chassis.

ACTION:

1. Reset the MCC card.
2. Be sure LEDs go through the reset sequence once. Then, a second time after 15–20 seconds.
3. Reconfigure each DSL card (see *Configuration* → *Card Status* (**A-A**) in Chapter 6).

System Does Not Recognize New DSL Cards

PROBLEM: System does not recognize new DSL cards with new addresses (Addresses not pre-configured on MCC card).

ACTION:

1. Configure new DSL cards from MCC screen.
2. Restart s1b interface (see *Configuration* → *DSL Cards* (**A-G**) in Chapter 6).
3. Reset DSL card from the MCC screen (see *Configuration* → *DSL Cards* (**A-G**) in Chapter 6).
4. Pull the card out and push it back in.

Large Number of TRAPS

PROBLEM: DSL cards not using MCC Router ID as source address for traps.

ACTION:

1. In standard configuration, MCC and DSL are in separate subnets and Router ID is the same as IP Base Address of MCC's LAN (*e1a*) interface. Set the Router ID to the management IP address on MCC's LAN interface.
2. Set this as "Base IP Address" for LAN interface.
3. Reset MCC and all cards (see *Configuration* → *DSL Cards* (**A-G**) in Chapter 4).

Cannot Communicate with Interface

PROBLEM: Cannot communicate with Ethernet or other interface after adding, changing, or deleting IP addresses on DSL or MCC card.

ACTION:

1. When you add, change, or delete addresses on a DSL card, you must restart that interface (see *Configuration* → *Interfaces* (**A-C**) in Chapter 6).

Cannot Upload Configurations to a Unix Server

PROBLEM: TFTP server denies write permission (Message is “TFTP recv failure”).

ACTION:

1. Before uploading configurations, create a dummy file and give it global Read-Write permissions.
2. Configure TFTP host to have Write permissions is specified directory.

Unexpected Subnet Data

PROBLEM: Proxy ARP not properly set for HotWire 5446 RTU.

ACTION:

1. Reconfigure DSL cards affected.
2. Set Proxy ARP only for HotWire 5446 RTU, not entire subnet.
3. Using structured subnetting, verify proper subnetting was utilized.

Cannot Communicate with 5446 RTU from MCC Card

PROBLEM: Error in setting peer address on s1b.

ACTION:

1. Set peer host address to 0., for example, where MCC’s *s1b* address is 198.152.180.10 and local subnet is “180”, peer address must be set to 198.152.180.0.

Checklist for Setting Up User Accounts on the MCC and DSL Cards

A

Overview

User accounts provide security for the DSLAM by requiring that anyone who is trying to log onto the system has a valid password to gain access. User accounts on the MCC provide security to users accessing the system from the VT100-compatible terminal interface and via Telnet over the management domain LAN.

It is recommended that user accounts also be set up for each DSL card, even if you do not intend to telnet directly to the DSL cards, so that no unauthorized telnet sessions can be made. Each card will support up to 10 user accounts with either Operator (read only) or Administrator (read/write) permissions.

MCC User Accounts (For Telnet Terminal Access to MCC Card)

Use the following checklist when configuring MCC user accounts.

From the MCC Main Menu, select *Configuration* → *Users* → *Accounts* (**A-D-A**).

- ❑ Enter the login name (up to 15 characters). This field is case sensitive.
- ❑ Enter the password for this account (up to 15 characters). This field is case sensitive.
- ❑ Re-enter the password.
- ❑ Enter the privilege level (operator for read-only access, administrator for read/write access).
- ❑ Enter **Y** to save changes and Ctrl-z to return to the HotWire Chassis Main Menu tree.

Reboot Card (MCC)

Use the following checklist to reboot MCC card after changes have been made.

From the MCC Main Menu, select *Configuration* → *Card Status* → *Card Reset* (**A-A-F**).

- ❑ Enter **Y** at the yes/no prompt.
- ❑ At the initial screen display after reboot, press Return.

  To verify that a DSLAM system account has been setup, at the prompt:
- ❑ Enter Operator ID.
- ❑ Enter Operator Password.

  The HotWire Chassis Main Menu is displayed.

DSL User Accounts

Use the following checklist when configuring DSL user accounts (if telneting directly to the DSL card).

From the DSL Main Menu, select *Configuration* → *Users* → *Accounts* (**A-D-A**).

- ❑ Enter the login name (up to 15 characters). This field is case sensitive.
- ❑ Enter the password for this account (up to 15 characters). This field is case sensitive.
- ❑ Re-enter the password.
- ❑ Enter the privilege level (operator for read-only access, administrator for read/write access).
- ❑ Enter **Y** to save changes and Ctrl-z to return to the HotWire Chassis Main Menu tree.

