DIGITAL WAN Modular Interface

DELHW-UA
Local Management Guide

DIGITAL WAN Modular Interface

DELHW-UA
Local Management Guide

Part Number: 9032784

October 1998

This guide explains how to manage the DIGITAL DELHW-UA WAN modular interface.

Revision/Update Information: This is a new document.

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL CABLETRON SYSTEMS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

SPECTRUM and **QuickSET** are registered trademarks of Cabletron Systems, Inc.

DIGITAL and the DIGITAL logo are trademarks of Digital Equipment Corporation.

All other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies.

UNITED STATES GOVERNMENT RESTRICTED RIGHTS

The enclosed product (a) was developed solely at private expense; (b) contains “restricted computer software” submitted with restricted rights in accordance with Section 52227-19 (a) through (d) of the Commercial Computer Software - Restricted Rights Clause and its successors, and (c) in all respects is proprietary data belonging to Cabletron and/or its suppliers.

For Department of Defense units, the product is licensed with “Restricted Rights” as defined in the DoD Supplement to the Federal Acquisition Regulations, Section 52.227-7013 (c) (1) (ii) and its successors, and use, duplication, disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at 252.227-7013. Cabletron Systems, Inc., 35 Industrial Way, Rochester, New Hampshire 03867-0505.

FCC Notice — Class A Computing Device:
This equipment generates, uses, and may emit radio frequency energy. The equipment has been type tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules, which are designed to provide reasonable protection against such radio frequency interference. Operation of this equipment in a residential area may cause interference in which case the user at his own expense will be required to take whatever measures may be required to correct the interference. Any modifications to this device - unless expressly approved by the manufacturer - can void the user's authority to operate this equipment under part 15 of the FCC rules.

DOC Notice — Class A Computing Device:
This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la class A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

VCCI Notice — Class A Computing Device:

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Taiwanese Notice — Class A Computing Device:

警告使用者:

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

CE Notice — Class A Computing Device:

Warning!
This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Achtung!
Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

Avertissement!
Cet appareil est un appareil de Classe A. Dans un environnement résidentiel cet appareil peut provoquer des brouillages radioélectriques. Dans ce cas, il peut être demandé à l'utilisateur de prendre les mesures appropriées.

CABLETRON SYSTEMS, INC. PROGRAM LICENSE AGREEMENT

IMPORTANT: Before utilizing this product, carefully read this License Agreement.

This document is an agreement between you, the end user, and Cabletron Systems, Inc. (“Cabletron”) that sets forth your rights and obligations with respect to the Cabletron software program (the “Program”) contained in this package. The Program may be contained in firmware, chips or other media. BY UTILIZING THE ENCLOSED PRODUCT, YOU ARE AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE AND THE LIMITATION OF WARRANTY AND DISCLAIMER OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE UNUSED PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

CABLETRON SOFTWARE PROGRAM LICENSE

1. LICENSE. You have the right to use only the one (1) copy of the Program provided in this package subject to the terms and conditions of this License Agreement.

   You may not copy, reproduce or transmit any part of the Program except as permitted by the Copyright Act of the United States or as authorized in writing by Cabletron.

2. OTHER RESTRICTIONS. You may not reverse engineer, decompile, or disassemble the Program.

3. APPLICABLE LAW. This License Agreement shall be interpreted and governed under the laws and in the state and federal courts of New Hampshire. You accept the personal jurisdiction and venue of the New Hampshire courts.

EXCLUSION OF WARRANTY AND DISCLAIMER OF LIABILITY

1. EXCLUSION OF WARRANTY. Except as may be specifically provided by Cabletron in writing, Cabletron makes no warranty, expressed or implied, concerning the Program (including its documentation and media).

   CABLETRON DISCLAIMS ALL WARRANTIES, OTHER THAN THOSE SUPPLIED TO YOU BY CABLETRON IN WRITING, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE PROGRAM, THE ACCOMPANYING WRITTEN MATERIALS, AND ANY ACCOMPANYING HARDWARE.

2. NO LIABILITY FOR CONSEQUENTIAL DAMAGES. IN NO EVENT SHALL CABLETRON OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR RELIANCE DAMAGES, OR OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THIS CABLETRON PRODUCT, EVEN IF CABLETRON HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, OR ON THE DURATION OR LIMITATION OF IMPLIED WARRANTIES, IN SOME INSTANCES THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU.

