HOTWIRE® 8540 AND 8546 RADSL CARDS

USER'S GUIDE

Document No. 8000-A2-GB20-50

April 2000

PARADYNE®

Notice

Warranty, Sales, Service, and Training Information

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

- **Internet:** Visit the Paradyne World Wide Web site at **www.paradyne.com**. (Be sure to register your warranty there. Select *Service & Support* → *Warranty Registration*.)
- **Telephone:** Call our automated system to receive current information by fax or to speak with a company representative.
  - — Within the U.S.A., call 1-800-870-2221
  - — Outside the U.S.A., call 1-727-530-2340

Trademarks

Document Feedback

We welcome your comments and suggestions about this document. Please mail them to Technical Publications, Paradyne Corporation, 8545 126th Ave. N., Largo, FL 33773, or send e-mail to **userdoc@paradyne.com**. Include the number and title of this document in your correspondence. Please include your name and phone number if you are willing to provide additional clarification.

Printed on recycled paper

Contents

3 RADSL Card Configuration

4 Monitoring the Hotwire DSL System

5 Diagnostics and Troubleshooting

A Download Code

B SNMP Traps

C 5446 RTU Setup

Glossary

Index

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. Specifically, this document addresses the use of the following cards in the DSLAM:

- 8540 Rate Adaptive Digital Subscriber Line (RADSL) card.
- 8546 Rate Adaptive Digital Subscriber Line (RADSL) card.

This document 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 forwarding (also referred to as IP routing)

It is also assumed that you have already installed either the Hotwire 8600/8610, 8800/8810 DSLAM, or 8820 GranDSLAM. If you have not done so already, refer to the appropriate Hotwire DSLAM or GranDSLAM installation document 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 Network Configuration Guide provides introductory information about the Hotwire DSLAM network model and theories. It is also recommended that you read the *Hotwire Management Communications Controller (MCC) Card User's Guide*.

Document Summary

Section	Description
Chapter 1	*Hotwire DSL System Description.* Provides an overview of the Hotwire DSLAM and GranDSLAM 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	*RADSL Card Configuration.* Describes the optional procedures for configuring the DSL cards on the Hotwire system.
Chapter 4	*Monitoring the Hotwire DSL System.* Describes operator programs that monitor the Hotwire system.
Chapter 5	*Diagnostics and Troubleshooting.* Describes common Hotwire operational problems and solutions.
Appendix A	*Download Code.* Describes how to work with the Download Code and Apply Download menus.
Appendix B	*SNMP Traps.* Describes the traps that are generated by the Hotwire system.
Appendix C	*5446 RTU Setup*. Describes MIB details including the Injection MIB and other enterprise MIBs.
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*
5038-A2-GN10	*Hotwire 5038 Distributed POTS Splitter Installation Instructions*
5216-A2-GN10	*Hotwire 5216 RTU Customer Premises Installation Instructions*
5246-A2-GN10	*Hotwire 5246 RTU Customer Premises Installation Instructions*
5446-A2-GN10	*Hotwire 5446 RTU Customer Premises Installation Instructions*

Document Number	Document Title
7700-A2-GB23	*OpenLane DCE Manager for HP OpenView for Windows User's Guide*
7800-A2-GB26	*OpenLane DCE Manager User's Guide*
7800-A2-GB28	*OpenLane Performance Wizard User's Guide*
8000-A2-GB21	*Hotwire 8540 and 8546 RADSL Cards Network Configuration Guide*
8000-A2-GB25	*Hotwire 8100/8200 Interworking Packet Concentrator (IPC) Network Configuration Guide*
8000-A2-GB29	*Hotwire Management Communications Controller (MCC) Card User's Guide*
8000-A2-GB90	*Hotwire 8100/8200 Internetworking Packet Concentrator (IPC) User's Guide* (Feature No. 8200-M2-901)
8000-A2-GN11	*Hotwire Management Communications Controller (MCC) Card Installation Instructions*
8540-A2-GN10	*Hotwire 8540 RADSL Card Installations Instructions*
8546-A2-GN10	*Hotwire 8546 RADSL Card Installation Instructions*
8600-A2-GN20	*Hotwire 8600 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide*
8610-A2-GN10	*Hotwire 8610 DSLAM Installation Instructions*
8800-A2-GN21	*Hotwire 8800 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide*
8810-A2-GN11	*Hotwire 8810 DSLAM Installation Instructions*
8820-A2-GN20	*Hotwire 8820 GranDSLAM Installation Guide*

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

Paradyne documents are also available on the World Wide Web at **www.paradyne.com**. Select *Library* → *Technical Manuals*

Hotwire DSL System Description

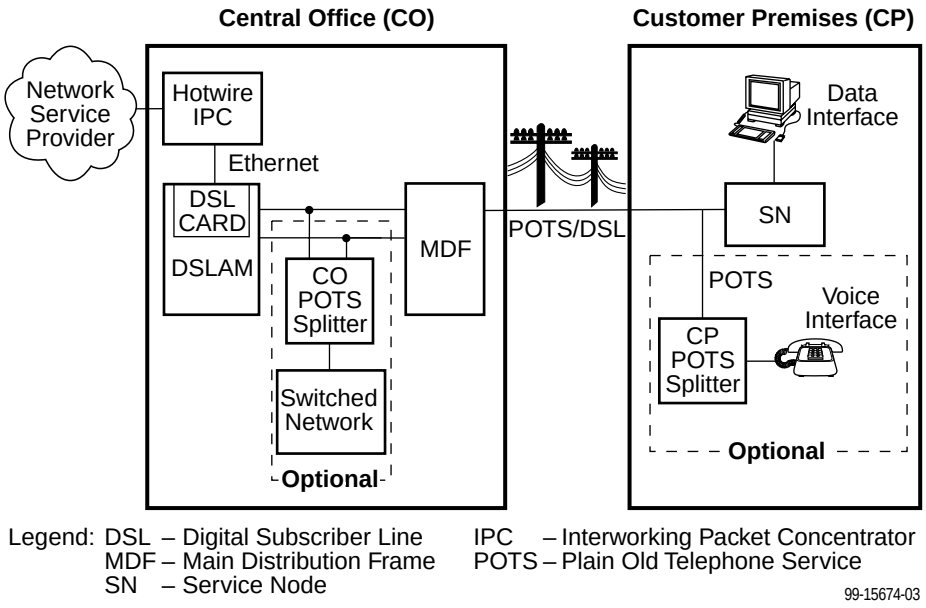
1

What is the Hotwire DSL System?

The Hotwire® Digital Subscriber Line (DSL) system is a set of central site products that terminate and consolidate packet data traffic from many customers in a serving area. The DSL card(s) then forwards the traffic to one or more network access provider networks.

High-speed Internet and intranet access is bridged on the DSL port cards and multiplexed over backbone networks. By enabling very high speeds using DSL technology and concentrating Internet Protocol (IP) traffic, greater performance is realized.

The following illustration shows a typical Hotwire configuration.



The DSL platform houses a Management Communications Controller (MCC) card and up to 18 DSL cards (for example, 8540 RADSL cards, 8546 RADSL cards, or a combination of cards). The DSL chassis 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 RADSL card interoperates with the following Hotwire RTUs:

- 5216
- 5246

The 8546 RADSL card interoperates with the following Hotwire RTU:

- 5446

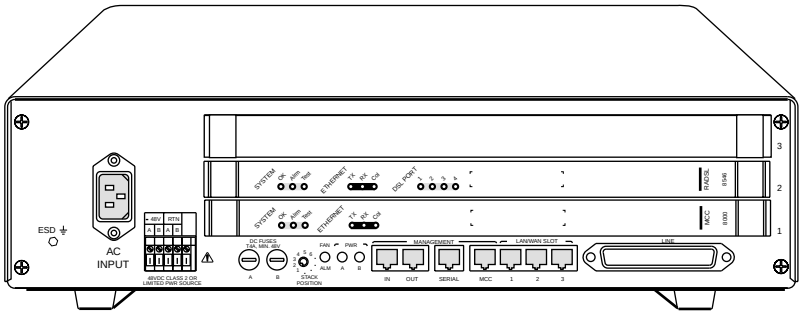
NOTE:

If you would like more information on DSL-based services, applications, and network deployment, refer to Paradyne's *DSL Sourcebook.* The book may be ordered by calling 1-800-PARADYNE or from the Paradyne website at **www.paradyne.com**.

Hotwire DSL Chassis

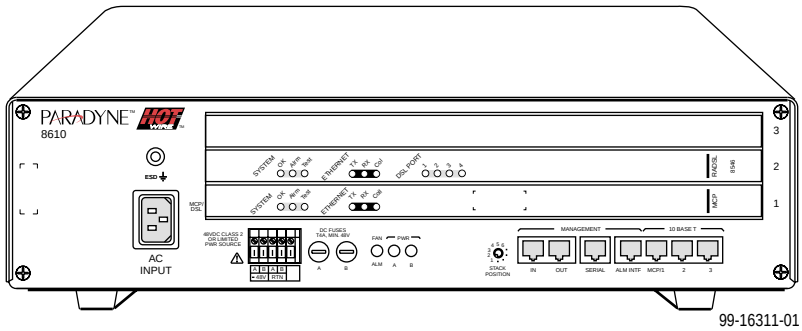
There are four types of chassis:

- The **Hotwire 8600 DSLAM** chassis is an independent, standalone system. The stackable design provides for up to six chassis to share management access through a single MCC card, which in turn, allows an additional slot for a DSL card in each of up to five additional chassis. For more information, see the *Hotwire 8600 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide*.



98-15350-02

- The **Hotwire 8610 DSLAM** chassis offers the same benefits as the 8600 chassis, with the added capability of accepting future high-density DSL cards (5–25 ports). Management access is through the MCP card. For more information, see the *Hotwire 8610 DSLAM Installation Instructions*.

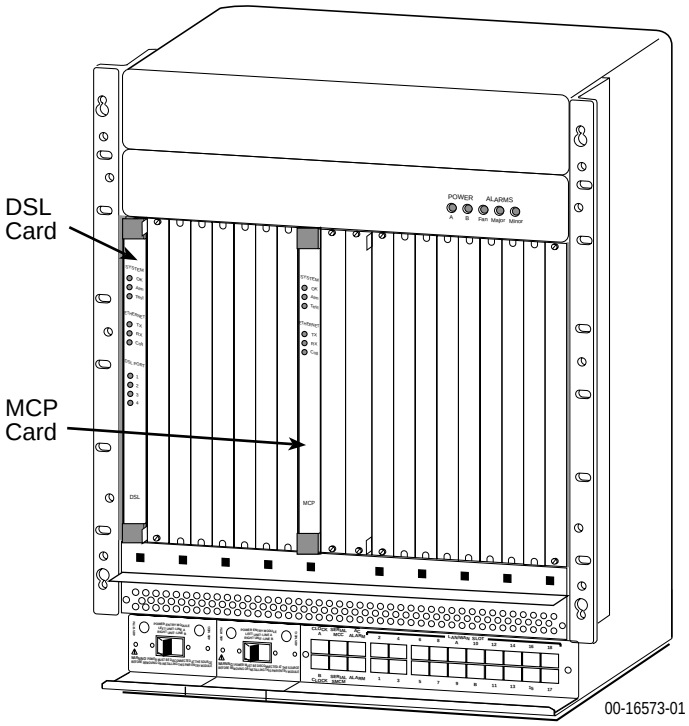


99-16311-01

In a stacked configuration, the first or base chassis must contain an MCC card for 8600 or MCP card for 8610 in Slot 1. The 8600 and 8610 chassis can be mixed in a stack. 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.

- The **Hotwire 8800 DSLAM** chassis is a 20-slot chassis designed to house up to 18 4-port DSL cards and one MCC card. (The remaining slot is reserved for the future use of a redundant MCC card.) For more information, see the *Hotwire 8800 Digital Subscriber Line Access Multiplexer (DSLAM) Installation Guide*.
- The **Hotwire 8810 DSLAM** chassis is a higher density carrier, for use with future high-density port cards, as well as lower density cards (4 ports or less). This 20-slot chassis with integral power, alarm, cooling, and interface subsystems is designed to house up to 18 DSL cards and one MCC or MCC Plus card. (The remaining slot is reserved for the future use of a redundant MCC Plus card.) For more information, see the *Hotwire 8810 DSLAM Installation Instructions*.

- The **Hotwire 8820 GranDSLAM** is a 20-slot chassis with integral power, alarm, cooling, and interface subsystems designed to house up to 17 DSL cards, as well as an SCM card for aggregating DSL traffic to an ATM uplink and an MCP card. Layer 3 systems do not use SCM card functionality. Also for Layer 3 systems, the 8820 GranDSLAM houses 8546 cards only, **not** 8540 cards. For more information, see the *Hotwire GranDSLAM Installation Guide*.



Front View of a Hotwire 8820 GranDSLAM Chassis

MCC Card

The DSLAM and GranDSLAM chassis require one MCC card, which is a processor card that administers and provides management 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 OpenLane™ 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 chassis. The following MCC cards are used in the Hotwire chassis:

Use this MCC Card . . .	In this Hotwire Chassis. . .
MCC, MCC Plus	8600, 8800, or 8810 DSLAM
MCP	8610 DSLAM or 8820 GranDSLAM

For more information, see the *Hotwire Management Communications Controller (MCC) Card User's Guide.*

NOTE:

All references to MCC cards in this document refer to the MCC, MCC Plus and MCP cards, unless specifically noted otherwise.

RADSL Cards

In addition to an MCC card, the chassis requires at least one DSL card, such as an 8540 or 8546 RADSL card. These circuit cards contain RADSL ports, an Ethernet interface to the Internet Service Provider (ISP), and a processor/packet forwarder. The processor/packet forwarder controls the endpoints and forwards the packet traffic via the Ethernet and RADSL interfaces.

When this card . . .	Fully populates this Hotwire chassis . . .	Total number of DSL ports supported is . . .
8540 or 8546 (4 ports)	8600/8610 with 5 expansion chassis	68
	8800/8810	72
8546 (4 ports)	8820	68

- **8540/8546 RADSL Cards** – Contains four ports. RADSL cards are targeted primarily for commercial environments and offer high-speed, rate-adaptive services over copper wire. Applications such as Internet access, video teleconferencing and LAN extension are supported.

Features

The Hotwire DSL system provides the following features:

- High-speed Internet or intranet access.
- Rate Adaptive Digital Subscriber Line ports.
- Subscriber authentication, 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 nondisruptive tests.

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 DSL Cards

The Hotwire DSL software provides DSL configuration options to:

- Configure the 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 DSL and RTU 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 Chapter 3, *RADSL Card Configuration*.

Monitoring the DSL Cards

The Hotwire DSLAM software provides submenu options to monitor the activity of the Hotwire 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 4, *Monitoring the Hotwire DSL System*.

Troubleshooting and Diagnostics

The Hotwire DSL system provides DSL diagnostic submenu options that:

- Perform PING tests and display results
- Perform a BERT test
- Display selftest results for CPU, memories, and ports
- Show major alarms such as Selftest Failure, Processor Failure, and DSL or Ethernet port failure
- Show minor alarms such as Config Error and thresholds exceeded for DSL Margin and Error Rate or Link Down events
- 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 nondisruptive tests as a user with Operator permission.

For more information about troubleshooting and diagnostics, see Chapter 5, *Diagnostics and Troubleshooting*.

Hotwire Menus and Screens

2

Menu and Screen Formats

The Hotwire DSL System has an ASCII-based menu- and screen-driven user interface system that enables the user to configure and monitor the Hotwire cards. This section describes the components of a typical Hotwire menu and screen.