Reboot Card (DSL)

Use the following checklist to reboot DSL cards after changes have been made.

At the Card Selection screen, enter DSL*nn*.

From the DSL Main Menu, select *Configuration* → *Card Status* → *Card Reset* (**A-A-F**).

❑ Enter **Y** at the yes/no prompt.

To verify that a DSL card account has been set up:

❑ After reboot, enter MCC at the Card Selection screen.

Select *Applications* → *Telnet* (**C-B**).

❑ Enter the IP Address of Ethernet card and verify that you can telnet there.

❑ Enter Operator ID.

❑ Enter Operator Password.

The DSL Main Menu is displayed.

Checklist for Setting Up SNMP Features

B

Setting Up SNMP Features

Use the following checklist when setting up SNMP features.

MCC SNMP Community Strings and Authentication Failure Trap

From the MCC Main Menu, select *Configuration* → *SNMP* → *Communities/Traps (***A-F-C**).

- ❑ Enter Read Only community string name(s).
- ❑ Enter Read Write community string name(s).
- ❑ If desired, enable the Authentication Failure Trap.
- ❑ Enter the IP address of addresses of the NMS.

Management System Source Validation for MCC

While optional, it is recommended, for additional security, that source validation is enabled.

From the MCC Main Menu, select *Configuration* → *SNMP* → *Security* (**A-F-A**).

- ❑ Enable IP address security validation.
- ❑ Enter the IP address of up to five NMS managers that will be permitted access to the MCC card.
- ❑ Enter access permission to be granted to each NMS system (ReadOnly(ro)/Read/Write(rw)/NoAccess(na)).

Management System Source Validation for DSL cards

From the DSL Main Menu, select *Configuration* → *SNMP* → *Security* (**A-F-A**).

- ❑ Enable IP address security validation.
- ❑ Enter the IP addresses of up to five NMS managers that will permitted access to this DSL card.

  ☑ Each card does not have to have the same set of managers as any other card or as the MCC.

- ❑ Enter access permission to be granted each NMS system (ReadOnly(ro)/Read/Write(rw)/NoAccess(na)).

DSL SNMP Community Strings and Authentication Failure Trap

From the DSL Main Menu, select *Configuration* → *SNMP*→ *Communities/Traps* (**A-F-C**).

- ❑ Enter Read Only community string name(s).
- ❑ Enter Read/Write community string name(s).
- ❑ If desired, enable the Authentication Failure trap.

Enable DSL Port Traps

From the DSL Main Menu, select *Configuration* → *Ports* → *DSL Ports* (**A-B-B**).

- ❑ Select a DSL port.
- ❑ If desired, enter a value for the Margin Threshold.
- ❑ If desired, enter a value for the Link Down Count Threshold.
- ❑ If desired, enter a value for the Error Rate (minute) Threshold.
- ❑ If desired, enter a value for the Error Rate (hour) Threshold.
- ❑ Reset the port (**A-C-C**).

Enable/Disable Endpoint Security to 5446 RTU

From the DSL Main Menu, select *Configuration* → *SNMP*→ *Security* (**A-F-A**).

- ❑ Select an endpoint cookie.
- ❑ Enable/Disable endpoint security for the specified port.

Download Code and Apply Download

C

The Download Code menu option on the HotWire DSLAM gives you the ability to upgrade your software with a new version of code and then apply this code to your system.

> **NOTE:**
>
> Before attempting a download, verify that you can ping or telnet to the TFTP server. If you can not, do not proceed with the download. Also, make certain that the files that you are going to download from exist in the system.

New firmware releases are typically applied to either the MCC or DSL cards in your system. When a software upgrade affects both the MCC and the DSL cards, you must download and apply a new version of code into each of the DSL cards **before** you download and apply a new version of code into the MCC.

Download Code

From the MCC or DSL Configuration Main Menu, select *Configuration* → *Card Status* → *Download Code* (**A-A-G**). This selection brings you to the Download submenu. Select Download Code.

Scenario One: Fully Operational System

Enter the path and image file name and the TFTP Server IP address and select yes to begin the file transfer. When you are downloading the new firmware, this does not impact service or the operation of the system. Depending on the network traffic, this download may take a minimum of 10 minutes. You may apply the newly acquired firmware load at any time following the successful transfer.

> **CAUTION:**
>
> **When the download is completed, if you elect to apply the code, service will be disrupted while the card restarts and the new code is installed.**

Scenario Two: Download Only System

In order for the system to become fully functional again, you **must** start the Download Code file transfer procedure. Enter the image file name and the TFTP Service IP address and select yes to begin the file transfer. When the file transfer has successfully completed, the system will automatically restart and become fully functional with the newly acquired firmware.