DECLARATION OF CONFORMITY

Application of Council Directive(s):	**89/336/EEC** **73/23/EEC**
Manufacturer’s Name:	**Cabletron Systems, Inc.**
Manufacturer’s Address:	**35 Industrial Way** **PO Box 5005** **Rochester, NH 03867**
European Representative Name:	**Mr. J. Solari**
European Representative Address:	**Cabletron Systems Limited** **Nexus House, Newbury Business Park** **London Road, Newbury** **Berkshire RG13 2PZ, England**
Conformance to Directive(s)/Product Standards:	**EC Directive 89/336/EEC** **EC Directive 73/23/EEC** **EN 55022** **EN 50082-1** **EN 60950**
Equipment Type/Environment:	**Networking Equipment, for use in a Commercial or Light Industrial Environment.**

We the undersigned, hereby declare, under our sole responsibility, that the equipment packaged with this notice conforms to the above directives.

Manufacturer	Legal Representative in Europe
Mr. Ronald Fotino	Mr. J. Solari
Full Name	Full Name
Principal Compliance Engineer	Managing Director - E.M.E.A.
Title	Title
Rochester, NH, USA	Newbury, Berkshire, England
Location	Location

CONTENTS

PREFACE

SAFETY

CHAPTER 1 LOCAL MANAGEMENT

CHAPTER 2 MIB NAVIGATOR

CHAPTER 3 ADDITIONAL INFORMATION

INDEX

PREFACE

Welcome to the *DIGITAL WAN Modular Interface DELHW-UA Local Management Guide*. This guide describes how to manage a DELHW-UA and its attached segment through a TELNET connection.

USING THIS GUIDE

A working knowledge of network operations and an understanding of management applications is a prerequisite to using Local Management.

STRUCTURE OF THIS GUIDE

This guide is organized as follows:

Chapter 1, **Local Management**, explains how to access and manage an HSIM and its attached segments through a TELNET connection.

Chapter 2, **MIB Navigator**, explains how to use the MIB Navigator utility. The MIB Navigator allows access to a command set from which you can configure and manage your HSIM.

Chapter 3, **Additional Information**, provides information about frame relay errors.

DOCUMENT CONVENTIONS

Throughout this guide, the following symbols are used to call attention to important information.

Note symbol. Calls the reader’s attention to any item of information that may be of special importance.

Caution symbol. Contains information essential to avoid damage to the equipment.

RELATED DOCUMENTATION

The following manuals may help the user to set up and manage the DELHW-UA:

Use the *DIGITAL DELHW-UA Read Me First!* to set up a computer before beginning the configuration.

Use the *DIGITAL WAN Modular Interface DELHW-UA User’s Guide* to install, configure, and troubleshoot the DELHW-UA.

Use the *DIGITAL WAN Modular Interface DELHW-UA QuickSET Configuration Guide* to configure the DELHW-UA.

Use the *CyberMONITOR User’s Guide* to monitor the WAN using the CyberMONITOR graphical user interface.

Use the appropriate *WPIM Local Management Guide* to connect your DELHW-UA to a WAN using a Telnet connection.

The manuals referenced above can be obtained on the World Wide Web in Adobe Acrobat Portable Document Format (PDF) at the following site:

http://www.networks.digital.com

CORRESPONDENCE

Documentation Comments

If you have comments or suggestions about this manual, send them to DIGITAL Network Products:

Attn.:	Documentation Project Manager
E-MAIL:	doc_quality@lkg.mts.dec.com

World Wide Web

To locate product-specific information, refer to the DIGITAL Network products Home Page on the World Wide Web at the following locations:

North America:	http://www.networks.digital.com
Europe:	http://www.networks.europe.digital.com
Asia Pacific:	http://www.networks.digital.com.au

GETTING HELP

Contact your DIGITAL representative for technical support. Before calling, have the following information ready:

- A description of the failure
- A description of any action(s) already taken to resolve the problem (e.g., changing mode switches, rebooting the unit, etc.)
- A description of your network environment (layout, cable type, etc.)
- Network load and frame size at the time of trouble (if known)
- The device history (i.e., have you returned the device before, is this a recurring problem, etc.)

SAFETY

OVERVIEW

The caution that appears in this guide is defined as follows:

⚠	CAUTION	Contains information essential to avoid damage to the equipment.
	ACHTUNG	Liefert wichtige Informationen, um einen Geräteschaden zu vermeiden.
	ATTENTION	Informations indispensables permettant d'éviter les dommages matériels.
	PRECAUCIÓN	Contiene información esencial para evitar daños al equipo.