Components of a Hotwire Menu

A typical Hotwire menu format is shown below:

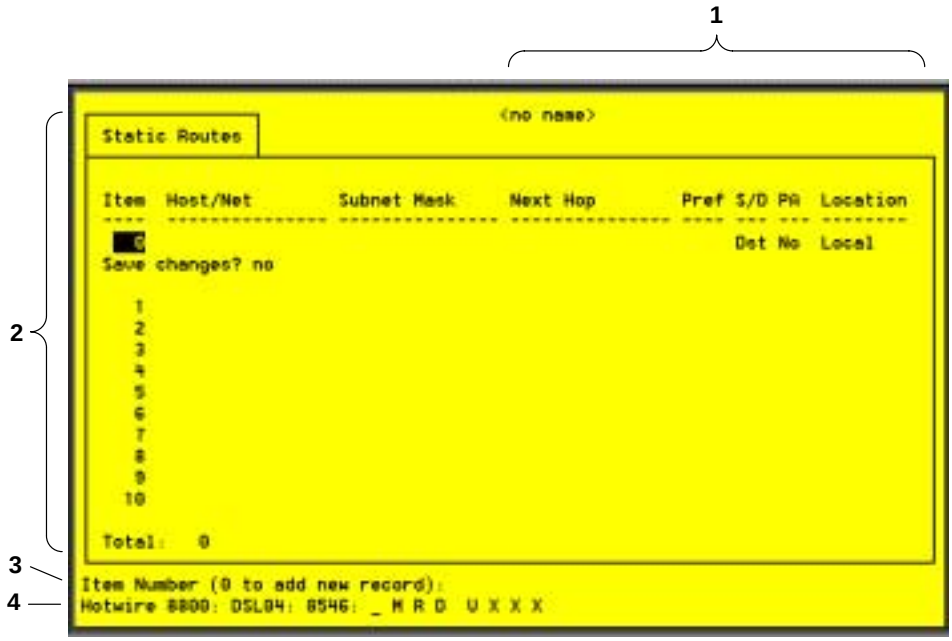
1. **Menu Title** is the top line of the menu window that displays the title of the menu or submenu.
2. **Menu List** is the portion of the menu window that displays the list of menu options. When selected, a menu option displays a submenu window or screen.
3. **Letter Navigation Keys** are provided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

   For example, from the Hotwire – DSL 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 **A** key to select the Card Status menu item. This action displays the Card Status menu. (You can also use the arrow keys on your keyboard to select a menu item. See *Commonly Used Navigation Keys* on page 2-4 for more information.)

   To back up one menu level, press Ctrl-z. To go to the Main Menu, 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 two 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 DSL user interface will display **<no name>**.

   — The second 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**.

2. **Display Area** is the top portion of the screen on which pertinent DSL 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 #3 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 Static Routes screen above, the Item Number field is highlighted. If you want to add a new record, you must enter **0** at the item number **(0 to add new record):** 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 8610: DSL01: 8546: __ M __ D XXXX`

   The first field indicates the chassis type. In this case, the system in use is the Hotwire 8610 DSLAM system. The second field indicates the card selected. In this example, the DSL01 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 2-11.

Commonly Used Navigation Keys

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

Keys	Definition
Backspace, Del, Ctrl-d	Erases the character to the left of the prompt.
Ctrl-c	Moves to top of current menu.
Ctrl-e	Returns to the Card Selection screen from any screen.
Ctrl-r	Resets counters (on monitoring statistics displays).
Ctrl-u	Clears the current input or prompt line.
Ctrl-v	Displays pop-up menus.
Esc h, ?	Displays the online Help screen.
Esc l, Ctrl-l	Refreshes the screen.
Esc n	Goes to the next window.
Esc p, Ctrl-z	Goes back to the previous window.
Esc t, Ctrl-a, Ctrl-t, or Ctrl-y	Goes back to the original, top-level window.
Left arrow, Ctrl-b	Moves the cursor to the left.
Right arrow, Ctrl-f	Moves the cursor to the right.
Up arrow, Ctrl-p	Moves up to the previous menu selection or entry field.
Down arrow, Ctrl-n	Moves down or to the next selection.
Enter or Return	Accepts entry.

Levels of Access

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

- **Administrator**. The Administrator has complete read/write access to the DSL system. With Administrator permission, you can set specific parameters and variables to configure cards, ports, interfaces, and endpoint selection.
- **Operator.** The Operator has read-only access and can view configuration information and monitor performance but has no configuration menu access or modification permission.

The default access is no login and password with Administrator status. To provide login security to the DSL system, user accounts must be configured.

NOTE:

There must be at least one Administrator configured in order to have system security.

For information on configuring user accounts, see the *Hotwire Management Communications Controller (MCC) Card User's Guide.*

User Login Screen

You can log in to the Hotwire DSL system using either a local VT100- compatible terminal or a remote Telnet connection. However, each card in the Hotwire DSL system accepts only one login session at a time.

NOTE:

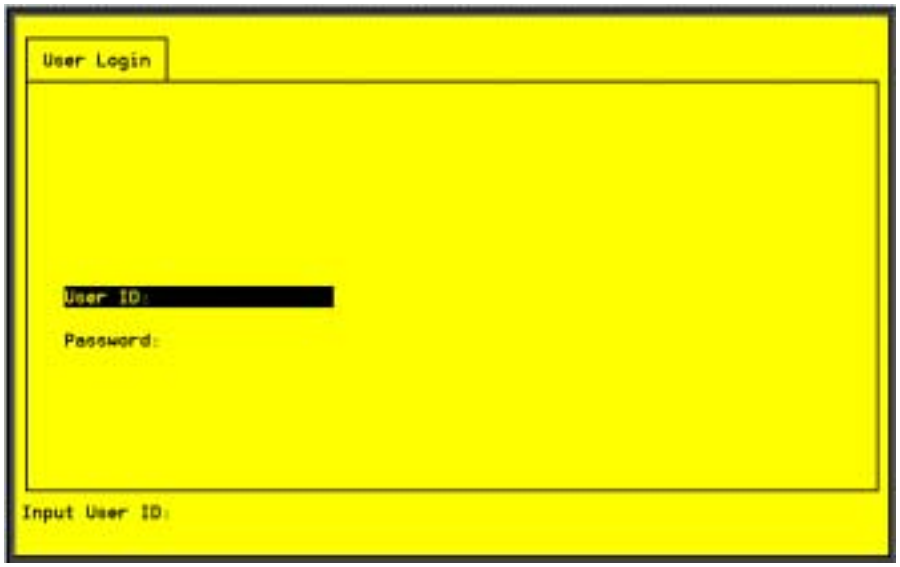
The User Login screen only appears if one or more users have been defined on the MCC.

At the User Login screen, enter your login ID and password. You must wait until your login is verified, anywhere from two seconds to 12 minutes. If you have RADIUS Authentication, this verification takes some time while each RADIUS server is contacted one at a time.

If you are denied access during a Telnet session, the session stops and an error is logged. If you are using a console, return to the User Login screen.

NOTE:

If you forget your password, contact our Technical Service Center. Have the serial number of the MCC card available, and the service representative will provide you with a password.



The user ID and password are case-sensitive; that is, the system recognizes both upper- and lowercase letters. For example, if you enter your user name and password information in uppercase letters and your assigned user name and password are in upper- and lowercase letters, the system will not let you log in. User ID and password are limited to a maximum of 15 characters. Any user account with a user ID or password exceeding 15 characters is treated as invalid by the MCC.

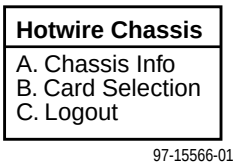
After entering your user ID and password, the system displays the Hotwire Chassis Main Menu.

Hotwire Menu Hierarchy

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.
- **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 (Hotwire – DSL menu).

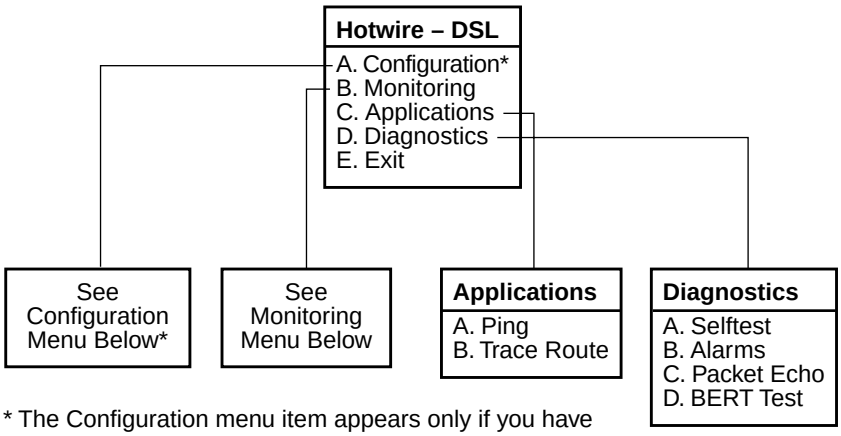
  For more information, see *Card Selection Screen* on page 2-11.
- **C. Logout** to exit from the current Hotwire DSL login session.

  For more information, see *Exiting From the System* on page 2-13.

For information on the MCC card, see the *Hotwire Management Communications Controller (MCC) Card User's Guide.*

Hotwire – DSL Menu

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

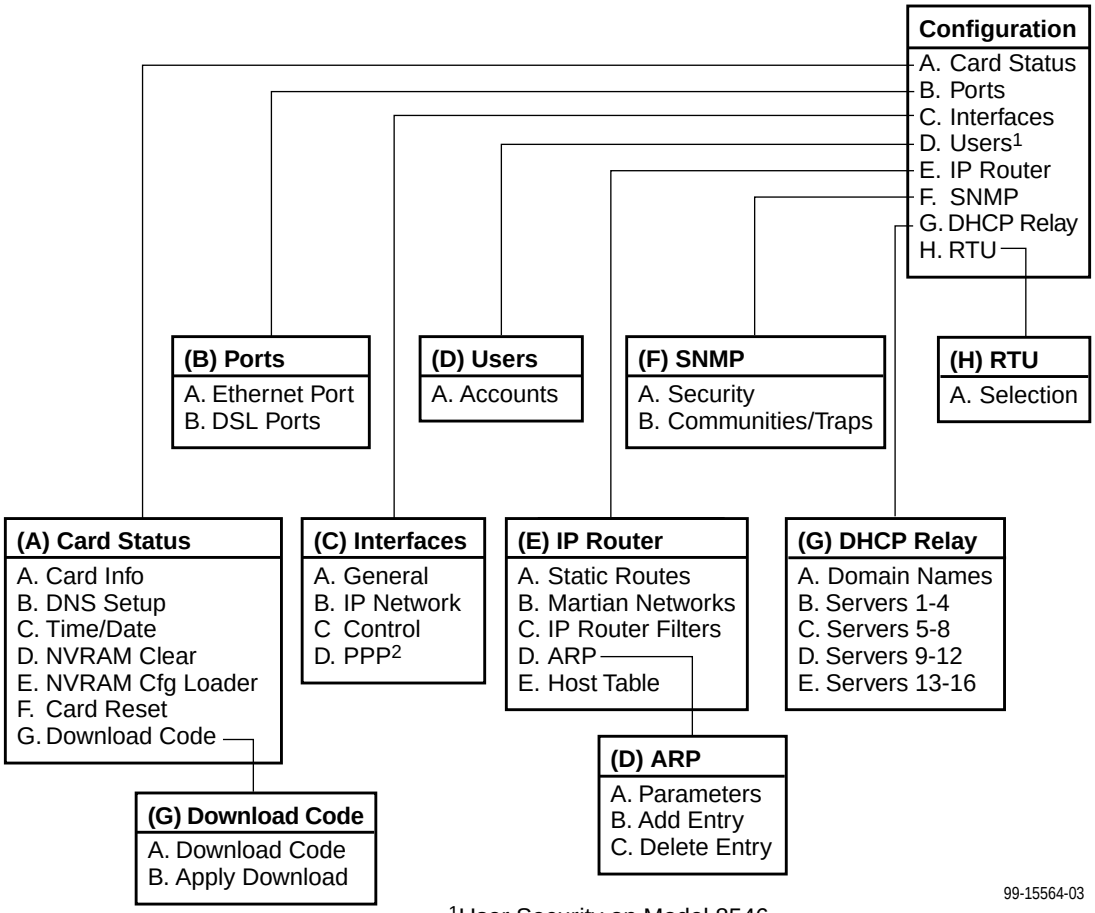


* The Configuration menu item appears only if you have Administrator permission.

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

DSL Card Configuration Menu

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



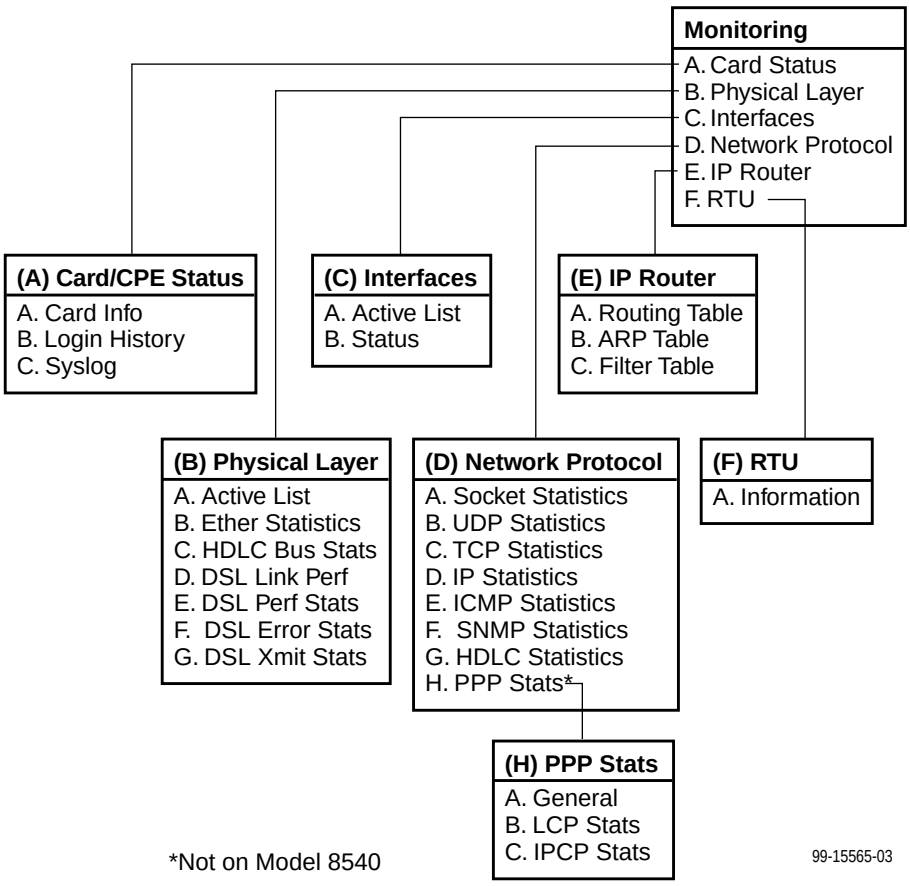
[1]User Security on Model 8546
[2]Not on Model 8540

NOTE:

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

DSL Card Monitoring Menu

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



Logging In to the System

This section describes how to log in to the Hotwire DSL system after the system has been configured.

NOTE:

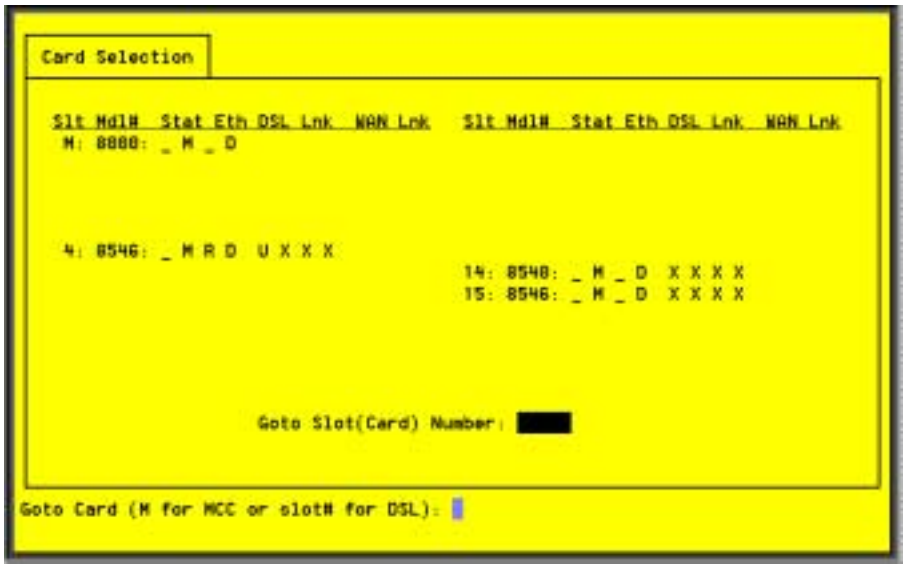
When you power on the system for the first time, the system displays the Who Am I screen. This screen can be accessed only from the local console.

Card Selection Screen

From the Hotwire Chassis Main Menu, select Card Selection to display the status of any of the 18 DSL cards installed in the 8800/8810 chassis (or 17 DSL cards installed in the 8820 GranDSLAM chassis) by type and slot number. The Card Selection screen also displays general and interface status for each card.

NOTE:

The Card Selection screen for the Hotwire 8600/8610 chassis displays the same information, but the slot order is different.



The status of each DSL card is indicated by codes being displayed in any of eight positions to the right of the card selected.