Apply Download

From the MCC or DSL Configuration Main Menu, select *Configuration* → *Card Status* → *Download Code* (**A-A-G**). This selection brings you to the Download submenu. Select Apply Download.

Navigation Keys

D

The following table lists navigation keys and their definitions. These commands are used to move around the HotWire DSLAM menus and screens.

Keys	Definition
Ctrl-a	Moves Home or to the top of the menu
Ctrl-b	Moves left
Ctrl-c	Moves Home or to the top of the current menu
Ctrl-f	Moves right
Ctrl-k	Moves up to the previous menu selection or entry field
Ctrl-l	Refreshes the screen
Ctrl-n	Moves down or to the next selection
Ctrl-p	Moves up or to the next selection
Ctrl-r	Resets counters (on monitoring statistics displays)
Ctrl-t	Moves Home or to the top of the menu
Ctrl-u	Clears the current input or prompt line
Ctrl-v	Displays a pop-up list of all interfaces on IP Network screen. Displays a pop-up list of all accounts in system on Configure Accounts screen.
Ctrl-y	Moves Home or to the top of the menu
Ctrl-z	Moves back or exits from screen
Up arrow	Moves up to the previous menu selection or entry field
Down arrow	Moves down to the next menu choice or entry field
Left arrow	Moves left to the previous menu box or entry field
Right arrow	Moves right to the next menu box or entry field
Enter or Return	Accepts entry
Tab	Moves down or to the next selection
?	Displays the Online help screen

Traps

E

Traps are configured via a Telnet or terminal session. The addition or removal of a card or another hardware component within the HotWire DSLAM system causes a trap to be generated. These traps indicate a configuration change notification (CCN) of a card (a hardware replacement or a software upgrade).

The DSL card sends the following traps.

Event	Trap Class	Comment
Device failure	major	—
Self-test failure	minor	Sent if any portion of a restart/self test fails.
CCN (Configuration Change Notice)	warning	Configuration change caused by one the following events: ■ software download ■ configuration download ■ card removed
Entity MIB CCN (Configuration Change Notice)	warning	Configuration changed caused by changes affecting the entity MIB.
xDSL link up or down Transitions threshold exceeded	minor	Number of link down events above threshold. This rate is limited to once every 15 minutes.
Authentication failure	minor	SNMP community string.
Authentication failure	minor	Telnet passwords. This trap may be overloaded for Telnet based auth failures. In these cases, the following will also be sent along with the trap PDU: ■ Access mode used ■ Number of Auth failures
xDSL port speed low	warning	Port speed decreased to lower bound threshold setting.
xDSL port speed normal	normal	Port speed now above lower bound.

Event	Trap Class	Comment
Ethernet link down	major	—
Ethernet link up	normal	—
xDSL margin low	minor	Margin estimate below customer set threshold.
xDSL margin normal	normal	Margin estimate above customer set threshold.
xDSL error rate high	minor	Error rate estimate above customer set threshold.
xDSL error rate normal	normal	Error rate estimate now below customer set threshold.
xDSL port failure	major	Processor detected bad DSL modem chip set.
xDSL port operational	normal	Processor can now communicate with DSL modem chip set.
Cold start	warning	Card has been reset and performed a cold start.
Warm start	warning	Power on reset.
xDSL test start	normal	Test started by any means.
xDSL test clear	normal	Test over.
DHCP filter security failure	minor	Filter based security could not be enabled because the maximum number of filter rules has been reached.
Dynamic filter injection failure	warning	Cannot inject or delete dynamic filters to RTU on port N.

The MCC card sends the following traps.

Event	Trap Class	Comment
Device failure	major	—
Self test failure	minor	Sent if any portion of a restart or selftest fails.
CCN (Configuration Change Notice)	warning	Configuration changed or software upgraded.
Entity MIB CCN (Configuration Change Notice)	warning	Configuration changed due to differences affecting Entity MIB.
Authentication failure	minor	SNMP community string mismatches.
Authentication failure	minor	Telnet and terminal password mismatches. This trap may be overloaded for terminal and Telnet based auth failures. In these cases the following will also be sent along with the trap PDU: — Access mode used — Number of auth failures For SNMP based auth failures, no information will be sent.
Fan module failure	major	Fan module reporting subnormal performance.
Fan module operational	normal	Fan module back to normal operation.
A power source failure	minor	Power source A has failed and the system is now operating off one source.
A power source normal	normal	Power source A is now operating normally.
B power source failure	minor	Power source B has failed and the system is now operating off one source.
B power source normal	normal	Power source B is now operating normally.
Ethernet link down	major	—
Ethernet link up	normal	—
Slot poll failure	major	No response to slot poll. Responds to hardware MIP query, but not general poll.
New card detected	warning	New card detected by MCC on slot poll.
Cold start	warning	MCC card is being powered up.
Warm start	warning	Power on reset.