SAFETY REQUIREMENTS

The caution that must be observed for the hardware described in this guide is listed below in English, German, French, and Spanish.

⚠	CAUTION	If you edit the super-user community name, be certain you do not forget it. If you do, you cannot perform Local Management functions without returning the device to its factory default configurations. This effectively erases any configuration work you have done.
	ACHTUNG	Stellen Sie sicher, daß Sie den Super-User-Community-Namen nicht vergessen, nachdem Sie ihn geändert haben. Wenn Sie ihn nämlich vergessen, können Sie keine lokalen Verwaltungsfunktionen durchführen, ohne das Gerät auf die Standardkonfiguration des Herstellers zurückzusetzen. Durch das Zurücksetzen werden alle von Ihnen durchgeführten Konfigurationseinstellungen gelöscht.
	ATTENTION	Si vous modifiez le nom de communauté super-user, notez-le pour ne pas l'oublier. Vous ne pourriez en effet plus effectuer de fonctions de gestion locale (Local management), à moins de revenir à la configuration usine, ce qui aurait pour conséquence de supprimer les modifications de configuration que vous auriez pu effectuer.
	PRECAUCIÓN	Si modifica el nombre de la comunidad de superusuarios, téngalo en cuenta y no lo olvide. En tal caso, no podrá hacer uso de las funciones de gestión local sin devolver el dispositivo a su configuración original de fábrica. Si así fuera, se perderá todo el trabajo de configuración que haya realizado.

CHAPTER 1

LOCAL MANAGEMENT

This chapter explains how to access and manage a DELHW-UA and its attached segments through a TELNET connection.

If you have a WPIM installed in your DELHW-UA, refer to the specific WPIM Local Management User’s Guide for information about how to configure your WPIM in a WAN environment.

1.1 CHAPTER ORGANIZATION

The following list shows the organization of this chapter:

- **Local Management Overview** outlines the contents of this chapter, provides an overview of Local Management, and explains how to use the management screens.
- **Accessing Local Management** describes how to access the Main Menu screen and navigate through the Local Management screens.
- **System Level Screen** describes how to use the System Level screen, its functions, and operations.
- **SNMP Community Names Screen** explains how to control access to an DELHW-UA by assigning community names.
- **SNMP Traps Screen** explains how to configure an DELHW-UA to send SNMP traps to multiple network management stations.
- **Flash Download Screen** describes how to download new firmware to an DELHW-UA.
- **Bridge Setup Screen** describes how to configure an DELHW-UA for bridge functions.
- **IP Configuration Screen** describes how to configure an DELHW-UA for IP routing functions.
- **IPX Configuration Screen** describes how to configure an DELHW-UA for IPX routing functions.

1.2 LOCAL MANAGEMENT OVERVIEW

Local Management is a management tool that allows a network manager to perform the following tasks:

- Configure interconnected devices to form a network.
- Monitor the performance of the network.
- Control user access to the network and its components for the purpose of security.

1.2.1 Management Agent

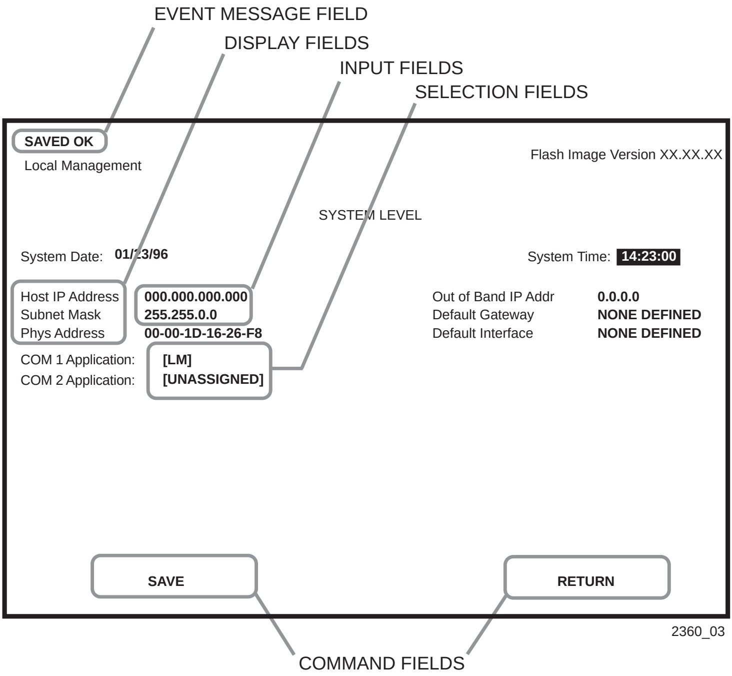
The management agent is a process within the DELHW-UA that collects information about the operational performance of the managed network. Local Management communicates with the management agent for the purpose of issuing management commands to network devices.