NOTE:

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

Column Heading	Position	Display	Description
Slt	<slot number>		M = MCC, MCP or MCC Plus card 1–18 = slot number for DSL card
Mdl #	<card type>		First four digits of the card model number: 8540 = 8540 RADSL card 8546 = 8546 RADSL card 8000 = MCC/MCP/MCC Plus card
Stat	1	T or _	Test mode. Card currently in test mode or _ for no active test.
	2	M or _	Major alarm. Major alarm present on card or _ for no active major alarm.
	3	R or _	Minor alarm. Minor alarm present on card or _ for no minor alarm active.
Eth	4	U, D, or X	Status of Ethernet link: U=Up, D=Down, X=Disabled
8546 (DSL card)	5 and up	U, D, X, or H	Status of DSL card Port 1–4 link: U=Up, D=Down, X=Disabled, or H=Handshaking
WAN Lnk	For M/SDSL and M/HDSL cards.		

For example, if you select DSL card in Slot 4, the following may be displayed:

```
    4: 8546  _ M R D  U X X X
Position:    1 2 3 4  5 6 7 8
```

This display shows the following:

- There is an 8546 card in Slot 4
- Position 1 – no current test (_)
- Position 2 – major alarm is present (M)
- Position 3 – minor alarm is present (R)
- Position 4 – Ethernet link is down (D)
- Position 5 – DSL port 1 is up (U)
- Positions 6, 7 and 8 – DSL ports 2, 3 and 4 are disabled (X)

On the Card Selection screen, there is a prompt used to select a specific card in the DSL chassis. When a DSL slot number is entered, you are connected to the DSL card you selected.

For more information about the status displayed on this screen, such as major and minor alarms, see *Troubleshooting* in Chapter 5, *Diagnostics and Troubleshooting*.

Accessing the Hotwire – DSL Menu

▶ 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 2-11 for more information.)

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

   The Hotwire – DSL menu appears.

Exiting From the System

You can manually log out of the system or the system will automatically log you out.

Manually Logging Out

▶ Procedure

To exit from the Hotwire DSL system:

1. Return to the Card Selection screen by selecting Exit from either the Hotwire – MCC menu or the Hotwire – DSL menu.

2. Press Ctrl-z.

3. From the Hotwire Chassis Main Menu, select Logout.

   The system exits from the current Hotwire DSL login session.

Automatically Logging Out

The DSL system has an automatic timeout feature that logs you out of the system after five minutes (on MCC) or ten minutes (on DSL port card) of inactivity. You will need to log back in to continue your work.

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

RADSL Card Configuration

3

Overview

This chapter describes configuration options on the 8540/8546 RADSL cards. Use these options to customize your applications. For information on customizing the MCC card, see the *Hotwire Management Communications Controller (MCC) Card User's Guide.*

NOTE:

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

Port Naming Conventions

The following are the naming conventions used for the Hotwire DSL 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 DSL system backplane bus.
- **s1c**, **s1d**, **s1e**, and **s1f** – Interface names of the four DSL ports on a RADSL card.

NOTE:

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

Configuring the MCC Card, DSL Cards, and RTUs

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

NOTE:

It is assumed that you have read the *Hotwire 8540 and 8546 RADSL Cards Network Configuration Guide* and have assigned service and management domain IP addresses for all devices (MCC, DSL, and RTUs).

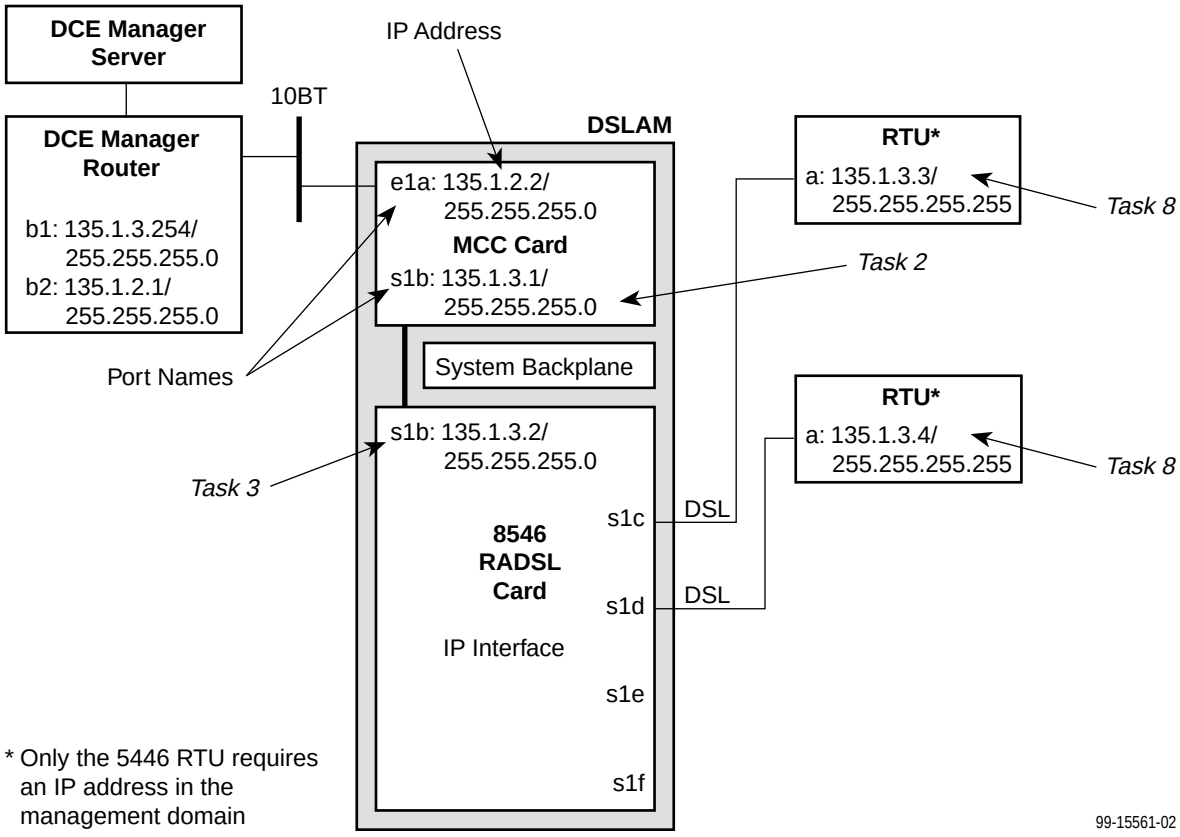
The following tables list the basic steps you need to do to configure the MCC cards, DSL cards, and RTUs.

For the Management Domain, perform task . . .	**On the . . .**	**See the . . .**
1. Configure time and date.	MCC	*Hotwire Management Communications Controller (MCC) Card User's Guide*
2. Assign the IP address to the backplane on the MCC card.	MCC	
3. Assign the IP addresses to the DSL cards.	MCC	
4. Create SNMP Community Strings and Authentication Failure Trap.	MCC	
5. Create default route.	MCC	
6. Reset the MCC card.	MCC	
7. Select a DSL card to configure.	DSL	*Card Selection Screen in Chapter 2, Hotwire Menus and Screens*.
8. Configure 5446 RTU IP host address for the 8546 RADSL card. (Not applicable to 8540 RADSL card.)	DSL	*DSL Card Configuration Interfaces Screens,* page 3-15 (**A-C-B**).

For each Service Domain, perform task . . .	**On the . . .**	**See . . .**
1. Configure a static route to the NMS.	DSL	*DSL Configuration IP Router Screens*, page 3-20 (**A-E-A**).
2. Assign IP addresses to the DSL card LAN.	DSL	*DSL Card Configuration Interfaces Screens,* page 3-15 (**A-C-B**).
3. Reset the DSL card.	DSL	*DSL Configuration Card Status Screens*, page 3-7 (**A-A-F**).
4. Create DHCP Relay Agent.	DSL	*Configuring DHCP Relay Agent (dynamic addressing)*, page 3-29 (**A-G**).
5. Create default route or source route on DSL.	DSL	*DSL Configuration IP Router Screens*, page 3-20 (**A-E-A**).
6. Create SNMP Community Strings and Authentication Failure Trap.	DSL	*DSL Configuration SNMP Screens*, page 3-26 (**A-F-B**).
7. Configure RTU Information	DSL	*DSL Configuration RTU Screens*, page 3-31 (**A-H-A**).

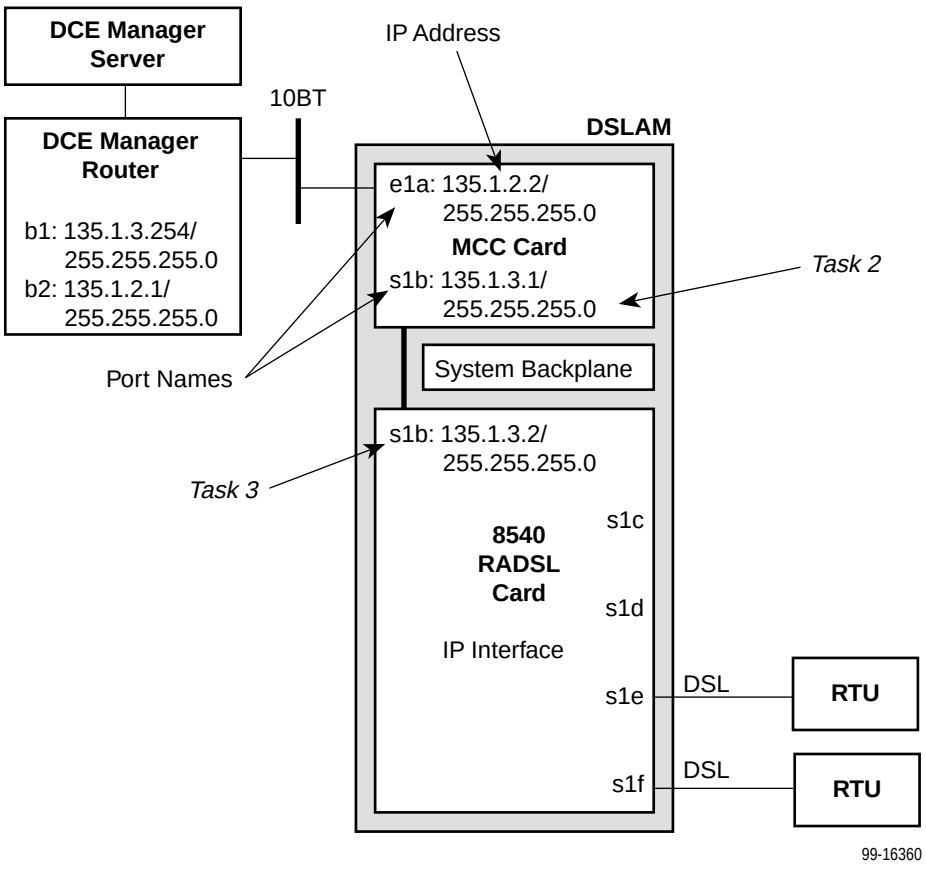
The following illustrates the management domain components that must be configured and examples of the various naming conventions for the 8546 card. Tasks refer to those listed in the table on page 3-2.

MANAGEMENT DOMAIN

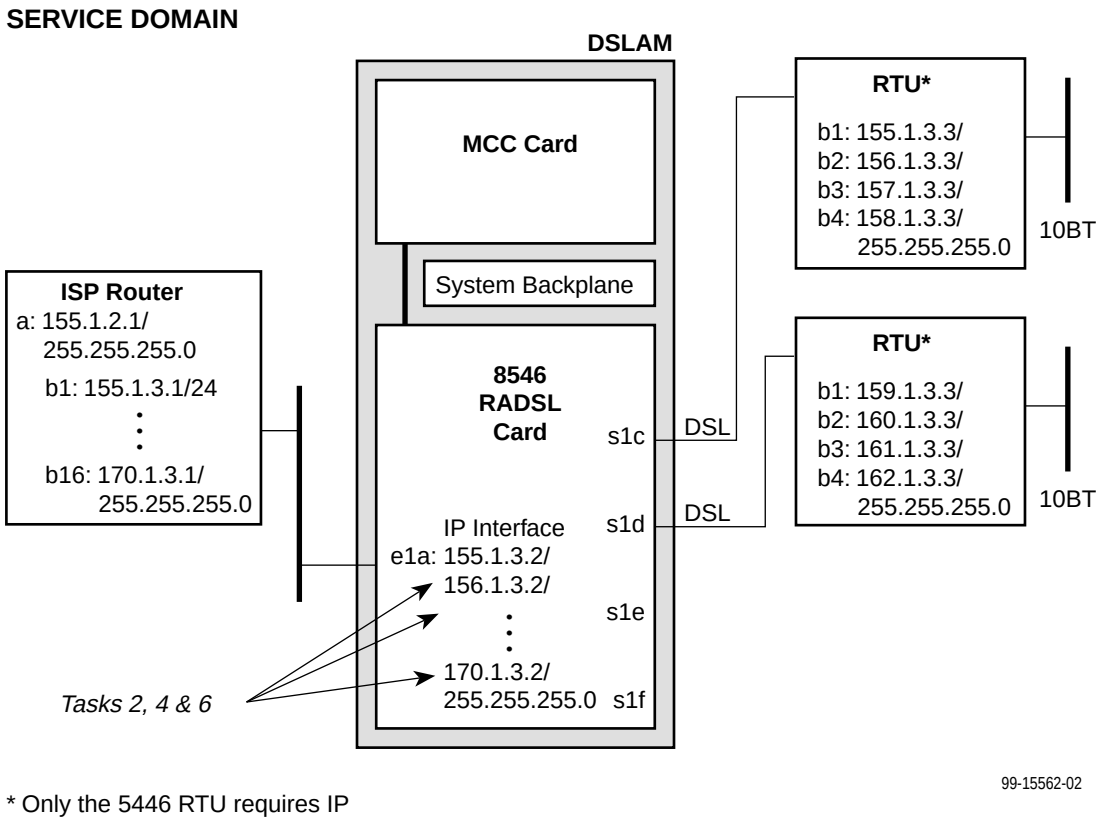


The following illustrates the management domain components that must be configured and examples of the various naming conventions for the 8540 card. Tasks refer to those listed in the table on page 3-2.

MANAGEMENT DOMAIN

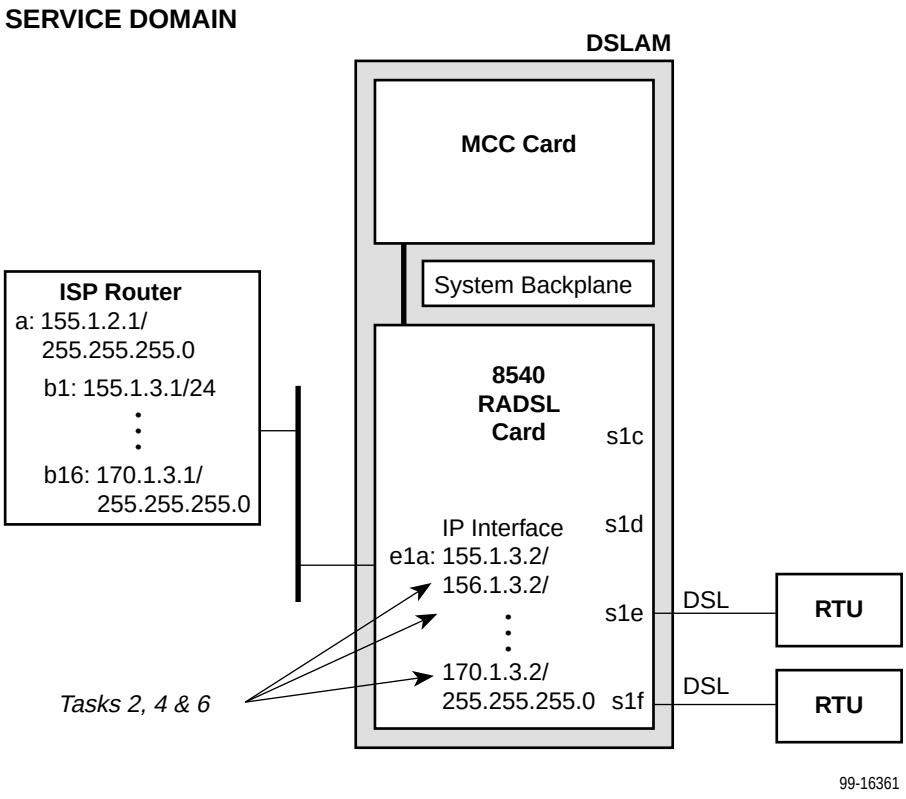


The following illustrates the service domain components that must be configured and examples of the various naming conventions for the 8546 card. Tasks refer to those listed in the table on page 3-2.