RTU Related Traps

The RTUs send the following traps. For a listing of Paradyne Enterprise MIBS, see Chapter 8 of the *Hotwire DSLAM for 8540 and 8546 DSL Cards Network Configuration Guide.*

Standard Traps

Event	Trap Class	Comment
Authentication Failure	minor	■ Community string used is not in the Community Table. ■ Use of read only community string for Set PDU.
Warm start	warning	RTU has been reset by an NMS.

Enterprise-Specific Traps

Event	Trap Class	Comment
Enterprise device failure	major	Operating software has detected an internal device failure. The RTU is still operating.
Enterprise selftest failure	minor	Failure of the RTU's hardware components. This trap is only sent if the hardware failure still allows sending traps.
Enterprise fatal reset	major	Variable-bindings field contains device failure code.
RTU device mismatch (Sent by the DSL card)	minor	RTU identified on port N does not match device described in port configuration table.
RTU device mismatch (Sent by the DSL card)	normal	RTU identified on port N now matches device described in port configuration table.

5446 RTU Setup

F

5446 RTU Overview

The RADSL 5446 RTU has an IP configuration table that is updated through an SNMP agent. The configuration table contains IP address and subnet mask information.

The network service provider for the 5446 RTU provisions the IP address information into the 5446 RTU's configuration table. The 8546 DSL card interoperates with the 5446 RTU. An NMS communicates via SNMP to Get or Set objects within the SNMP agent's control to update the IP configuration table. The 5446 RTU supports MIB objects relative to their RFC description.

The following sections explain:

- Accessing 5446 RTU MIBs
- Using Standard MIBs (MIB II)
- SNMP Traps supported by the RTU

For more information about the 5446 RTU installation, see the *HotWire 5446 Remote Termination Unit (RTU) Customer Premises Installation Instructions.*

Accessing 5446 RTU MIBs

There are three methods available to update the 5446 RTU IP configuration table:

- Paradyne's IP Injection Tool
- NMS DCE Manager
- MIB Browser

The IP Injection Enterprise MIB must be used to finalize the 5446 RTU setup. The IP Injection Tool and the Enterprise MIBs are available on Paradyne's World Wide Web site:

http://www.paradyne.com

IP Injection Tool

This tool is available from Paradyne's Power Pages World Wide Web site. The program is in a zip file that expands to three disks.

This tool can be loaded on a PC with a Windows 95 or a Windows NT 4.0 platform. The PC must be connected to the management interface for the MCC card *(e1a).*

▶ Procedure

To download the IP Injection Tool:

1. Access the Paradyne World Wide Web site:
   http://www.paradyne.com
2. Select:
   Service & Support → MIBs → HotWire DSL → ipinject.exe
3. Follow the steps for your program to unzip the IP Injection Tool. If you have:
   - — WinZip: Extract the files
   - — PKunzip: Unzip using the -d option to create three disks
4. Double-click on Disk 1 and double-click on **Setup.exe**.
5. At the prompt: Do you wish to install Microsoft OLE Automation?
   - — Windows 95 platform: answer Yes
   - — Windows NT 4.0 platform: answer No

When the program is successfully installed, an icon labeled IP Injection Tool is created. Utilize the online Help file for further information.

Network Management Systems

DCE Manager, Paradyne's Network Management System, communicates via SNMP to the RTU to update the IP configuration table. Display of the remote RTU and the use of the injection tool are features of this product.

The NMS workstation is typically connected to a router and the NMS can easily access devices on other subnets. If the NMS is connected to other hardware, such as a hub, then the explicit routes to the other subnets must be defined on the system that has the NMS.

To create the routes that would be discovered with a router connection, the DCE Manager must have access to the MCC backplane s1b subnet in the DSLAM. The MCC card acts as the gateway to add the first route to gain connectivity to the DSL cards and remote RTUs. Open a DOS window and enter the command Route.