1.2.2 Local vs. Remote Management

Network management applications can be defined as either local or remote applications. A Local Management application resides within the DELHW-UA management agent and is accessible via a TELNET connection through the DELHW-UA port of the device. Remote management applications such as Cabletron Systems **SPECTRUM**, **SPECTRUM Element Manager**, or **QuickSET** run in another device that provides management services. This allows you to perform network management and configuration from a remote location.

1.2.3 Local Management Screen Elements

There are five basic field elements, as shown in the Local Management screen in Figure 1-1.



SAVED OK

Local Management

Flash Image Version XX.XX.XX

SYSTEM LEVEL

System Date: **01/23/96**

System Time: **14:23:00**

Host IP Address **000.000.000.000**
Subnet Mask **255.255.0.0**
Phys Address **00-00-1D-16-26-F8**

Out of Band IP Addr **0.0.0.0**
Default Gateway **NONE DEFINED**
Default Interface **NONE DEFINED**

COM 1 Application: **[LM]**
COM 2 Application: **[UNASSIGNED]**

SAVE   RETURN

Figure 1-1 Sample Local Management Screen

The following list explains each of the basic Local Management screen fields:

Event Message Field

This field displays messages that indicate if a Local Management procedure was executed correctly or incorrectly, that changes were saved or not saved to Non-Volatile Random Access Memory (NVRAM), or that a user did not have access privileges to an application.

Table 1-1 describes the most common event messages. Event messages related to specific Local Management applications are described with those applications throughout this manual.

Table 1-1 Event Messages

Message	Meaning
SAVED OK	One or more fields were modified, and saved to NVRAM.
NOT SAVED?--PRESS SAVE TO KEEP CHANGES	One or more fields were modified, but not yet saved to NVRAM.
NOTHING TO SAVE	The SAVE command was executed, but nothing was saved to NVRAM.

Display Fields

Display fields cannot be edited. These fields may display information which never changes, or changes as the result of Local Management operations, user selections, or network monitoring information.

Input Fields

Input fields require keyboard characters to be entered. IP addresses, System Date, and System Time are examples of Input fields.

Selection Fields

Selection fields provide a series of possible values. Only applicable values appear in Selection fields.

Command Fields

Command fields are located at the bottom of Local Management screens. Command fields are used to exit Local Management screens and to save Local Management entries. Command fields perform a management action simply by being selected and activated. **Only command fields can make a change to a device’s configuration.**

1.2.4 Local Management Keyboard Conventions

All key names in this guide display as capital letters. For example, the ENTER key displays as ENTER, the Escape key displays as ESC, and the Backspace key displays as BACKSPACE. Table 1-2 explains the keyboard conventions used in this guide as well as the key functions.