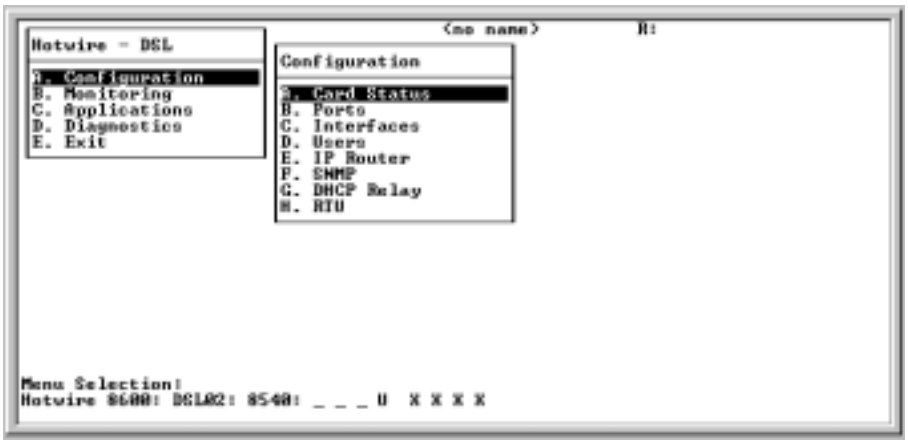
* Only the 5446 RTU requires IP addresses in the service domain

The following illustrates the service domain components that must be configured and examples of the various naming conventions for the 8540 card. Tasks refer to those listed in the table on page 3-2.



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 DSL system with Administrator permission can configure the DSL card.

▶ Procedure

To configure card information, DNS setup, time/date, clear NVRAM, upload or download configuration sets, 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 3-1 and press Enter.

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

Card Info (System Information)	**A-A-A**
Allows you to configure basic card-level information. **Card Name** – 16 alphanumeric characters. Name assigned to the card. **Card Contact** – 32 alphanumeric characters. Name or number of party responsible for card. **Card 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** – Either Standard (for USA keyboards) or Extended (for European keyboards). (Default = Standard). **Remote Control Terminal Port Mode** – Either Standard (for USA keyboards) or Extended (for European keyboards). (Default = Standard). **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** – Enter the primary Domain Name System Server address in *nnn.nnn.nnn.nnn* format (up to three). **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)?** – 1–300 seconds (Default = 5). Enter the time to wait for a response. **Number of times to retry server** – 1–10 times (Default = 5). Enter the number of times to retry the server.	

Table 3-1. 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 8540 RADSL card with network time and to synchronize the DSL system's clock via a Network Time Protocol (NTP) server. On the 8546 card, displays the time zone, local time, and date on the DSL card as received from the MCC card. 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. **Time zone** – Name of the system's time zone (Default = GMT). See the Help for a list of time zones. **Local Time/Date** – Time in *hh.mm* format (am or pm). Enter the date in *mm/dd/yy* format. **Client NTP Mode** – Broadcast/Unicast (Default = Broadcast). For the 8540 card, select the Client Network Time Protocol (NTP) Mode. **NTP Server** – *nnn.nnn.nnn.nnn* format. For the 8540 card, enter the NTP Server IP address. May be left blank since card will automatically synchronize with the MCC card, which should have the NTP server address. **Synchronized(hrs)** – 1–24 (Default = 1). For the 8540 card, enter the hours between synchronization.	
NVRAM Clear Screen (Clear NVRAM)	**A-A-D**
Clears 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 3-1. Card Status Options (3 of 4)

NVRAM Config Loader	**A-A-E**
Provides 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** – IP host name or address in *nnn.nnn.nnn.nnn* format. **TFTP Transfer Direction** – Upload-to-Server/Download-to-Server (Default = Upload-to-Server). Select Upload-to-Server to store a copy of the card's configuration on the server. Select Download-to-Server 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. **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 upload or download transfer.	
Card Reset (Reset System)	**A-A-F**
Resets the card. This resets all counters and if a new configuration or software version has been downloaded, the new code will then become active. Verify that the LEDs on the DSL card go through the reset sequence once, and then a second time after approximately 10 seconds (BOOTP). NOTE: This action disrupts the data flow for at least 30 seconds.	

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

Download Code (Download Code and Apply Download)	**A-A-G**
Provides the ability to download a new version of code and apply the downloaded code. For further information on this feature, see Appendix A, *Download Code*. Select **Download Code (A)** or **Apply Download (B)**. You must exit this screen and use the Apply Download screen.	
Download Code	**A**
Allows code download. 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 filenames must follow the 8.3 naming convention imposed by DOS. **TFTP Server IP Address** – IP host name or address in *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 (**A-A-G-B**) for the download to take effect.	
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 A, *Download Code*. NOTE: This option does not apply if the download to the DSL card was initiated from the MCC. Also, 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 as shown in Table 3-2 and press Enter.

Table 3-2. Ports Options (1 of 3)

Ethernet Port	**A-B-A**
Allows you to configure the Ethernet Port for full or half-duplex mode. **Port Name** – Enter the port name (up to 7 characters). **Full Duplex** – Enable for Full Duplex mode, Disable for half duplex mode (Default = Disable). **Action** – Edit/Reset. Select Reset to have changes become active.	

Table 3-2. Ports Options (2 of 3)

DSL Ports (DSL Parameters)	A-B-B
Allows configuration of the operational and alarm parameters of the DSL ports. Each DSL port is configured separately. **Action** – Edit to configure the DSL ports. Reset the port to make changes active. **Port #** – Enter port 1 to 4 (Default = 0). **RTU Type** – Model number of the service node. For Model 8540, selections are 5246/5216 (Default = 5216). For Model 8546, selections are 5446r1/5446r2 (Default = 5446r2). (This field is read-only.) **Port Desc** – Enter port description, such as user name, etc. (40 characters maximum). **Tx Power** – 0 dB, –3 dB, –6 dB. For the RADSL card. Enter the rate that allows you to reduce the transmit power by: –3 dB or –6 dB (Default = 0 dB). Short loops require less power, reducing crosstalk and giving better performance on longer loops in the same cable bundle. **RTU Tx Power** – 0 dB, –3 dB, –6 dB, –9dB. From the RTU. Enter the rate that allows you to reduce the transmit power by: –3 dB or –6 dB (Default = –6 dB). **Startup Margin** – The Startup Margin (SM) 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 3 dB, the speed will increase. Enter –3 to 9 (Default = 3). **Reed-Solomon Interleaving** – Long/Short (Default = Long). **Behavior** – Fixed/Adaptive (Default = Adaptive). In fixed rate mode, the DSL port will operate at the specified upstream and downstream 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. **Fixed: Dn Speed*** – 7168/6272/5120/4480/3200/2688/2560/2240/1920/1600/1280/1024/960/896/768/640/512/384/256 (Default = 2560 kbps). **Fixed: Up Speed*** – 1088/952/816/680/544/476/408/340/272/204/136/119/102/90.6/85/68/51/45.3/34/11.3 (Default = 1088 kbps). Enter the fixed upstream speed. **Adaptive: Max Dn Speed*** – 7168/6272/5120/4480/3200/2688/2560/2240/1920/1600/1280/1024/960/896/768/640/512/384/256 (Default = 7168 kbps). Enter the maximum downstream speed.	
* If you select a downstream speed of 2560 or higher, your upstream speed selection is limited to 1088/952/680/408 kbps.	

Table 3-2. Ports Options (3 of 3)

DSL Ports (DSL Parameters) *(cont'd)*	**A-B-B**
Adaptive: Max Up Speed* – 1088/952/816/680/544/476/408/340/272/204/136/119/102/90.6/85/68/51/45.3/34/11.3 (Default = 1088 kbps). Enter the maximum upstream speed.	
Thresholds for Trap Messages:	
Adaptive: Min Dn Speed* – 7168/6272/5120/4480/3200/2688/2560/2240/1920/1600/1280/1024/960/896/768/640/512/384/256 or d for Disable (Default = 256). Enter the thresholds to cause traps to occur. This field will not display if Behavior is set to Fixed.	
Adaptive: Min Up Speed* – 1088/952/816/680/544/476/408/340/272/204/136/119/102/90.6/85/68/51/45.3/34/11.3 or d for Disable (Default = 11.3). Enter the minimum upstream speed. This field will not display if Behavior is set to Fixed.	
Margin Threshold: – In Fixed mode, sends a trap message if the margin falls below the selected Margin Offset value. Enter a value for the margin threshold trap (–5 dB to +10 dB, or D to Disable). (Default = +3). In Adaptive mode, the value entered is relative to the startup margin. For example, with a startup margin of +3 dB and a threshold offset of +3 dB, the Low Margin Trap will be sent if the margin falls below 0 dB.	
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, or D to Disable). (Default = 0.)	
NOTE: If you have made changes, exit the screen, then save. The changes are then activated. You can only save changes on one port at a time.	
* If you select a downstream speed of 2560 or higher, your upstream speed selection is limited to 1088/952/680/408 kbps.	

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 3-3 and press Enter.

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

General (Interfaces)	**A-C-A**
Provides the capability of configuring and viewing basic card interface information about a given interface. **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 prepopulated 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 for your network. Do a card reset or reset the Ethernet interface.	

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

IP Network	**A-C-B**
Allows you to configure up to 16 IP addresses for a port. Configure one IP address for each service domain on the DSL card. **IP Interface** – Name of the interface. Enter up to 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. (Blank to disable filtering.) Prevents unwanted packets from entering the RADSL card through a specified interface. **Output Filter** – Optional. (Blank to disable filtering.) Prevents unwanted packets from going out of the RADSL card through a specified interface. **Source Routing** – Directs data to the correct address. Set to enable for networks with multiple ISPs. Leave blank to disable filtering. If you disable source routing for an interface, any existing source route for that interface is removed from the active routing table. Source routing should be disabled on the e1a interface for most installations. Use care when enabling source routing on the e1a interface as it can create routing loops. (Default = Disable for e1a interface or Enable for s1*x* interface). **Peer IP Address** – *nnn.nnn.nnn.nnn* format. IP address associated with the other end of the link; i.e., the 5446 RTU. This field does not appear if the card is an 8540 or if e1a is the IP interface name. **Route to Peer** – Net or Host. Must be Net for s1b. Routing method used to get to peer (i.e., host or net). This field does not appear if the card is an 8540 or if e1a is the IP interface name. 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.	

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

PPP	A-C-D
Allows configuration of 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 prepopulated, the values can be changed.	

DSL Configuration Users Screens

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

User accounts provide security for the DSL system by requiring that anyone who is trying to log on to the system has a valid password to gain access.

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 RADSL 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.

For information on setting up user accounts on the MCC card, see *Hotwire Management Communications Controller (MCC) Card User's Guide.*

▶ Procedure

To configure RADSL user accounts (if Telneting directly to the RADSL card) (for Model 8540 only):

1. Follow this menu sequence from the DSL Main Menu:

   Configuration →*Users*→*Accounts* (**A-D-A**)

2. The Accounts screen appears. Enter the desired values in the fields as shown in Table 3-4.

3. Enter **Y** to save changes and press Ctrl-z to return to the Hotwire Chassis Main Menu tree.

   Press Ctrl-v to see a list of all user accounts at the **`Login id`** prompt.

4. Reboot the RADSL card after the changes have been made (**A-A-F**).

5. To verify that a RADSL card account has been set up, go to the MCC card and follow this menu sequence:

   Applications → *Telnet* (**C-B**)

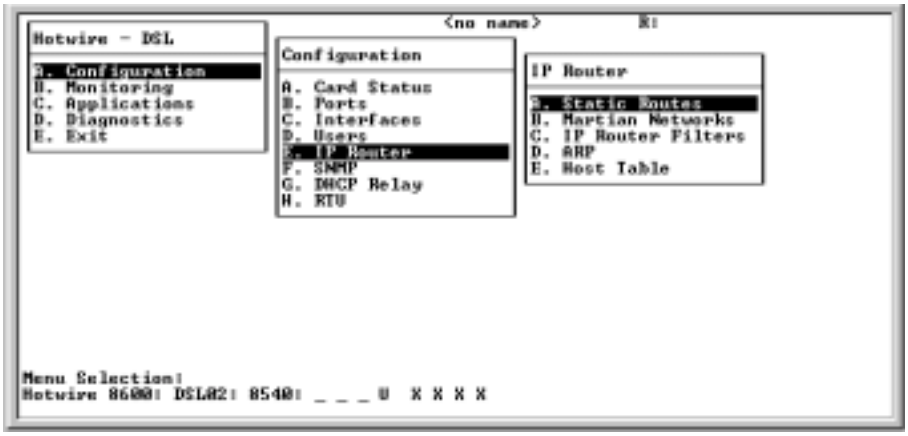
   See the *Hotwire Management Communications Controller (MCC) Card User's Guide* for more information.

Table 3-4. Users Options

Users* (Configure Account)	**A-D-A**
For Model 8540 only. Allows you 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 DSL system 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. This field is case-sensitive. **Password** – Enter the password associated with the login ID. **Repeat Password** – Reenter your password. **Privilege** – Operator/Administrator. Enter Operator for read-only access; enter Administrator for complete system access. NOTE: Press Ctrl-v to see a list of all user accounts at the login ID prompt.	
* Displays User Security for Model 8546 card, which is reserved for future use. For 8546 cards, user accounts are defined on the MCC card or on a RADIUS Authentication server, if configured on the MCC. See the *Hotwire Management Communications Controller (MCC) Card User's Guide* for more information.	

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, IP router filters, ARP and Host tables:

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 3-5 and press Enter.

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 *IP Address Allocation, IP Routing,* and *IP Filtering*, in the *Hotwire 8540 and 8546 RADSL Cards Network Configuration Guide*.

The following table lists warnings and error messages displayed on the Static Routes screen (**A-E-A**).

Message	**Meaning**
Routing Table: Route not added	Route was saved into NVRAM but not added to the active routing table.
Routing Table: Route limit reached for interface	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	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 (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 (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	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	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	Route was not saved into NVRAM and not added to the active table because the NVRAM is full.
Cannot delete a remote route	You cannot delete a remote route.
Cannot modify a remote route	You cannot modify a remote route.

Table 3-5. IP Router Options (1 of 4)

Static Routes	**A-E-A**
Allows you 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 router and downstream to those hosts that require static routes. **Item** – Press Enter on 0 field to add entry. You cannot select dynamic routes or routes identified as rmt s1*x* on the location field. The remote entries can only be modified from RTU Static Routes menu. If a static route is identified as "both s1*x,"* only the DSL (local) portion of the static route can be modified. NOTE: s1*x* = s1c, s1d, s1e, or s1f. **Host/Net** – *nnn.nnn.nnn.nnn* format or space to delete entry. Destination of the route to the NMS. This field is read-only for dynamic routes. **Subnet Mask** – Associated subnet mask for the specified destination IP address to the NMS. 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. IP address of the next hop router for the specified destination to the NMS. On Model 8540, the next hop is DSL port name s1c, s1d, s1e, or s1f. This field is read-only for dynamic routes and will be blank for those routes identified as rmt s1*x* on the location field. **Pref** – Measure of how preferable one route is to another, if you have two or more 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. Proxy ARP is only used when the RTU and the ISP router are on the same subnet. NOTE: When you define a source route, the Proxy ARP field is no longer selectable. **Location** – Shows the location of the route. – *Local* indicates that the route is a local route on the RADSL card. – *Rmt s1x* indicates that the route is a remote route on the 5446 RTU connected to interface s1*x*. (The next hop field will be blank.) – *Both s1x* indicates that the remote route is applicable to both the RADSL card and the 5446 RTU connected to the s1*x* interface. (The next hop field will display the peer IP address of the s1*x* interface.)	

Table 3-5. IP Router Options (2 of 4)

Martian Networks	**A-E-B**
Gives the user the ability to configure addresses that the system recognizes as invalid (addresses from which the RADSL card will not accept routing information). **Item** – Press Enter on 0 field to add entry, or enter the item number to change an 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 (labeled “fixed”). It is recommended that you do not remove entries. If you have made changes to this screen, you must do a card reset.	
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. **# Static Rules** – Number of static routes in filter. **# Dynamic Rules** – Number of dynamic routes in filters. **Ref Cnt** – Reference Count. Number of active interfaces using the filter. **Def 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 3-5. 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 RADSL card, a maximum of 8 filters can be configured. For additional information on IP Router filters, see *IP Filtering* in the *Hotwire 8540 and 8546 RADSL 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 filters. **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 Rule Number** – Enter the number of the rule desired as displayed in the Rule # field.	