Windows 95 syntax example:

- NMS = 135.90.51.1
- MCC card = 135.90.51.220 on the same subnet as the NMS 130.90.51
- DSL card = 135.90.52.10 on subnet 135.90.52
- 5446 RTU = 135.90.52.12 on the same subnet as the DSL card 135.90.52

Windows 95 route statement for the NMS at 135.90.51.1:

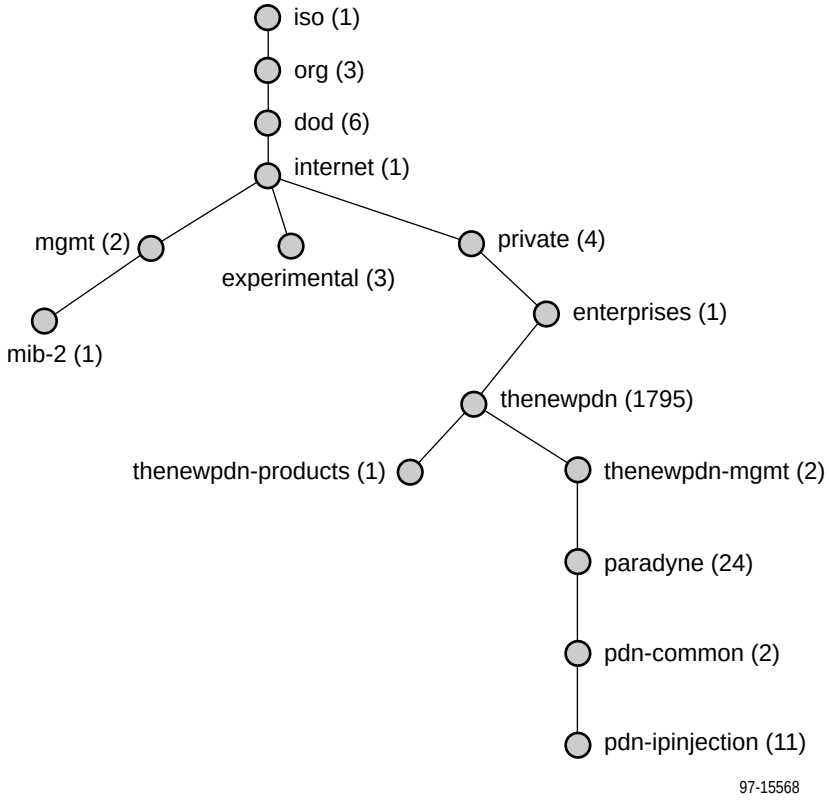
```
route add 135.90.52.10 135.90.51.220
route add 135.90.52.12 135.90.51.220
```

MIB Browser Techniques

There are two MIB browser techniques. The Enterprise MIB allows the use of a null entry or a table index. Use a MIB browser to access the ipInjectionTable. Refer to the *Assigning IP Addresses to the DSL Card LAN* section in Chapter 4, for additional IP address information.

The Enterprise IP Injection MIB OID (Object ID) is 1.3.6.1.4.1.1795.2.24.2.11.

IP Injection MIB OID



▶ Procedure

From an SNMP workstation:

1. To load the MIB, access the Paradyne World Wide Web site:
   http://www.paradyne.com
2. Select:
   Service & Support → MIBs → HotWire DSL → pdndce.mib
3. Enter the IP address of the RTU.
4. Press Options to change Set Community to Private.
5. Locate the MIB group pdn-ipinjection.

From a MIB browser, do a single set with a unique entry containing the required fields. Refer to Table F-1 for IP injection group objects.

Using the null entry:

▶ Procedure

1. Change the Null entry by entering the IP address (ipInjectionAddress).
2. Change the mask by entering a subnet mask (ipInjectionMask).
3. Change the Type to Service Provider or Host (ipInjectionType).
4. Select Set.
5. Do a Get or Query to verify before continuing to the next entry.

Using the table index:

▶ Procedure

1. Enter the three fields into the Index:
   - ipInjectionType
   - ipInjectionAddress
   - ipInjectionMask
2. Enter the status value:
   - ipInjectionStatus
3. Select Set.

If a null entry does not appear, the table is full. Delete entries from the table by setting the ipInjectionStatus to invalid.

5446 RTU IP Configuration Table

Host routes use the IP address assigned to the end-user systems supported by the 5446 RTU. Service domain IDs use the IP address information pertaining to the 5446 RTU within the service domain.

There must be three entries in the 5446 RTU IP configuration table:

- **NAP address.** This address is automatically injected across the DSL link from the DSLAM and cannot be modified.
- **Host address.** This is the IP address of the end-user system connected to the 5446 RTU and is the same IP address configured for the DSL port card. The address could also be a subnet address.
- **Service domain address.** This is the IP address for the 5446 RTU in the service provider domain.

IP and Device MIBs Supported

The following pdn-IP Injection Objects (pdn-common 11) contain IP address information. Information built from this table:

- Host IP routing. Displayed in the MIB II IP Route Table as read only.
- Service IP address. Displayed in the MIB II IP Address Table as read only.