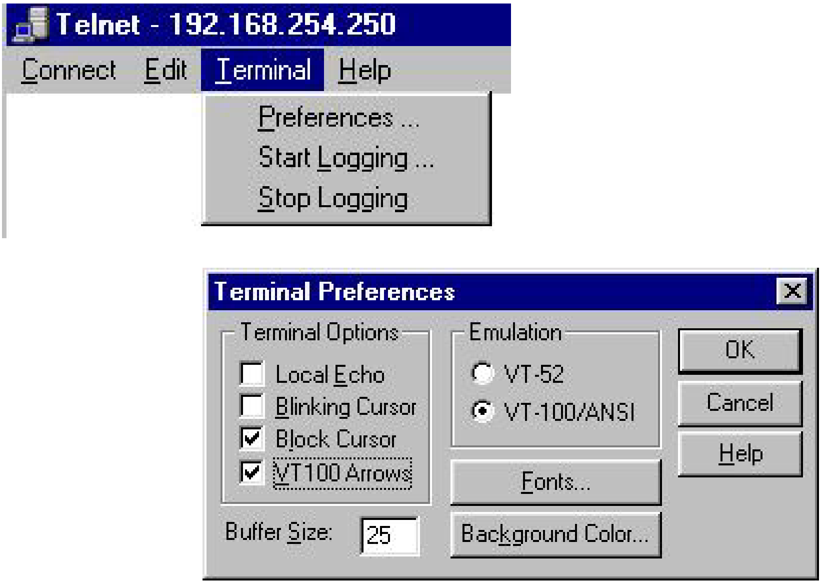
Table 1-2 Keyboard Conventions

Key	Function
ENTER and RETURN	These selection keys perform the same Local Management function. For example, “Press ENTER” means that you can press either ENTER or RETURN, unless this guide specifically instructs you otherwise.
ESC	This key lets you escape from a Local Management screen without saving your changes. For example, “Press ESC twice” means that you must quickly press the ESCAPE key two times to exit the Local Management screen.
SPACE bar and BACKSPACE	These keys cycle through selections in some Local Management fields. Press the SPACE bar to cycle forward through selections and press BACKSPACE to cycle backward through selections.
Arrows	These are navigation keys. Use the UP-ARROW, DOWN-ARROW, LEFT-ARROW, and RIGHT-ARROW keys to move the screen cursor. For example, “Use the arrow keys” means to press whichever arrow key moves the cursor to the desired field on the Local Management screen.
SHIFT-[+/=]	This key combination increments values in some Local Management selection fields. For example, “Press SHIFT-[**+/=**]” means to hold down the SHIFT key while pressing the PLUS/EQUAL key.
[–]	This key decreases values from some Local Management selection fields. For example, “Press [**–**]” means to press the MINUS key.
DEL	The DEL (Delete) key removes characters from a Local Management Selection field. For example, “Press DEL” means to press the DELETE key.

You can use QuickSET to initiate a TELNET session if you have no other TELNET application. Your PC's arrow keys are used extensively to navigate within TELNET screens. In order to use the arrow keys effectively for navigating within Local Management screens, you must set your PC up to emulate a Digital Equipment Corporation VT52 terminal.

Start QuickSET and click the **NEXT** button on the first two windows. Under the **File** menu on the title bar of the third window, select **Telnet**. In the title bar of the first Telnet screen, click on **Terminal** and the Terminal menu will display as shown below in Figure 1-2.

Click on **Preferences** in the Terminal menu, and the Terminal Preferences window will display as shown below in Figure 1-2.



Terminal Options
- □ Local Echo
- □ Blinking Cursor
- ☑ Block Cursor
- ☑ VT100 Arrows

Emulation
- ○ VT-52
- ● VT-100/ANSI

Buffer Size: 25

Figure 1-2 Terminal Menu and Terminal Preferences

Select **VT100 Arrows** in the Terminal Options panel, and then select **VT100/ANSI** in the emulation panel if it is not already selected. Click **OK** when you have finished. You are now ready to navigate within any of the Local Management screens.

1.2.5 Navigating Within Local Management Screens

To navigate within a Local Management screen, use the arrow keys of the terminal or the workstation providing terminal emulation services. The Local Management screen cursor responds to the LEFT-ARROW, RIGHT-ARROW, UP-ARROW, and DOWN-ARROW keys. Each time you press an arrow key, the Local Management screen cursor moves to the next available field in the direction of the arrow key.

The Local Management screen cursor only moves to fields which can be selected or used for input. This means that the cursor jumps over display fields and empty lines on the Local Management screen.

The Local Management screen cursor provides wrap-around operation. This means that a cursor located at the edge of a screen, when moved in the direction of that edge, “wraps around” to the outermost selectable item on the opposite side of the screen which is on the same line or column.

1.2.5.1 Selecting Local Management Menu Screen Items

To select items in a Local Management menu screen, follow these steps:

1. Use the arrow keys to highlight a menu item.

2. Press **ENTER**. The selected Local Management menu screen displays.

1.2.5.2 Exiting Local Management Screens

To exit any of the Local Management screens, follow these steps:

1. Use the arrow keys to highlight the **RETURN** command at the bottom of the Local Management screen.

2. Press **ENTER**. The previous screen in the Local Management hierarchy displays.

You can also exit Local Management screens by pressing ESC twice. **This exit method does not warn you about unsaved changes and all unsaved changes are lost**.