Table 3-5. 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)** – 1–255 (Default = 3). **Default Route Entry Timeout (minutes)** – 1–20 (Default = 1). This is the time, in minutes, that a default route is to remain in the ARP table. If the default route entry times out without being referenced, an ARP request is sent to the next hop router. If no response is received, the default route entry is removed from the ARP table and the RADSL card switches to the next reachable default route with the highest preference. 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 No to exit. **Add another Entry?** – Enter Yes to add another entry or No to exit. **Delete Entry (Delete ARP Entry)(C)** Allows you 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 Enter. NOTE: For the Add and Delete ARP Entry screens, any information entered is not stored in NVRAM and will be lost when you reset the card.	
Host Table (IP Host Table)	**A-E-E**
Allows you 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. In this way, you can connect to foreign hosts by name, rather than by IP address. 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 Enter 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, community names, and trap addresses.

▶ Procedure

1. Follow this menu sequence:

   Configuration →*SNMP* (**A-F**)

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

Management System Source Validation for RADSL Cards

▶ Procedure

To set up management System source validation for RADSL cards:

1. Follow this menu sequence from the DSL Main Menu:

   Configuration → *SNMP* →*Security* (**A-F-A**)

2. Enable IP address security validation.

3. 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.

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

Table 3-6. SNMP Options

Security (SNMP Security)	**A-F-A**
Enables you to configure security for the RTU SNMP agent. CAUTION: Endpoint cookies must be kept confidential. **Endpoint Cookie** – Security string for endpoint. Enter up to eight alphanumeric characters (Default = nosets). This cookie replaces the RTU RW community string when SNMP SET is restricted at the RTU. **Restrict SNMP SET at RTU on Port *n* (*n* = port 1-4)** – Four SNMP security features to enable or disable SNMP sets for a specific endpoint. When this field is set to Enable, the endpoint cookie will be used by both the port card and the endpoint as the RW community string. Any external SNMP SET to the RTU (including the IP Injection Tool) will be denied due to community string mismatch. Automatic updates originating from the DSL port card will be the only SNMP sets accepted by the RTU. You must disable cookie security in order to make any changes to the RTU from the IP Injection Tool or any other SNMP manager.	
Logical Entities (SNMP Logical Entities)	**A-F-B**
This screen displays information contained in the logical table of the Entity MIB. Make sure that the information you configure matches the community strings as configured on the RADSL cards. If only the RADSL card is set, the community string that the MCC card has in its entity MIB will not match. ■ **I** (Index) – The index number of RADSL ports 1 to 4. ■ **T** (Type) – Remote. ■ **Logical Descr.** – Name you can assign to the RTU/customer for each port. ■ **Read Write Comm.** – The community strings of the RTU attached to this port. It is used when the DSL system downloads configuration data to the RTU.	
Communities/Traps (SNMP Communities/Traps)	**A-F-C**
Allows you 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 RADSL card sends trap messages. It also lets you configure four communities with three trap destinations each, 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** – SNMP community string name. You can enter up to 32 characters, and up to four unique entries per screen. Default names are public (ro), mcc (rw), nms (rw), nms-2 (ro). **Access** – Permission that is granted for each community. ReadOnly(RO)/ReadWrite(RW)/NoAccess(NA), up to four entries per screen. **IP Address** – *nnn.nnn.nnn.nnn* format. Enter NMS system host IP address. **Input Number (port)** – *nnn* format. Enter NMS system port number. (Default = 162 for traps.) **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 3-7 and press Enter.

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 Next Hop Router 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 the ISP domain names in the Domain Name field, and press Enter after each entry.

   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 1–4, Servers 5–8, Servers 9–12, or Servers 13–16* (**A-G-B**, **C**, **D**, or **E**).
5. Enter values for the fields listed in Table 3-7 and press Enter after each entry.

Table 3-7. 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. **Interface IP Address –** Read-only. **ISP Domain Name –** Enter the corresponding domain name (32 nonnull characters). Delete the Domain name by entering the – (hyphen) character. The first ten characters entered will display on the DHCP server configuration pages.	
Servers 1-4 **Servers 5-8** **Servers 9-12** **Servers 13-16**	**A-G-B** **A-G-C** **A-G-D** **A-G-E**
Allows you to configure the DHCP and Authentication Server IP addresses for the 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 up to two DHCP servers and up to two authentication servers. The full domain name will be displayed at the bottom of the page if the character “n” is entered in any of the associated IP address fields. **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 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. **Authentication wait time** – Length of time, in seconds, the system waits for a response before timing out. (Default = 3). **Number of Authentication attempts** – Number of attempts to the authentication server (Default = 2). **Dynamic access control security** – Security control flag. (Default = Enable). **Port *n* Default DHCP Domain index (0–16, 0 for none)** – Which domain’s DHCP service will be used. (Default = 0).	

DSL Configuration RTU Screens

Use the system information submenu of the RTU screens to configure RTU information.

▶ Procedure

1. Follow this menu sequence:

   Configuration →*RTU* (**A-H**).

2. The RTU menu appears. Enter the desired value on the selected screen and field as shown in Table 3-8 and press Enter.

Table 3-8. RTU Options

RTU Selection	A-H-A
Displays RTU information such as RTU type, system, location, 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 5246/5216. For Model 8546, possible endpoints are 5446r1/5446r2. **System Name** – 16 alphanumeric characters. Name assigned to the RTU. **System Contact** – 32 alphanumeric characters. Name or number of the person responsible for the RTU. **System Location** – 16 alphanumeric characters. Physical location of the RTU. **System Circuit ID** – 32 alphanumeric characters. Circuit ID of the RTU. **Model Num*** – Model number of card. (This field is read-only.) **Serial Num*** – Serial number of card. (This field is read-only.) **Firmware Rev.*** – Version of firmware. (This field is read-only.) **Hardware Rev.*** – Version of hardware. (This field is read-only.) **CAP Rev*** – Version of CAP Release. (This field is read-only.) **Reset RTU?** – Yes/No. (This field will not appear if the RTU type is 5446r1 or 5446r2.) **RTU Selftest Result** – The results of the RTU selftest, if supported by the RTU.	
* If available, information in these fields is displayed.	

Monitoring the Hotwire DSL System

4

Overview

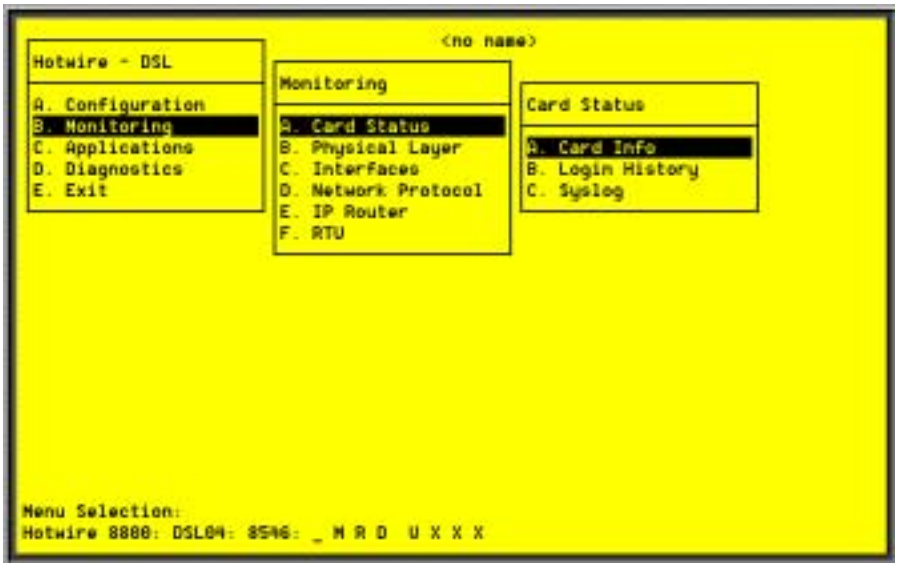
The Hotwire DSL system lets you to monitor the activity of the Hotwire DSL cards. When you select Monitoring from the Hotwire DSL Main Menu, a menu tree of selections on history and error logs, performance statistics, card status, and physical and logical interface status information is presented.

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 5, *Diagnostics and Troubleshooting*.

DSL Monitoring Menu

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**)

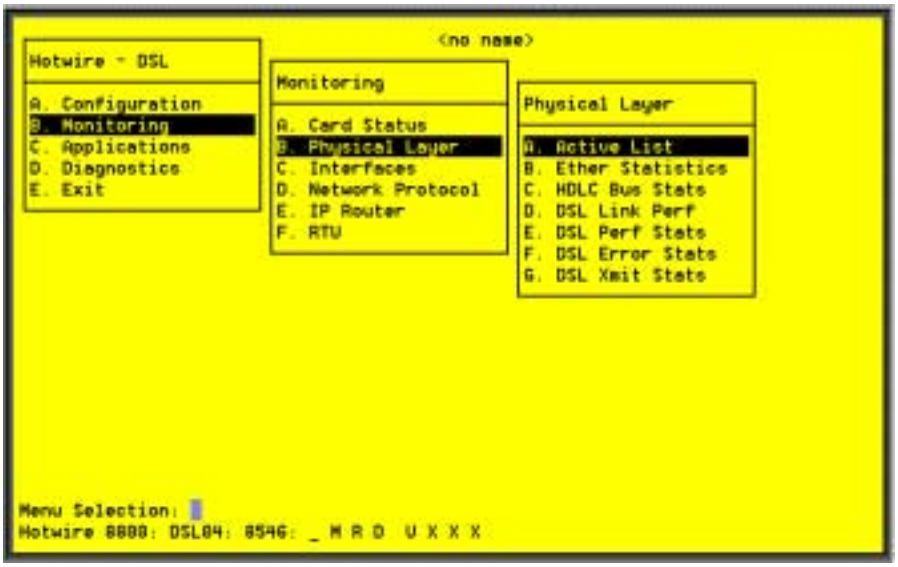
2. The Card Status menu appears. Select the submenu option as shown in Table 4-1 and press Enter.

Table 4-1. 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. **Card Name** – Name assigned to the card. **Card Location** – Physical location of the system. **Card Contact** – Name or number of the person responsible for the card. **Card 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. **Available** – 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 first). Logins can either be local (shows user login name) or remote (shows remote IP address). A remote IP address of 0.0.0.0 is the MCC card. **User** – User ID of local logins. **Time** – Time of login (read-only). **Remote** – IP address of remote logins. **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. See Chapter 5, *Diagnostics and Troubleshooting*, for SYSLOG error message information.	

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 4-2 and press Enter.

Table 4-2. 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** – SNMP ID number. **Name** – System name. **Description** – Type of port. **MAC Address** – MAC address of the active port. (Internal dummy address used for non-Ethernet ports.) **Status** – Active, disconnected, in-use.	
Ether Statistics (Ethernet Statistics)	**B-B-B**
Displays a list of the Ethernet statistics of the LAN port (e1a). You may press 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. **Packets Received** – Number of packets transmitted by the Ethernet port and what type (multicasts, broadcasts, flooded, local origin, queued). – Multicasts – 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. – 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.	

Table 4-2. Physical Layer Options (2 of 5)

Ether Statistics (Ethernet Statistics) (continued)	**B-B-B**
Bytes Transmitted – Number of bytes transmitted on the Ethernet port. **Packets Transmitted** – Number of packets transmitted by the Ethernet port and what type. ■ Multicasts – 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. ■ 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 = 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. ■ Deferrals ■ Carrier Loss ■ Underflow ■ Buffer **Disconnects** – Number of fast restarts and what type. ■ Disable ■ MAU Drop ■ XMIT Fail (Cable on floor?) **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 press Ctrl-r at any time to reset counters. **Port** – 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 4-2. Physical Layer Options (3 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. Tells you the number of times the link has been down and the elapsed time the link has been up. Enter port number 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 1-hour period (data updated every hour), and current day (automatically resets at midnight from the system clock, data is updated every hour). **Port #** – Enter number of the port (1–4) you wish to monitor. **Operating Speeds** – The upstream and downstream operating speeds in kbps. **dn margin** – Measure of the noise margin on the specified port in the downstream direction. A positive margin number reflects a lower error rate with a higher tolerance. Margin is averaged over five measurements. **up margin** – Measure of the noise margin on the specified port in the upstream direction. A positive margin number reflects a lower error rate with a higher tolerance. Margin is averaged over five measurements. **dn err rate** – Block error rate in the upstream direction. Error rate = bad blocks/good blocks and is expressed as A x 10^{-B}. **up err rate** – Block error rate in the upstream direction. Error rate = bad blocks/good blocks and is expressed as A x 10^{-B}. **dn att est** – Measure of the estimate of loss on the DSL line in a downstream direction based on transmitter power and receiver gain. The larger the attenuation, the more loss on the loop (and generally, the larger the loop). **up att est** – Measure of the estimate of loss on the DSL line in an upstream direction based on transmitter power and receiver gain. The larger the attenuation, the more loss on the loop (and generally, the larger the loop). **link dn count** – Number of times the DSL link has gone down. **elp lnk up** – Count of the elapsed time in seconds that the link has been up. **elp time** – Count of the elapsed time in seconds since the DSL card was last reset. **pct link up** – Percentage of time the DSL link has been up.	

Table 4-2. Physical Layer Options (4 of 5)

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 to see the fields for current 15-minute period (real-time count of events during the past 0–15 minutes); previous 15-minute period (data updated every 15 minutes); previous 1-hour period (data updated every hour); and current day, starting at 12:01 a.m. (data updated every hour).

Port # – Enter number of the port (1–4) you wish to monitor.

15min Valid – Number of 15-minute intervals in which downstream performance data, which is measured by the 5446 RTU, has been received across the DSL link from the RTU.

All Data

pkt rcv dn – Number of downstream packets received.

pkt snt dn – Number of downstream packets sent.

pkt lost dn – Number of downstream packets lost.

pkt rcv up – Number of upstream packets received.

pkt snt up – Number of upstream packets sent.

pkt lost up – Number of upstream packets lost.

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.

Customer Data

k octs sent dn – How many thousands of octets of customer data have been sent by the RADSL card to the RTU.

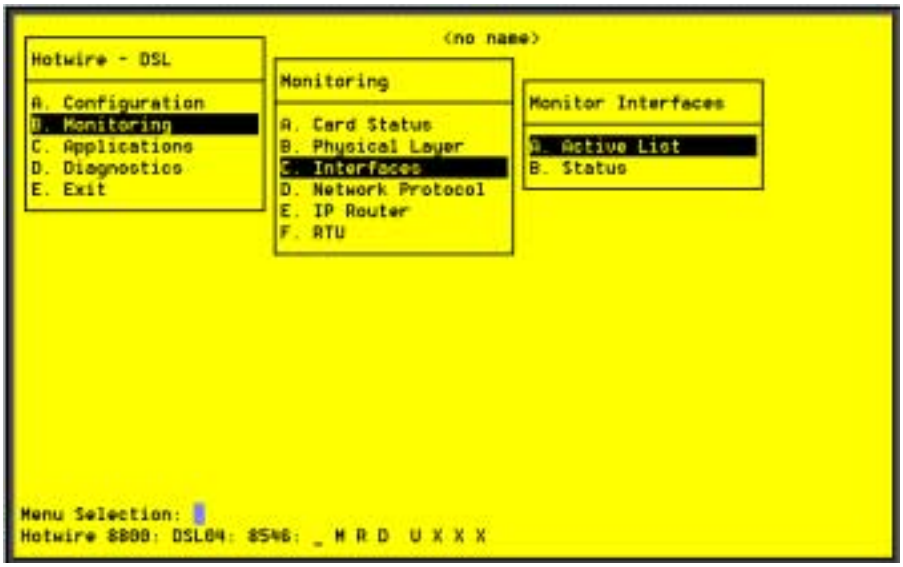
k octs rcv up – How many thousands of octets of customer data have been received by the RADSL card from the RTU.