IP Injection Table supports:

- One NAP IP Address injected as the Peer IP Address from the DSLAM. The NAP IP Address cannot be added, deleted, or changed from SNMP.
- Four service domain IDs.
- Thirty-two Host Routes and/or Subnets.

Table F-1. IP Injection Group Objects (ipInjectionTable 1)

Object	Description	Setting/Contents
ipInjectionType *(ipInjectionEntry 1)*	Type of address for each entry. Changing the NAP IP address resets the database and an entry of serviceProvider(3) or host(4) is cleared.	■ **null(1)** – Use to add a row. Factory defaults: – Address: **0.0.0.0** – Mask: **255.255.255.255** – Status: **static** ■ **nap(2)** – Network Access Provider IP entry. Cannot be added, modified, or deleted from SNMP. ■ **serviceProvider(3)** – Network Service Provider IP entry. ■ **host(4)** – Host IP entry.
ipInjectionAddress *(ipInjectionEntry 2)*	IP address information.	IP address for service domain ID, and NAP IP address: ■ ***nnn*.255.255.255** – Range for the first byte *nnn* is 001 to 223, with the exception of 127. Range for the remaining three bytes is 000 to 255. IP address for Host Route: ■ ***nnn*.255.255.255** – Range for the first byte *nnn* is 001 to 239, with the exception of 127. Range for the remaining three bytes is 000 to 255.
ipInjectionMask *(ipInjectionEntry 3)*	Subnet mask.	Subnet mask cannot be 0.0.0.0.
ipInjectionStatus *(ipInjectionEntry 4)*	Status of each entry.	Specify address status. When the RTU is reset, the static addresses are saved and dynamic addresses are not saved. Default is **static(1)**. ■ **static(1)** – Static addresses are assigned for the duration of the service subscription. ■ **dynamic(2)** – Dynamic addresses are only assigned for the duration of the application session. ■ **invalid(3)** – Used to delete an entry from the table.

Additional pdn-common MIBs Supported

The RTU also supports the following pdn-common MIBs:

- Device Status Group, pdn-common 4
- Device Traps Manager Group, pdn-common 9
- Device Control Group, pdn-common 10

Static Route Warning Messages

G

The following table lists warnings and error messages displayed on the Static Routes screen.

Message . . .	Meaning . . .
Routing Table: Route not added (MCC and DSL)	Route was saved into NVRAM but not added to the active routing table.
Routing Table: Route limit reached for interface (DSL)	Route was saved into NVRAM but not added to the active routing table because there are already 32 routes for the interface.
Routing Table: Route limit reached for routing table (MCC and DSL)	Route was saved into NVRAM but not added to the active routing table because the active routing table is full.
Routing Table: Client limit reached for interface (DSL – 8540 only)	Route was saved into NVRAM but not added to the active routing table because the endpoint connected has reached its client limit.
Routing Table: Interface not active (DSL – 8540 only)	Route was saved into NVRAM but not added to the active routing table because the endpoint is not connected at this time. When the interface comes up. the route will be added.
Routing Table: Next hop gateway currently unreachable (MCC and DSL)	Route was saved into NVRAM but not added to the active routing table because there is no way to reach the next hop gateway. If an interface comes up that has the next hop gateway, the route will be added.
Routing NVRAM: Database Error (MCC and DSL)	Route was not saved into NVRAM and not added to the active table. This is a general database error.
Routing NVRAM: Database Route Limit Reached (MCC and DSL)	Route was not saved into NVRAM and not added to the active table because the NVRAM is full.

Glossary

10BaseT	An Ethernet LAN that works on twisted-pair wiring.
Address	A symbol (usually numeric) that identifies the interface attached to a network.
Alarm System	Consists of an audible or visual alarm in the central office indicating the rack with an alarm condition.
ARP	Address Resolution Protocol. The TCP/IP protocol used to dynamically bind a high-level IP address to a low-level physical hardware address. ARP is only across a single physical network and is limited to networks that support hardware broadcast.
Authentication Server	An authentication server can either be a RADIUS server or an XTACACS server. An authentication server is used to confirm an end-user system's access location.
Backplane	A common bus at the rear of the HotWire 8800 DSL Access System chassis connecting each DSL card to the MCC card for diagnostic and network management. It also distributes dc power to each slot.
Bandwidth	The range of frequencies that a circuit can pass. The greater the bandwidth, the more information that can be sent in a given amount of time.
Bit	Binary digit. The smallest unit of information, representing a choice between a one or a zero (sometimes called mark or space).
BOOTP	Bootstrap Protocol. Protocol a host uses to obtain startup information , including its IP address, from a server.
bps	Bits per second. Indicates the speed at which bits are transmitted across a data connection.
byte	A sequence of successive bits (usually eight) handled as a unit in data transmission.
Central Office	The physical building where all local telephone service wiring is distributed to a surrounding area.
Default Route	An IP address specified as 0.0.0.0. A route used when no others have the desired destination.
DHCP	Dynamic Host Configuration Protocol.
DHCP Relay Agent	A component of the dynamic IP-addressing mechanism. The DSL card in the DSLAM acts as a DHCP relay agent between the end-user system and the DHCP server. The DHCP relay agent detects and forwards a DHCP discover or request message to the appropriate DHCP server. It also tracks the end-user IP address and lease time from the DHCP acknowledgement by updating the routing tables automatically.
DNS	Domain Name System. An online distributed database that maps machine names into IP addresses.
Domain	A block of IP addresses. Syntactically, all IP addresses within a given domain would share a common IP address prefix of some length.
Downstream	In extended networks, the direction in which diagnostic messages flow from the diagnostic control site to any intermediate links and then to the final tributary modem.
DSL	Digital Subscriber Line. DSL is a copper loop transmission technology enabling high-speed access in the local loop.