1.2.5.3 Exiting the Local Management Session

To exit from DELHW-UA Local Management, perform the following steps:

1. Use the arrow keys to highlight the **RETURN** command at the bottom of the Local Management screen.
2. Press ENTER. The previous screen in the Local Management hierarchy displays.
3. Repeat steps 1 and 2 until the Main Menu screen displays.
4. Use the arrow keys to highlight the **EXIT** command at the bottom of the Main Menu screen.
5. Press **ENTER**. The DELHW-UA Local Management Password screen displays and the Local Management session ends.

1.2.6 Establishing a TELNET Connection

The DELHW-UA is shipped with a temporary IP Address of **192.168.254.254** so that your computer can communicate with it over your Local Area Network (LAN) through a TELNET connection. However, to establish a TELNET connection, your computer must be on the same subnet as the DELHW-UA. DIGITAL recommends that you assign a temporary IP Address of **192.168.254.253** to your computer to ensure that both devices are on the same subnet. TELNET connections to the host device require the community name passwords assigned at the SNMP Community Names screen or if you are doing an initial configuration, you can use the default password, **public**.

See the instructions included with the TELNET application for information about establishing a TELNET session.

1.2.7 Local Management Screen Hierarchy

Local Management consists of a series of menu screens that provide a path to each of the Local Management function screens. Navigate through Local Management by selecting items from the menu screen. Figure 1-3 shows the hierarchy of the Local Management screens.

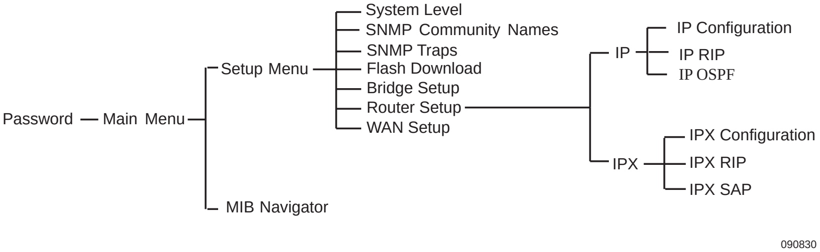


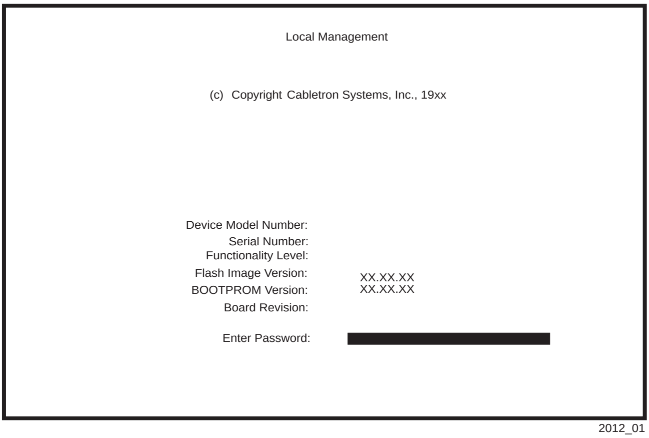
Figure 1-3 Hierarchy of Local Management Screens

1.3 ACCESSING LOCAL MANAGEMENT

This section explains how to access and use the Local Management menu screens. Menu screens provide a path to the setup and status screens.

1.3.1 Using the Menu Screens

Once you have accessed the DELHW-UA through a TELNET connection, the Password screen, shown in Figure 1-4, displays.



```
                    Local Management

      (c)  Copyright Cabletron Systems, Inc., 19xx



  Device Model Number:
        Serial Number:
    Functionality Level:
   Flash Image Version:     XX.XX.XX
     BOOTPROM Version:      XX.XX.XX
        Board Revision:

       Enter Password:
```

2012_01

Figure 1-4 Password Screen

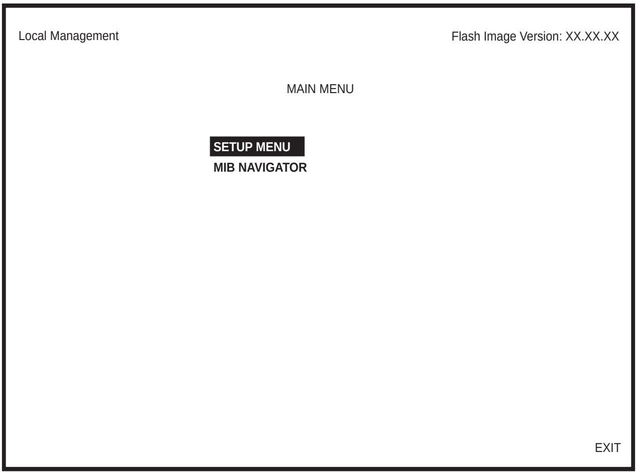
Type in your password and press ENTER. If you are doing an initial configuration, you can type the default super-user access password "*public*" or just press ENTER.