Table 4-2. 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 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 1-hour period (data updated every hour), and current day, starting at 12:01 a.m. (data 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 press Ctrl-r at any time to reset counters. **Port #** – Enter number of the port (1–4) you wish to monitor. **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 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 1-hour period (data updated every hour), and current day, starting at 12:01 a.m. (data updated every hour). You may press Ctrl-r at any time to reset counters. **Port #** – Enter number of the port (1–4) you wish to monitor. **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 RADSL 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**)

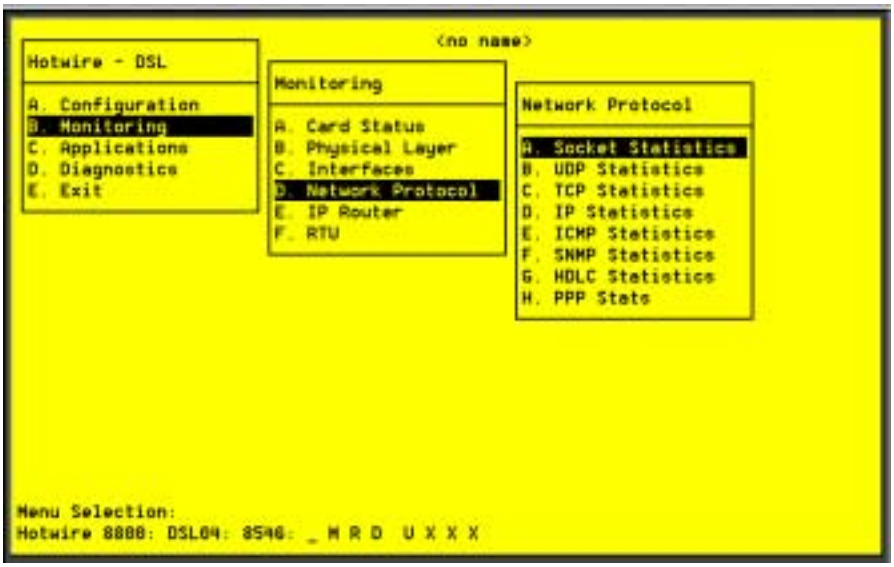
2. The Monitor Interfaces menu appears. Select the submenu option as shown in Table 4-3 and press Enter.

Table 4-3. Monitor 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 interface has been restarted. **user** – 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 4-4 and press Enter.

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

Socket Statistics	**B-D-A**
Displays information on the active sockets. 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).	
UDP Statistics	**B-D-B**
Displays information on User Datagram Protocol (UDP) statistics for packets that terminate on the RADSL card. The counters increment in real time and you may press 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 4-4. Network Protocol Options (2 of 7)

TCP Data Stats (TCP Data Statistics)	B-D-C
Displays a summary of the Transmission Control Protocol (TCP) data activity (packets and bytes transmitted and received) on all interfaces on the RADSL 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 press 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 rcvd 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/bytes rcvd out-of-order** – Packets received out of order. **pkts/bytes 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 rcvd 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 pkt 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** – Number of the sent packets that were data packets instead of TCP control packets. **data pkts/bytes retransmit** – Number of packets/bytes that had to be transmitted. **ack-only pkts** – Number of sent packets that contained only an ack of a received packet and no additional data. **URG only pkts** – Number of packets that contained only an Urgent flag and no data. **window probe pkts** – Number of packets that were window probes. **window update pkts** – Number of packets that were advertising our new window size. **control pkts** – Number of control packets sent (SYN, FIN, or RST flag).	

Table 4-4. Network Protocol Options (3 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 packets received** – Total number of IP packets received by this card, with errors broken down on the right of the screen. **fragments received** – Number of packet fragments received, with dropped fragments on the right of the screen. **packets were fragmented 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 for local networks** – Number of network broadcasts received for local networks. **network broadcasts forwarded by media broadcast** – Number of network broadcasts for local networks sent. **network broadcasts partially processed** – Number of network broadcasts dropped due to an error.	

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

ICMP Statistics (ICMP Packet Statistics)	**B-D-E**

Displays a summary of the Internet Control Message Protocol (ICMP) activity on the backplane that terminates on the DSL card, such as echo replies.

The columns show output and input packet counts.

The counters increment in real time and you may press Ctrl-r at any time to reset the counters. Press Enter to see more ICMP statistics.

The following statistics appear:

- echo reply
- destination unreachable
- source quench
- routing redirect
- echo
- time exceeded
- parameter problem
- time stamp request
- time stamp reply
- information request
- information request reply
- address mask request
- address mask reply
- calls to icmp_error
- messages too short were ignored
- icmp messages received with an error were ignored
- messages with bad code fields
- messages < minimum length
- bad checksums
- messages with bad length
- messages responses generated

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

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 Enter, the SNMP Authentication Statistics screen is displayed, giving you additional Community Administration information. The counters increment in real time and you may press 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 Parse Errors** – 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 4-4. Network Protocol Options (6 of 7)

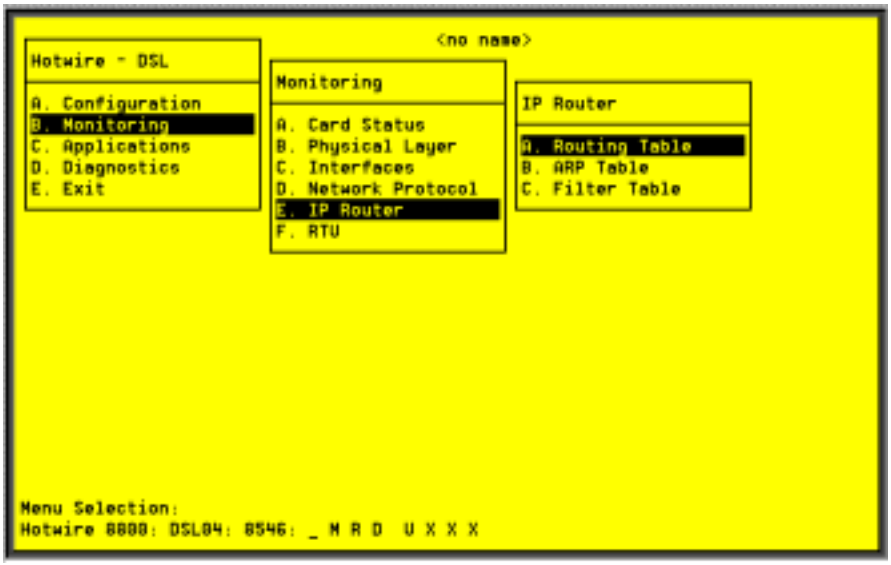
SNMP Authentication Statistics (continuation of previous screen)	**B-D-F**
The SNMP Authentication Statistics screen displays the following information: **Community Administration** – Number of SNMP PDUs with community based authentication. **Bad Versions** – Total number of SNMP messages delivered to 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 press 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 4-4. 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 DSL interface (s1c, s1d, s1e, s1f). **Link Phase** – Current phase/state of this link (Init, Link Control). **Octets Transmitted** – Number of octets (8 bit bytes) transmitted. **Octets Received** – Number of octets received. **Frames Transmitted** – Number of frames (groups of data bits) transmitted. **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** – Number of packets received with unknown address. **Bad Checksum Packets Received** – Number of packets received with bad checksum. **Frame Errors Received** – Number of packets received with bad framing. **Other Pkt Errors Received** – Number of packets 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 side 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. **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 side 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). **IPCP Configuration** – Configuration of the IPCP 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 4-5 and press Enter.

Table 4-5. IP Router Options (1 of 2)

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). NOTE: This screen will not display any routes that were identified as rmt s1*x* in the location field on the Static Routes screen.	
Route Information Window 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 without a preference, 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. NOTE: **lb0** is equal to **e1a**. **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 nonpermanent 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.	

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

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. NOTE: **lb0** is equal to **e1a**. **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).	
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. **# Static Rules** – Number of static routes in filter. **# Dynamic Rules** – Number of dynamic routes in filters. **Ref Cnt** – Number of active interfaces using the filter. **Def Action** – Default action for the filter.	

DSL Configuration RTU Screens

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

▶ Procedure

1. Follow this menu sequence:

   Monitoring →*RTU* (**B-F**)

2. The RTU menu appears. Select the submenu option as shown in Table 4-6 and press Enter.

   NOTE:

   For Model 8540, only menu items Information (**B-F-A**) and Static Routes (**B-F-B**) appear.

Table 4-6. RTU Options

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 5246/5216. For Model 8546, possible endpoints are 5446r1/5446r2). **System Name** – Name assigned to the RTU. **System Contact** – Name of number of the person responsible for the RTU. **System Location** – Physical location of the RTU. **System Circuit ID** – Circuit ID of the RTU. **Model Num*** – Model number of card. **Serial Num*** – Serial number of card. **Firmware Rev*** – Version of firmware. **Hardware Rev*** – Version of hardware. **CAP Rev** – Version of CAP Release.	
* These fields may be blank if older version RTUs are connected to that port.	

Diagnostics and Troubleshooting

5

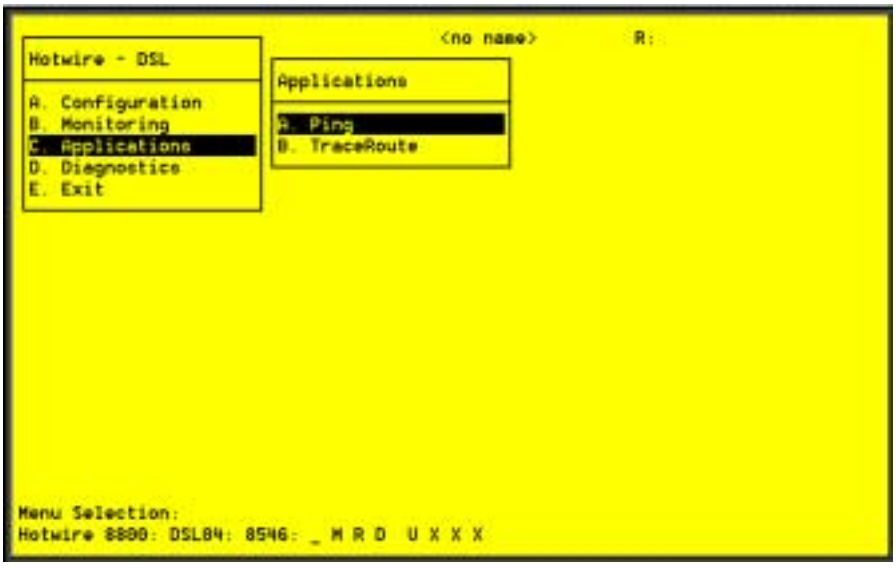
Overview

Diagnostics for the system are available through the following:

- Applications menu (**C**) – For a Ping or TraceRoute.
- Diagnostics menu (**D**) – To display the results of a selftest or alarm conditions, and to conduct a nondisruptive packet test.
- SYSLOG (**B-A-C**) – To display SYSLOG messages.

Applications Screens

Use the Applications submenu to perform a Ping or TraceRoute.



▶ Procedure

To use the Ping or TraceRoute function:

1. Follow these menu sequences:

   Applications → *Ping* (**C-A**)

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

2. Select Applications from the Hotwire 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 5-1 and press Enter.

Table 5-1. Applications Options

Ping IP Settings	**C-A**
Allows you to conduct a nondisruptive 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. **Destination IP address** – IP hostname or address in *nnn.nnn.nnn.nnn* format. **Packet Size** – 12–1600 bytes (Default = 64). **Timeout** – Maximum time (in seconds) that the system should wait before assuming that the packet was lost. 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 this information is entered, a results screen is displayed. Results include a list of reporting hops, each with a hop number and IP address.	

Diagnostic Screens

Use the Diagnostics submenu to perform selftests or view alarm status.

▶ Procedure

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

1. Follow these menu sequences:

   Diagnostics →*Selftest* (**D-A**)

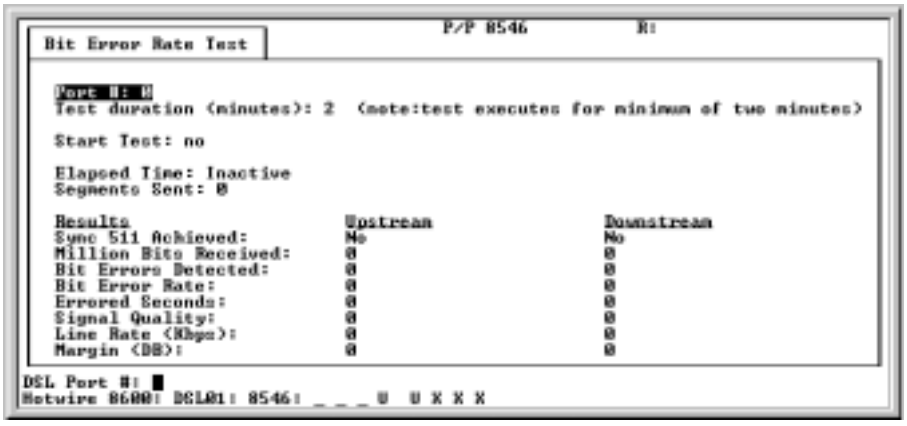
   Diagnostics → *Alarms* (**D-B**)

   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 5-2 and press Enter.

Table 5-2. 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**
Allows you to conduct a nondisruptive 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 (5 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 tested at a time.	
BERT Test	**D-D**
For Model 8546 only. Allows you to conduct a nonstoppable, disruptive 511 BERT Test on each DSL port. Using the current operating speed, the test lasts two minutes, after which the connection with the RTU is disconnected. Information provided by the test includes elapsed time, sync of 511 pattern achieved/not achieved, bits received (in millions), bit errors detected, bit error rate, and errored seconds for both up and down directions.	



Troubleshooting

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

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.

No Response at Startup

DSL cards do not respond at startup after rebooting chassis. Reset the MCC card. Be sure LEDs go through the reset sequence twice within about one minute.

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. See *SYSLOG Messages* on page 5-9.

Major Alarms

Use Table 5-3 to determine the appropriate action to take for each Major Alarm.

Table 5-3. 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 5-3. Major Alarms (2 of 2)

Failure Type	Action
Ethernet port failure	1. Check cable connections to the DSL chassis. – 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 5-4 to determine the appropriate action to take for each Minor Alarm.

Table 5-4. 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 nonvolatile 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

Table 5-4. Minor Alarms (2 of 2)

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.

SYSLOG Messages

The SYSLOG contains an historical list of special system messages which serves as a log of certain significant events that occur in the DSL network. SYSLOG messages consist of a date and timestamp, followed by the message.

To view SYSLOG messages, access the SYSLOG menu entry (**B-A-C**).

Example SYSLOG Messages

Interpreting SYSLOG messages sometimes involves viewing a series of messages to determine the problem. Event messages can indicate that certain thresholds have been exceeded.

By comparing the embedded timestamp received from the remote unit to the timestamp in the port card message, you can determine which end of the DSL link entered the retrain state first, and which simply reacted to the training sequence from the other end. The port card SYSLOG message always appears first.

See the following examples.

Example 1. Port Card (Upstream Channel) Retrain

The following SYSLOG messages have been received:

```
Thu Apr 22 09:53:26 1999 S/N Threshold Reached, port DSL port 4

Thu Apr 22 09:53:50 1999 Remote Restarted at Thu Apr 22 09:53:34
1999

Thu Apr 22 09:53:50 1999 Remote Reed Solomon Restart, Port 4
```

Meaning:

The upstream Signal-to-Noise (S/N) ratio has dropped below the acceptable threshold and the port card has retrained. The remote unit retrain has occurred after the port card retrain.

Example 2. Remote Unit (Downstream Channel) Retrain

The following SYSLOG messages have been received:

```
Fri Apr 23 09:53:32 1999 S/N Threshold Reached, port DSL port 4

Fri Apr 23 09:53:50 1999 Remote Started at Fri Apr 23 09:53:28 1999

Fri Apr 23 09:53:50 1999 Remote Reed Solomon Restart, Port 4
```

Meaning:

The port S/N ratio has been reached. The port card retrained after the remote unit as indicated by the embedded timestamp at the end of the remote SYSLOG message. This retrain was caused by Reed Solomon errors. In general, if the port card is experiencing a line performance problem and enters the retrain state first, the remote unit typically retrains due to Reed Solomon Restart. If the remote unit enters the retrain state first, the port card will typically show a S/N Threshold Reached error message.

Example 3. System Status Message

The following SYSLOG message have been received:

```
Fri Apr 9 11:13:15 1999 Link Transition Threshold Exceeded, port
DSL2
```

Meaning:

The number of DSL retrains (transitions) has exceeded the Link Down Count configured on the DSL Parameters screen (**A-B-B**). This is checked every 15 minutes when the current 15-minute bucket is shifted to the previous 15-minute bucket. There will never be more than one SYSLOG message for each 15-minute period. The Link Down Count only determines if a trap is sent. It has no effect on when the units will retrain.

Example 4. Port Card Status Messages

The following SYSLOG messages have been received:

```
Mon May 3 10:25:31 1999 Margin Threshold Exceeded, DSL port 3

Mon May 3 10:26:36 1999 ALARM: DSL3 Margin Low Set

Mon May 3 10:27:42 1999 Margin Threshold Normal, port DSL3

Mon May 3 10:28:50 1999 ALARM: DSL3 Margin Low Clear
```

Meaning:

The margin has gone below what was set as a startup margin on the DSL Parameters screen (**A-B-B**) and an alarm message has been sent to the NMS. Then, the margin returned to a value above what has been set on the DSL Parameters screen and the message has been sent to the NMS.