DSLAM Digital Subscriber Line Access Multiplexer. DSLAM provides simultaneous high-speed digital data access and analog POTS over the same twisted-pair telephone line.

Ethernet A type of network that supports high-speed communication among systems. It is a 10-Mb/s standard for LANs. All hosts are connected to a coaxial cable where they contend for network access using a Carrier Sence Multiple Access with Collision Detection (CSMA/CD) paradigm.

Ethernet Address A six-part hexadecimal number in which a colon separates each part (for example, 8:0:20:1:2f:0). This number identifies the Ethernet communications board installed in a PC and is used to identify the PC as a member of the network.

Filter A rule or set of rules applied to a specific interface to indicate whether a packet can be forwarded or discarded.

FTP File Transfer Protocol. A protocol that allows a user on one host to access, and transfer files to and from, another host over a network. The FTP application is used to provide file transfer services across a wide variety of systems through the use of the File Transfer Protocol (FTP). Usually implemented as application level programs, FTP uses the TELNET and TCP protocols. The server side requires a client to supply a login identifier and password before it will honor requests.

gateway address The subnet that the end-user system is on. This address, which is the e1a address of the domain, is used as the return address when the authentication server responds.

HDLC High-Level Data Link Control. A communications protocol defined by the International Standards Organization (ISO).

ICMP Internet Control Management Protocol. Internet protocol that allows for the generation of error messages, tests packets, and information messages related to IP.

Internet Worldwide interconnected networks that predominantly use the TCP/IP protocol. The Internet is a three level hierarchy composed of backbone networks, mid-level networks, and sub networks.

Intranet Private network that uses internet software and internet standards. The Intranet is reserved for use by people who have been given the authority and passwords necessary to use that network.

IP Internet Protocol. The TCP/IP standard protocol that defines the IP as a unit of information passed across an Internet and provides the basis for packet delivery service. IP includes the ICMP control and error message protocol as an integral part. The entire protocol suite is often referred to as TCP/IP because TCP and IP are the two most fundamental protocols.

IP Address Internet Protocol address. This is a 32-bit address assigned to host on a TCP/IP Internet. The IP address has a host component and a network component.

ISN Interservice Network.

ISP Internet Service Provider.

LAN Local Area Network. A network that spans a small geographic area (e.g., a building).

MAC Media-specific Access Control. A protocol where packets transmitted over LAN ports are encapsulated in Ethernet II MAC frames.

MAC Address Media Access Control Address. Areas of memory your CPU uses to distinguish between the various peripheral devices connected to your system when transferring or receiving data. The MAC address is also known as the physical address.

margin DSL margin is defined as the additional noise measured in db that would need to be added to (or if the margin is negative, subtracted from) the existing noise present on a given DSL loop to bring the Bit Error Rate (Ber) to IE-7 ($10^{7)}$ · Unless the noise source is defined (such as 24 BRI disturbers or 24 DSL disturbers, it is assumed to be Noise Model A (white noise).

MCC Card Management Communications Controller Card. The card in a HotWire DSLAM system or stack that is used primarily for monitoring and configuring the HotWire DSLAM.

MIB Management Information Base. A collection of information (e.g., configuration, status, and statistical data) within an SNMP agent that forms a database of information about the agent which is accessible from the NMS manager. MIB II is the current standard.

Multiplex Combine many low-speed data sources into a single, high speed serial data stream. The data is coded at transmission, and decoded at reception. Interleave or simultaneously transmit two or more messages on a single circuit. Some multiplexing techniques include Frequency Division Multiplexing (FDM), Time Division Multiplexing (TDM), and Statistical Multiplexing (Stat MUX).