Your password is one of the community names specified in the SNMP Community Names screen. Access to certain Local Management capabilities depends on the degree of access accorded that community name. See the SNMP Community Names section.

- If you enter a valid password, the associated access level displays at the bottom of the screen and the Main Menu screen, shown in Figure 1-5, on the following page, displays.
- If you enter an invalid password, the cursor returns to the beginning of the password entry field.
- If no activity occurs for several minutes, the Password screen displays again, ending your current session. You must reenter the password to perform Local Management tasks.

1.3.2 Main Menu Screen

The Main Menu screen, as shown in Figure 1-5, is the starting point from which all the Local Management screens are accessed.



2012_02

Figure 1-5 Main Menu Screen

The Main Menu screen displays the following menu items:

Setup Menu

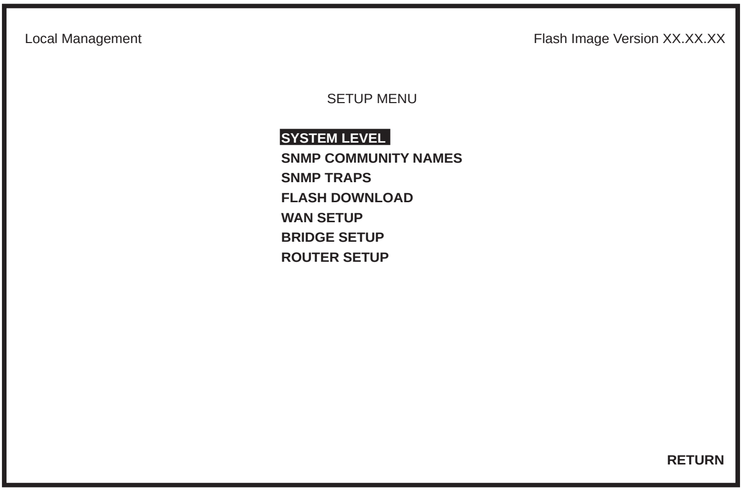
The Setup Menu provides access to Local Management screens that are used to configure the DELHW-UA.

MIB Navigator

The MIB Navigator is a Local Management utility that lets you access, monitor, and set specific Management Information Base (MIB) items within the DELHW-UA.

Setup Menu Screen

The Setup Menu screen provides access to the Local Management screens that are used to configure the DELHW-UA. Examples of functions accessible through the Setup Menu include configuring the host IP address and Subnet Mask, assigning the SNMP community names, and configuring the SNMP trap notification. Figure 1-6 shows the Setup Menu screen.



```
Local Management                                    Flash Image Version XX.XX.XX

                               SETUP MENU

                           SYSTEM LEVEL
                           SNMP COMMUNITY NAMES
                           SNMP TRAPS
                           FLASH DOWNLOAD
                           WAN SETUP
                           BRIDGE SETUP
                           ROUTER SETUP






                                                                      RETURN
```

2012_03

Figure 1-6 Setup Menu Screen

The Setup Menu screen displays the following menu items:

System Level

The System Level screen allows you to configure basic operating parameters for the DELHW-UA.

SNMP Community Names

The SNMP Community Names screen allows you to change or review the community names used as access passwords for local management operation.

SNMP Traps

The SNMP Traps screen provides display and configuration access to the table of IP addresses used for trap destinations and associated community names.

Flash Download

The Flash Download screen lets you download a firmware image from a TFTP server to the DELHW-UA.

WAN Setup – The WAN Setup menu item accesses two other screens that provide WAN physical configuration and WAN Interface configuration access to enable a WAN link to be set up.

Bridge Setup

The Bridge Setup screen lets you select a Spanning Tree protocol and enable/disable switch ports.

Router Setup

The Router Setup screen accesses two other screens that provide general IP or IPX routing configuration and allow you to enable or disable the Routing Information Protocol (RIP) and the Service Advertising Protocol (SAP) features.