Example 5. Link Restart Commanded Retrain Messages

The following SYSLOG messages have been received:

```
Mon Jul 19:15:16:15 1999 Restart Caused by Link Restart DSL port 2

Mon Jul 19 15:17:01 1999 Remote Restarted at Mon Jul 20 15:16:52
1999

Mon Jul 19 15:17:01 1999 Remote Reed Solomon Restart, DSL port 2
```

Meaning:

The port card retrained because of a Link Restart command issued by an operator. The remote unit retrained because the port card retrained.

Network Problems

Review Table 5-5 for symptoms and possible solutions to help in solving any network problems you may encounter in the Hotwire DSL system.

Table 5-5. Network Problems (1 of 3)

Problem	Action
Cannot communicate with Ethernet or other interface after adding, changing, or deleting IP addresses on DSL or MCC card.	When you add, change, or delete addresses on a DSL card, you must restart that interface (see *Configuration* → *Interfaces* (**A-C**) in Chapter 3, *RADSL Card Configuration*).
Cannot establish an SNMP session/ connection.	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 the *Hotwire Management Communications Controller (MCC) Card User's Guide*. 3. If there is an IP address, then check the routing tables in the MCC card and RADSL 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 RADSL 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 4, *Monitoring the Hotwire DSL System*, and *Configuration* → *SNMP* (**A-F**) in Chapter 3, *RADSL Card Configuration*).

Table 5-5. Network Problems (2 of 3)

Problem	Action
Cannot Ping or Telnet after entering IP address.	1. Restart the interface (see *Configuration → Interfaces* (**A-C**) in Chapter 3, *RADSL Card Configuration*). 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 the *Hotwire Management Communications Controller User's Guide*). 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 subnet mask is set correctly. If in doubt, leave the default subnet mask (see *Who Am I* screen in the *Hotwire Management Communications Controller (MCC) Card User's Guide*). 6. Check to see that the IP next hop address matches that of the router (if communicating through IP router) (see *Configuration → IP Router* (**A-E**) in Chapter 3, *RADSL Card Configuration*). 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 4, *Monitoring the Hotwire DSL System*).
DSL cards do not respond at startup after rebooting chassis.	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 3, *RADSL Card Configuration*).
DSL cards not using MCC Router ID as source address for traps.	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 3, *RADSL Card Configuration*).
Excessive collisions on an Ethernet port.	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.
Filters are not working properly.	1. Check to see that filters have been configured properly (see *Configuration → Interfaces* (**A-C**) in Chapter 3, *RADSL Card Configuration*). 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.

Table 5-5. Network Problems (3 of 3)

Problem	Action
Intranetworking communication problems.	1. Verify that the internetworking network cables meet IEEE standards for local Ethernet networks. 2. Check cable connections to DSL chassis and other devices in the network. 3. Determine whether or not your system is the only one in the network with a problem.
Performance is slow.	1. Verify that there are enough buffers on the System Info screen and reset the system (see *Monitoring → Card Status* (**B-A**) in Chapter 4, *Monitoring the Hotwire DSL System*). 2. Check the Ethernet Statistics screen for excessive Cycle Redundancy Check (CRC) errors, a bad connection, or a bad cable (see *Monitoring → Physical Layer* (**B-B**) in Chapter 4, *Monitoring the Hotwire DSL System*).
PPP circuit is forwarding no traffic.	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.
Proxy ARP not properly set for Hotwire 5446 RTU.	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.
Stations cannot communicate through the router. Incorrect IP address. Incorrect Subnet Mask.	1. Check to see that IP addresses have been configured correctly (see *Who Am I* screen in the *Hotwire Management Communications Controller User's Guide*, and *Configuration → Interfaces* (**A-C**) in Chapter 3, *RADSL Card Configuration*). 2. Go to: *Configuration →Interface →Control* (**A-C-C)** and monitor the state of the system for e1a Bridge Up (forwarding).
System does not recognize new DSL cards with new addresses (Addresses not preconfigured on MCC card).	1. Configure new DSL cards from MCC screen. 2. Restart s1b interface (see *Configuration → DSL Cards* (**A-G**) in Chapter 3, *RADSL Card Configuration*). 3. Reset DSL card from the MCC screen (see *Configuration → DSL Cards* (**A-G**) in Chapter 3, *RADSL Card Configuration*). 4. Pull the card out and push it back in.
TFTP server denies write permission (Message is **`TFTP recv failure`**).	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.

Download Code

A

The Hotwire DSL system's Download Code menu option 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 cannot, 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 RADSL cards in your system. When a software upgrade affects both the MCC and the RADSL cards, you must download and apply a new version of code into each of the RADSL cards **before** you download and apply a new version of code into the MCC.

When you are attempting to download to the RADSL cards, refer to *Download Code*. In general, the following sections describe what to expect when you have initiated a download from the configuration menu.

Download Code

When you are attempting to download to the RADSL cards, refer to Table 3-1, Card Status Options, in Chapter 3, *RADSL Card Configuration*. In general, the following describes what to expect when you have initiated a download from the configuration menu.

From the DSL Configuration Main Menu, select:

Configuration →*Card Status* →*Download Code* (**A-A-G**).

This selection brings you to the Download submenu. Select Download Code (**A**).

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. 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 DSL Configuration Main Menu, select:

Configuration →*Card Status* →*Download Code* (**A-A-G**).

This selection brings you to the Download submenu. Select Apply Download (**B**).

SNMP Traps

B

Traps are configured via a Telnet or terminal session. The addition or removal of a card or another hardware component within the Hotwire DSL 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).

Setting Up SNMP Trap Features

Use the following procedures for setting up SNMP trap features.

DSL SNMP Community Strings and Authentication Failure Trap

▶ **Procedure**

To set up DSL SNMP Community Strings and enable the Authentication Failure Trap:

1. Follow this menu sequence from the DSL Main Menu:
   Configuration →*SNMP*→*Communities/Traps* (**A-F-C**)
2. Enter Read Only community string name(s).
3. Enter Read/Write community string name(s).
4. If desired, enable the Authentication Failure trap.
5. Enter the IP address of addresses of the NMS.

Enable DSL Port Traps

▶ Procedure

To enable DSL Port Traps:

1. Follow this menu sequence from the DSL Main Menu:
   Configuration →*Ports* →*DSL Ports* (**A-B-B**)
2. Select a DSL port.
3. If desired, enter a value for the following:.
   - — Margin Threshold
   - — Link Down Count Threshold
   - — Error Rate (minute) Threshold.
   - — Error Rate (hour) Threshold.

   See Table 3-2, Port Options, in Chapter 3, *RADSL Card Configuration,* for more information.
4. Reset the port following this menu sequence:.
   Configuration →*Interfaces* →*Control* (**A-C-C**)

   See Table 3-3, Interfaces Options, in Chapter 3, *RADSL Card Configuration*, for more information.

DSL Card Traps

The DSL card sends the following traps.

Table B-1. DSL Card Traps (1 of 4)

Event	Severity	Comment	Trap #	MIB
Authentication failure	minor	SNMP community string.	4	MIBII (RFC 1213)
		Telnet passwords. This trap may be overloaded for Telnet based authentication failures. In these cases, the following will also be sent along with the trap PDU: ■ Access mode used ■ Number of Auth failures ■ Source IP address of failed message ■ Attempt type (local, Telnet, SNMP get, SNMP set) Also sent for RADIUS authentication failure with the following information: ■ Access mode used (Telnet or terminal) ■ Number of Auth failures ■ Interface index ■ Authentication type (remote = RADIUS authentication)	8	hot_sys.mib (Hotwire system)
CCN (Configuration Change Notice)	warning	Configuration change caused by one the following events: ■ software download ■ configuration download ■ card removed (objective)	7	hot_sys.mib (Hotwire system)
		Configuration change caused by one the following events: ■ change affecting the entity MIB		hot_domain.mib (Enterprise domain)
Cold start	warning	Card has been reset and performed a cold start.	0	MIBII (RFC 1213)
Configuration download failure	warning	Configuration download has failed.		

Table B-1. DSL Card Traps (2 of 4)

Event	Severity	Comment	Trap #	MIB
Device failure	major	Access Node's operating software has detected an internal device failure.	15	hot_sys.mib (Hotwire system)
DHCP filter security failure	minor	Cannot add new route to route table because maximum number of stored rules reached.	11	hot_dhcp.mib (Hotwire DHCP Relay Agent)
xDSL link down analysis trap	major	Sending protocol entity recognizes that the xDSL communication link is down and lists reason: ■ Normal – Normal power-up training sequence ■ Rate adaption – Retrain due to rate adaption speed change ■ Low margin – Retrain due to margin falling below threshold ■ Low RSL – Retrain due to receive signal level too low ■ High SNL – Retrain due to signal-to-noise level too high ■ High CRCs – Retrain due to excessive cyclic redundancy check errors ■ High RS – Retrain due to excessive Reed-Solomon buffer overflows ■ Change power – Retrain due to startup message containing a different transmitter power level than the current operating level ■ Default power – Retrain and revert to default -6bl transmitter level after a failure to train at the last configured level	21	hot_xdsl.mib (Hotwire XDSL Interface)
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.	1	hot_xdsl.mib (Hotwire XDSL Interface)

Table B-1. DSL Card Traps (3 of 4)

Event	Severity	Comment	Trap #	MIB
xDSL margin low	minor	Margin estimate below customer set threshold.	3	hot_xdsl.mib (Hotwire XDSL Interface)
xDSL margin normal	normal	Margin estimate above customer set threshold.	103	hot_xdsl.mib (Hotwire XDSL Interface)
xDSL port failure	major	Processor detected bad DSL modem chip set.	5	hot_xdsl.mib (Hotwire XDSL Interface)
xDSL port operational	normal	Processor can now communicate with DSL modem chip set.	105	hot_xdsl.mib (Hotwire XDSL Interface)
xDSL port speed low	warning	Port speed decreased to lower bound threshold setting.	2	hot_xdsl.mib (Hotwire XDSL Interface)
xDSL port speed normal	normal	Port speed now above lower bound.	102	hot_xdsl.mib (Hotwire XDSL Interface)
xDSL RTU selftest fail	warning	Selftest failure from a 5546 RTU.	16	hot_xdsl.mib (Hotwire XDSL Interface)
xDSL test start	normal	Test started by any means.	6	hot_xdsl.mib (Hotwire XDSL Interface)
xDSL test clear	normal	Test over.	106	hot_xdsl.mib (Hotwire XDSL Interface)
Dynamic filter injection failure	warning	Cannot inject or delete dynamic filters to RTU on port *N.*	10	hot_dhcp.mib (Hotwire DHCP Relay Agent)
Ethernet link down	major	—	2	MIBII (RFC 1213)
Ethernet link up	normal	—	3	MIBII (RFC 1213)
Remote host route delete failure	warning	Host route in the RTU could not be deleted.		
Remote host route inject failure	warning	Host route in the RTU could not be injected.		
RTU device mismatch	minor	RTU identified on port *N* does not match device described in port configuration table.	07	hot_xdsl.mib (Hotwire XDSL Interface)

Table B-1. DSL Card Traps (4 of 4)

Event	Severity	Comment	Trap #	MIB
RTU device mismatch clear	normal	RTU identified on port *N* now matches device described in port configuration table.	107	hot_xdsl.mib (Hotwire XDSL Interface)
RTU community name deletion failure	warning	Deletion of RTU community name failed.		
RTU remote service domain deletion failure	warning	Deletion of RTU remote service domain failed.		
RTU trap manager deletion failure	warning	Deletion of RTU trap manager failed.		
RTU static route deletion failure	warning	Deletion of RTU static route failed.		
RTU system information deletion failure	warning	Deletion of RTU system information failed (system name, system contact, system location).		
RTU system information injection failure.	warning	Injection of RTU system information failed (system name, system contact, system location).		
RTU community name injection failure	warning	Injection of RTU community name failed.		
RTU remote service domain injection failure	warning	Injection of RTU remote service domain failed.		
RTU Trap Manager injection failure	warning	Injection of RTU Trap Manager failed.		
RTU static route injection failure.	warning	Injection of RTU static route failed.		
Selftest failure	minor	Sent if any portion of a restart/selftest fails.	16	hot_sys.mib (Hotwire system)
Warm start	warning	Power on reset.	1	MIBII (RFC 1213)

RTU Related Traps

The RTUs send the following traps. For a listing of Paradyne Enterprise MIBS, see *SNMP Agent* in the *Hotwire 8540 and 8546 RADSL Cards Network Configuration Guide.*

Standard Traps

Table B-2. 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

Table B-3. 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.

5446 RTU Setup

C

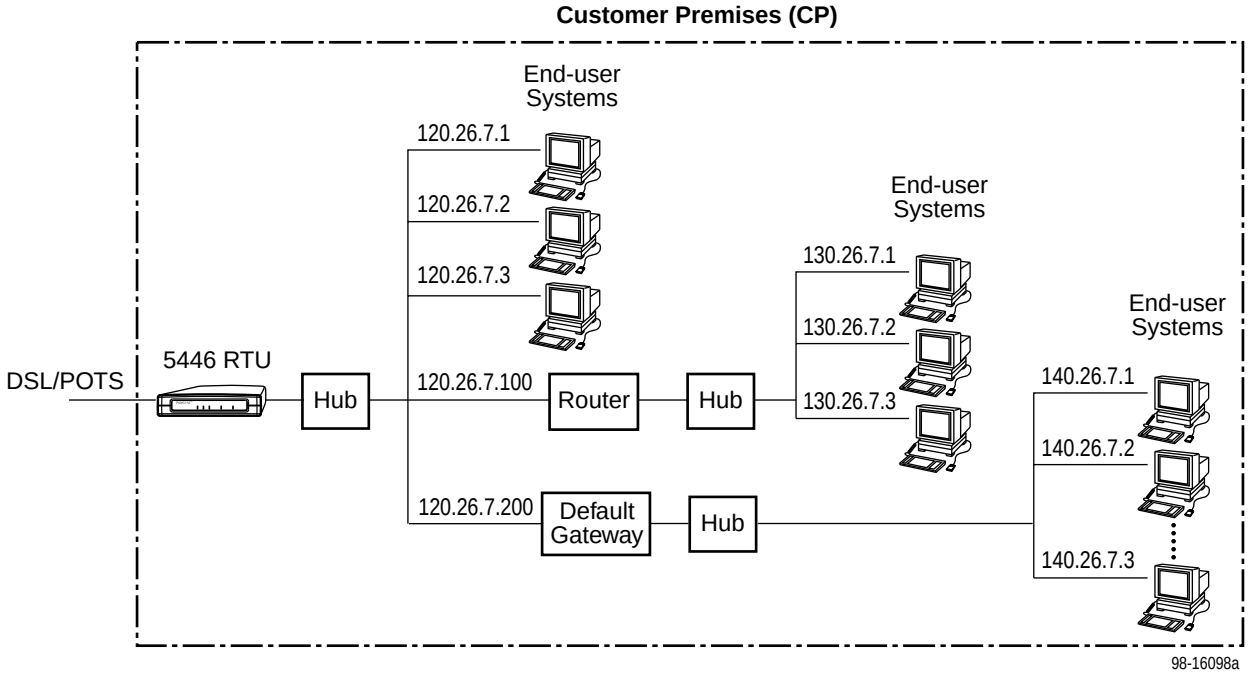
Hotwire 5446 RTU Setup Overview

The Hotwire 5446 RTU supports various customer premises distribution networks that contain IP forwarding devices or routers, in addition to locally attached hosts or subnets. The Hotwire 5446 RTU has an IP Routing 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.

For more information about the Hotwire 5446 RTU installation, see the *Hotwire 5446 RTU Customer Premises Installation Instructions.*

The 5446 RTU includes support for next hop routers and a default gateway. The following IP Routing Table Example, Figure C-1, includes connections using hubs. A host (end-user system) or router can also be connected directly to a 5446 RTU by using an Ethernet crossover cable.



IP Injection Type	IP Address	Network Mask	Next Hop Router
Host	120.26.7.1	255.255.255.255	0.0.0.0
Host	120.26.7.2	255.255.255.255	0.0.0.0
Host	120.26.7.3	255.255.255.255	0.0.0.0
Host	130.26.7.1	255.255.255.255	120.26.7.100
Host	130.26.7.2	255.255.255.255	120.26.7.100
Host	130.26.7.3	255.255.255.255	120.26.7.100
Default Gateway	0.0.0.0	0.0.0.0	120.26.7.200

Figure C-1. IP Routing Table Example

NOTES:

— If a Default Gateway is defined, all packets not destined for an entry in the IP Routing Table are sent to the Default Gateway. The Host devices (end-user systems) attached to the default gateway are not configured in the IP Routing Table (refer to IP addresses starting with 140 in Figure C-1).