NAP Network Access Provider. The NAP provides a transit network service permitting connection of service subscribers to Network Service Providers (NSPs). The NAP is typically the network provider (e.g., a Regional Bell Operating Company, an Alternate Local Exchange Carrier) that has access to the copper twisted pairs over which the DSLs operate.

NMS Network Management System. The system responsible for managing a portion of the network. An NMS communicates to a Simple Network Management Protocol (SNMP) agent via SNMP to obtain (get) or configure (set) specific parameters or variables within control of the SNMP agent (e.g., DCE Manager).

NSP Network Service Provider. NSPs can be either public data network providers (i.e., Internet Service Providers) or private data network providers (i.e., corporate intranets) who provide network services based on the Internet Protocol (IP). In some cases, the NSP and the NAP can be a single network provider.

Packet Used in this document to refer to a block of data sent across an IP switching network.

Peer Address IP address used to indicate directly connected systems.

Ping An IP-based application used to test reachability of destinations by sending an ICMP echo request and waiting for a reply. The ping program is supported from both the DSL and MCC cards.

POTS Plain Old Telephone Service.

POTS Splitter A device that filters out the DSL signal and allows the POTS frequencies to pass through. This device can be installed at the Central Office or Customer Premises.

PPP Point-to-Point Protocol. A protocol for framing IP when sending across a serial line. It allows a computer to connect to the Internet using a standard dial-up telephone line and a high-speed modem.

Proxy ARP Proxy Address Resolution Protocol (ARP). The technique in which one machine, usually a router, answers ARP requests intended for another by supplying its own physical address. By pretending to be another machine, the router accepts responsibility for forwarding packets. The purpose of proxy ARP is to allow a site to use a single IP network address with multiple physical networks.

RADIUS See Authentication Server.

RADSL Rate Adaptive Digital Subscriber Line. A transmission technology that supports both symmetric and asymmetric applications on a single twisted-pair telephone line and allows adaptive data rates.

Router	A special purpose, dedicated computer that attaches to two or more networks and forwards packets from one to the other.
Routing Table	A table that stores information about possible destinations for packets being routed through the HotWire DSLAM and identifies the next hop address to which to send the packet.
RTU	Remote Termination Unit. A device, such as the HotWire 5446 RTU, that is installed at the end-user site (customer premises). The RTU connects to the local loop to provide high-speed Internet or Intranet connectivity to the HotWire DSLAM.
s1b	Interface name of the card's interface to the DSLAM system backplane bus.
s1c	Interface name of a DSL card's DSL port #1.
s1d	Interface name of a DSL card's DSL port #2.
s1e	Interface name of a DSL card's DSL port #3.
s1f	Interface name of a DSL card's DSL port #4.
SNMP	Simple Network Management Protocol. A software program housed within a device to provide SNMP functionality. Each agent stores management information and responds to the manager's request for this information.
SNMP Agent	A software program housed within a device to provide SNMP functionality. Each agent stores management information and responds to the manager's request for this information.
SNMP Trap	A notification message to the SNMP manager when an unusual event occurs on a network device, such as a reinitialization.
Static Route	A permanent entry into the routing table that is manually entered. Static routes take precedence over routes chosen by dynamic routing protocols.
Subnet Address Mask	A bit mask used to select bits from an IP address for subnet addressing. The mask is 32 bits long and selects the network portion of the IP address and one or more bits of the local portion. This allows a subnet to be identified so that an IP address can be shared on a LAN.
TCP	Transmission Control Protocol. An Internet standard transport layer protocol defined in STD 7, RFC 793. It is connection-oriented and stream-oriented.
TCP/IP	Transmission Control Protocol/Internet Protocol. The dominant protocol in the worldwide Internet, TCP allows a process on one machine to send data to a process on another machine using the IP protocol. TCP can be used as a full-duplex or one-way simplex connection.
Telnet	A simple remote terminal protocol that is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. Telnet allows the user of one host computer to log into a remote host computer, and interact as a normal terminal user for that host.
Terminal Emulation	Software that allows a session to work as if it was running a specific type of terminal; e.g., VT100 or 3270 to logically connect your terminal to a mainframe computer.
TFTP	Trivial File Transfer application. A standard TCP/IP protocol that allows simple file transfer to and from a remote system without directory or file listing.
TraceRoute	A program that prints the path to a destination. It is a superset of the Ping utility used to evaluate the hops taken from one end of a link to another.
Upstream	In extended networks, the direction in which diagnostic messages flow from the final tributary diagnostic modem to the intermediate links to the diagnostic control site.
XTACACS	See Authentication Server.

Index

Numbers

A

C

D

E

G

H

I

L

M

N

O

P

R

S

T

U

W