— The Host devices attached to the Next Hop Router are configured once in the IP Routing Table with the Next Hop Router field (refer to IP addresses starting with 130 in Figure C-1). The Host entry can also specify a remote subnet, as needed.

Accessing the Hotwire 5446 RTU IP Injection MIB

The IP Injection Tool provides the ability to use the SNMP agent in the 5446 RTU to manage IP address, subnet mask, and community string information. 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.

Downloading the IP Injection Tool

This tool is available from Paradyne's 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 Windows 95 or Windows NT 4.0. The PC must be connected to the management interface for the MCC card *(e1a).*

▶ Procedure

To download the Hotwire 5446 RTU IP Injection Tool:

1. Access the Paradyne World Wide Web site at **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 then double-click on **`Setup.exe`**.
5. At the prompt: Do you wish to install Microsoft OLE Automation?
   - — Windows 95 platform: select Yes
   - — Windows NT 4.0 platform: select No

Accessing the IP Injection Tool

Once the program is successfully installed, an icon labeled IP Injection Tool is created. The Paradyne IP Injection Tool input screen appears when the tool is accessed. Access the online Help file for further information.

NOTES:

— Before using this tool, you must know the RTU Network Access Provider (NAP) and have established an active DSL link to the RTU. The NAP IP Address is also know as the Peer IP Address when configuring the corresponding port on the 8546 RADSL card.

— After initial installation, enter the RTU NAP IP Address and click on Get All to obtain the Device Information as shown on the next screen.

Community String Entries

The Community String Selection fields are located before the selection buttons near the bottom of the screen and can display a read-only and a read-write community string.

The read-write Community Name defaults to ‘private’. The read-write Community Name is used by the IP Injection tool to send SNMP messages to the 5446 RTU. The IP Injection tool and the 5446 RTU also use the private Community Name to make changes to the 5446 RTU configuration.

To change a community string, enter the new community string in the text input box (up to 32 characters). Click on the Inject button. Changes to:

- Read-write community string result in two messages: **`Operation successful`** followed by **`SNMP Timeout Error`**. Enter the newly created community string in the top right Community field and click on the Get All button to finalize the update.
- Read-only community string results in the message: **`Operation successful`**. If you click on the Get All button with the read-only community string, the read-write community string will display **<unknown>** for security purposes. The read-only Community Name defaults to ‘public’.

IP and Device MIBs Supported

The IP Injection MIB provides the capability to inject IP address information for hosts, applications, networks, or a local device. The following pdn-IP Injection Objects (pdn-common 11) contain IP address information. Information built from this table includes:

- **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.

The IP Injection Table supports:

- One NAP IP Address injected as the Peer IP Address from the Hotwire DSL system. The NAP IP Address should not be added, deleted, or changed via SNMP.
- Four service domain IDs.
- Thirty-two Host Routes, Routers, and/or Subnets.
- One Default Gateway.
- One Next Hop Router.

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

Configuration Requirements

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.

Refer to *IP Injection Tool Group Objects Table* on page C-11 for IP Injection group object details. The first three Route Type entries must be entered in the 5446 RTU IP configuration table:

- **NAP address.** This address is automatically injected across the DSL link by the corresponding DSL port of the 8546 card and should not be modified.
- **Service Provider address.** This is the IP address assigned to the 5446 RTU's Ethernet port in the service provider domain.
- **Host address.** The Host address is the IP address of the single end-user system or subnetwork connected to the 5446 RTU and is configured via the IP Injection tool.
- **Default Gateway address.** The default gateway is used:
  - — When Network Address Translation (NAT) must occur, or
  - — To forward any downstream traffic that does not meet any existing forwarding policies.

  If a default gateway is not configured, unknown traffic is dropped.

  Only one default gateway is used and is not included in the maximum of 32 locally attached hosts. The ipInjectionNHRAddr *(ipInjectionEntry 5)* object is used to enter the IP Address of the default gateway and requires a next hop router address.
- **Next Hop Router address.** The ipInjectionNHRAddr *(ipInjectionEntry 5)* object applies when the value of ipInjectionType is set to Host. This object can contain the IP address of a:
  - — Next Hop Router for a defined host or subnet, or
  - — Default Gateway used to send unknown traffic downstream.

  NOTE:

  Up to 32 host entries for end-user systems can be specified. Of the 32 entries, each can be statically provisioned with a Next Hop Router. The 5446 RTU continues to support a mix of dynamic and statically assigned addresses.

Network Management Systems

OpenLane DCE Manager, one of Paradyne's Network Management Systems, 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 Hotwire chassis. 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
```

Using a MIB Browser

Use a MIB browser to access the ipInjectionTable. The Enterprise IP Injection MIB OID (Object ID) is 1.3.6.1.4.1.1795.2.24.2.11.

From an SNMP workstation:

1. To load the IP Injection MIB, access the Paradyne World Wide Web site at **www.paradyne.com**.
2. Select the Paradyne Enterprise MIB:

   Service & Support → MIBs → Hotwire DSL
3. After the pdndce.mib appears, save the MIB file in the NMS MIB directory with other MIB files by either:

   — Clicking the right mouse button on pdndce.mib and selecting *Save As*

   — Clicking the left mouse button on pdndce.mib and selecting *File → Save Link As*
4. Enter the IP address of the 5446 RTU.
5. Press Options to change Set Community to Private.
6. Locate the MIB group pdn-ipinjection.

From a MIB Browser:

1. To load the IP Injection MIB, access the Paradyne World Wide Web site at **www.paradyne.com**.
2. Select the Paradyne Enterprise MIB:

   Service & Support → MIBs → Hotwire DSL
3. Using the MIB Browser, click on pdndce.mib and save the MIB file in the NMS MIB directory.
4. Compile the MIB Browser.
5. Select the MIB.
6. Do a single set with a unique entry containing the required fields.

Refer to the *IP Injection Tool Group Objects Table* on page C-11 for IP injection group objects and settings.

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.

▶ Procedures

Using the null entry:

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.

NOTE:

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

Using the table index:

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

IP Injection Tool Group Objects Table

Table C-1. IP Injection Group Objects (ipInjectionTable 1) (1 of 2)

Object	Description	Setting/Contents
ipInjectionType *(ipInjectionEntry 1)*	Indicates the type of IP address for each entry. Changing the NAP IP address resets the database and any of the following entries are cleared: ■ **serviceProvider(3)** ■ **host(4)** ■ **defaultGateway(5)**	■ **null(1)** – Use to add a new row. Defaults: – Address: **0.0.0.0** – Mask: **255.255.255.255** – Status: **static** ■ **nap(2)** – Network Access Provider IP address entry. Should not be added, modified, or deleted via SNMP. ■ **serviceProvider(3)** – Device IP address assigned to the 5446 Ethernet port in the Network Service Provider domain. ■ **host(4)** – Host IP address entry for local hosts, local subnets, remote subnets, and next hop router IP address. ■ **defaultGateway(5)** – Default gateway IP address entry.
ipInjectionAddr *(ipInjectionEntry 2)*	Specifies the IP address for the first object's entry of IP Injection Type. ■ **null(1)** – Null entry used to add a row to create an entry. ■ **nap(2)** – Device IP address in the NAP domain. ■ **serviceProvider(3)** – Device IP address in the Network Service Provider domain. ■ **host(4)** – Host IP address entry for locally attached host, local subnet, remote subnet, and next hop router IP address.	IP address for the NAP or service provider (NSP): ■ ***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. IP Injection type of Default Gateway: ■ **0.0.0.0** – Default IP address. Cannot be changed.
ipInjectionMask *(ipInjectionEntry 3)*	The subnet mask must be contiguous and left-justified. When an arbitrary mask is not supported, the SNMP agent constructs the value of the ipInjectMask based on the ipInjectionAddr entry as Class A, B, or C.	The subnet mask entry cannot be 0.0.0.0 for IP Injection type of NAP, Host, and service provider. When the IP Injection Type is default gateway, the subnet mask defaults to 0.0.0.0 and cannot be changed.

Table C-1. IP Injection Group Objects (ipInjectionTable 1) (2 of 2)

Object	Description	Setting/Contents
ipInjectionStatus *(ipInjectionEntry 4)*	Specifies the address status of static or dynamic. When the 5446 RTU is reset, static addresses are saved and dynamic addresses are not saved.	Type of static or dynamic addressing for each entry. The default is **static(1)**. ■ **static(1)** – Static addresses are assigned for the duration of the service subscription. For an ipInjectionType of serviceProvider(3), static(1) is the required entry. ■ **dynamic(2)** – Dynamic addresses are only assigned for the duration of the application session. ■ **invalid(3)** – Used to delete an entry from the table.
ipInjectionNHRAddr *(ipInjectionEntry 5)*	When using a Next Hop Router, the IP address of the router is entered. This entry is only valid when ipInjectionType is set to **host(4)** or **defaultGateway(5).** When the ipInjection type is set to **defaultGateway(5)**: ■ The Default Gateway IP address is entered in the Next Hop Router field. ■ The IP address and subnet mask default to 0.0.0.0. No other entry is valid. ■ Next Hop Router is the IP address of the locally attached host (route) that downstream traffic is forwarded to when the destination is unknown.	The Next Hop Router field is used to provide: ■ The IP address which identifies the input port of the Next Hop Router for a specific defined host or subnet. ■ Locally attached default gateway router for downstream traffic when the destination is unknown.

Viewable 5446 RTU ARP Table

The Viewable ARP Table is a standard MIB-2 object that should come with most browsers. This allows you to use the MIB browser to do a query on the 5446 RTU to retrieve ARP cache information.

To view the ARP Table, use the standard MIB-2 OID 1.3.6.1.2.1.4.22.

Glossary

10BaseT	A 10-Mbps Ethernet LAN that works on twisted-pair wiring.
address	A symbol (usually numeric) that identifies the interface attached to a network.
ARP	Address Resolution Protocol. Part of the TCP/IP suite, ARP dynamically links an IP address with a physical hardware address.
authentication server	A server whose function is to authenticate and log an end-user's access location.
backplane	A common bus at the rear of a nest or chassis that provides communications and power to circuit card slots.
bandwidth	The range of frequencies that can be passed by a transmission medium, or the range of electrical frequencies a device is capable of handling.
BOOTP	Bootstrap Protocol. Described in RFCs951 and 1084, it is used for booting diskless nodes.
bps	Bits per second. 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.
CAP	Carrierless Amplitude Modulation and Phase Modulation. A transmission technology for implementing a Digital Subscriber Line (DSL). The transmit and receive signals are modulated into two wide-frequency bands using passband modulation techniques.
central office	CO. The PSTN facility that houses one or more switches serving local telephone subscribers.
Community name	An identification used by an SNMP manager to grant an SNMP server access rights to MIB.
default route	The address used for routing packets whose destination is not in the routing table. In Routing Information Protocol (RIP), this is IP address 0.0.0.0.
DHCP	Dynamic Host Configuration Protocol. A Microsoft protocol for dynamically allocating IP addresses.
DHCP Relay Agent	A system that detects and forwards DHCP discover or request messages to the appropriate DHCP server.
DHCP server	A server which uses DHCP to allocate network addresses and deliver configuration parameters to dynamically configured hosts.
domain	A named group of machines on a network. In IP, a domain consists of a block of IP addresses with similar prefixes.
downstream	In the direction of the customer premises.
DSL	Digital Subscriber Line. The non-loaded, local-loop copper connection between the customer and the first node within the network.
DSLAM	Digital Subscriber Line Access Multiplexer. A platform for DSL modems that provides high-speed data transmission with POTS over traditional twisted-pair wiring.
e1a	Name of the DSL card's and MCC card's 10BaseT (Ethernet) interface.

Ethernet A type of network that supports high-speed communication among systems. It is a widely-implemented standard for LANs. All hosts are connected to a coaxial cable where they contend for network access using a Carrier Sense, 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 TCP/IP standard protocol that allows a user on one host to access and transfer files to and from another host over a network, provided that the client supplies a login identifier and password to the server.

gateway address The subnet that the end-user system is on.

GranDSLAM A high-density DSLAM supporting a variety of DSL transport types and network services.

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

host A computer attached to a network that shares its information and devices with the rest of the network.

host route An IP address having a subnet mask of 255.255.255.255.

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

Internet The worldwide internetwork that predominantly uses the TCP/IP protocol.

intranet A private network or internet using Internet standards and software, but protected from public access.

IP Internet Protocol. An open networking protocol used for internet packet delivery.

IP address Internet Protocol Address. The address assigned to an Internet host.

ISP Internet Service Provider. A vendor who provides direct access to the Internet.

LAN Local Area Network. A privately owned and administered data communications network limited to a small geographic area.

MAC Media Access Control. The lower of the two sublayers of the data link layer, the MAC sublayer controls access to shared media.

MAC address Media Access Control Address. The unique fixed address of a piece of hardware, normally set at the time of manufacture, and used in LAN protocols.

margin (DSL) The additional noise, measured in dB, that would need to be added to the existing noise on a given DSL loop to bring the Bit Error Rate to IE–7 (10^7).

MCC Card Management Communications Controller. The DSLAM circuit card used to configure and monitor the DSLAM.

MIB Management Information Base. A database of managed objects used by SNMP to provide network management information and device control.

NAP Network Access Provider. The provider of the physical network that permits connection of service subscribers to NSPs.

NMS Network Management System. A computer system used for monitoring and controlling network devices.

NSP	Network Service Provider. A local telephone company or ISP that provides network services to subscribers.
OpenLane DCE Manager	A proprietary network management program used with HP OpenView that helps a network administrator manage SNMP devices.
packet	A group of control and data characters that are switched as a unit within a communications network.
PING	Packet InterNet Groper. A program that is useful for testing and debugging networks. It sends an Echo packet to the specified host, and waits for a response. It reports success or failure and statistics about its operation.
POTS	Plain Old Telephone Service. Standard telephone service over the PSTN with an analog bandwidth of less than 4 Hz.
POTS splitter	A device that filters out the DSL signal and allows the POTS frequencies to pass through.
PPP	Point-to-Point Protocol. A protocol for packet transmission over serial links, specified by Internet RFC 1661.
Proxy ARP	Proxy Address Resolution Protocol (ARP). A technique for using a single IP address for multiple networks. A device responds to ARP requests with its own physical address, then routes packets to the proper recipients.
RADIUS	Remote Authentication Dial-In User Service. A user authentication protocol defined by RFC 2058.
RADSL	Rate Adaptive Digital Subscriber Line. A technique for the use of an existing twisted-pair line that permits simultaneous POTS and high-speed data communication at adaptive symmetric and asymmetric rates.
router	A device that connects LANs by dynamically routing data according to destination and available routes.
routing table	A table used by a node to route traffic to another node in the multiplexer network.
RTU	Remote Termination Unit. A DSL device installed at the customer premises.
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. Protocol for open networking management.
SNMP agent	An application level program that facilitates communication between an SNMP management system and a device. See NMS.
SNMP trap	A message sent to an SNMP manager to notify it of an event, such as a device being reset.
static route	A user-specified permanent entry into the routing table that takes precedence over routes chosen by dynamic routing protocols.
subnet address	The subnet portion of an IP address. In a subnetted network, the host portion of an IP address is split into a subnet portion and a host portion using an address (subnet) mask. This allows a site to use a single IP network address for multiple physical networks.
subnet mask	A number that identifies the subnet portion of a network address. The subnet mask is a 32-bit Internet address written in dotted-decimal notation with all the 1s in the network and subnet portions of the address.

TCP	Transmission Control Protocol. An Internet standard transport layer protocol defined in STD 7, RFC 793. It is connection-oriented and stream-oriented.
Telnet	Virtual terminal protocol in the Internet suite of protocols. Allows the user of one host computer to log into a remote host computer and interact as a normal terminal user of the remote host.
terminal emulation	Software that allows a PC to mimic the signals of a specific type of terminal, such as a VT100 or 3270, to communicate with a device requiring that terminal interface.
TFTP	Trivial File Transfer Protocol. A standard TCP/IP protocol that allows simple file transfer to and from a remote system without directory or file listing. TFTP is used when FTP is not available.
TraceRoute	A program that lists the hosts in the path to a specified destination.
upstream	In the direction of the telephone network.
XTACACS	EXtended Terminal Access Controller Access Control System. A user authentication protocol, it is a Cisco extension of RFC 927.

Index

I

L

M

N

O

P

R

S

T

U