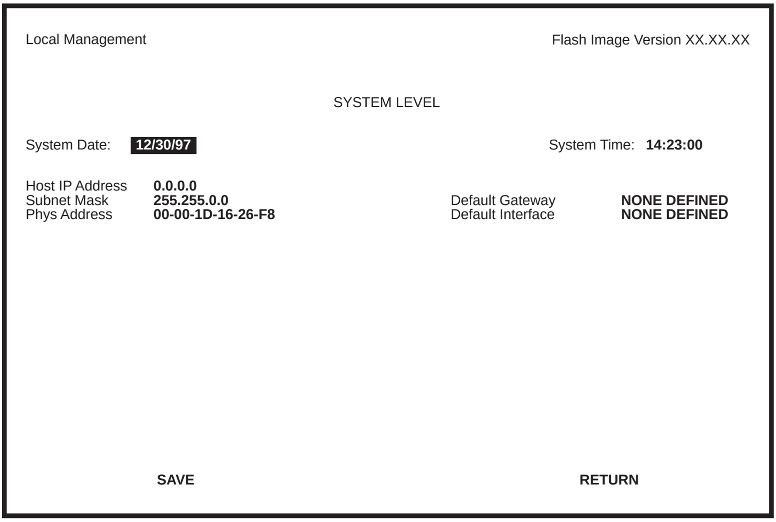
If you have a DELT1-UI a installed in your DELHW-UA, refer to the WAN Setup section of this chapter for configuration information. For all other WPIMs, refer to your specific WPIM(s) Local Management Guide for information on configuring the DELHW-UA for a Wide Area Network Interface.

1.4 SYSTEM LEVEL SCREEN

The System Level screen displays the physical address (MAC address) of the DELHW-UA and allows you to set the following parameters:

- System Date
- System Time
- Host IP Address
- Subnet Mask
- Physical Address
- Default Gateway
- Default Interface

Access the System Level screen (Figure 1-7) from the Setup Menu screen by using the arrow keys to highlight the **System Level** option and pressing ENTER. The System Level screen displays.



```
Local Management                                        Flash Image Version XX.XX.XX

                                  SYSTEM LEVEL

System Date:   12/30/97                                 System Time:   14:23:00

Host IP Address   0.0.0.0
Subnet Mask       255.255.0.0                  Default Gateway     NONE DEFINED
Phys Address      00-00-1D-16-26-F8            Default Interface   NONE DEFINED
```

2012_04

Figure 1-7 System Level Screen

The following definitions explain each System Level screen field. The sections which follow these definitions explain the use of these fields.

System Date

Use this field to enter the system date, as described in Setting the System Date.

System Time

Use this field to enter the system time, as described in Setting the System Time.

Host IP Address

Use this field to enter the IP address of the DELHW-UA, as described in Setting the Host IP Address.

Subnet Mask

This field displays the default Subnet Mask, and allows you to enter a new value for the Subnet Mask if necessary. Subnets are logical divisions of the network that isolate groups of devices. The Subnet Mask determines how the DELHW-UA directs SNMP traps to a management workstation. If the DELHW-UA resides on the same network as the management workstation, then the DELHW-UA sends SNMP traps directly to the management workstation. If the DELHW-UA resides on a different subnet as the management workstation, then the DELHW-UA sends SNMP traps to a gateway or router.

- When the management workstations designated to receive SNMP traps reside on the same network as the DELHW-UA, use the Subnet Mask default setting for the IP address entered on the System Level screen.
- Set a new value for the Subnet Mask when the management workstations designated to receive SNMP traps reside on a different subnet (for example, across a gateway or router).

To set a Subnet Mask, refer to the Setting the Subnet Mask section.

Phys Address

This field displays the physical address of the DELHW-UA. You cannot modify the physical address.

Default Gateway

Use this field to enter the Default Gateway for the DELHW-UA. When routing packets, the DELHW-UA uses the IP Forwarding Table to find the route to each destination address. The IP Forwarding Table contains the routes to all networks and hosts within a certain area. However, the IP Forwarding Table on its own cannot provide all of the routes that may be needed. The DELHW-UA relies on a Default Gateway to provide the routes to destinations that are not listed in its own IP Forwarding Table. The Default Gateway is the IP address of the network device (gateway or router) used to forward SNMP traps to a management station. The default setting for this field is NONE DEFINED. To set the Default Gateway, refer to Setting the Default Gateway.

Default Interface

Use this field to select the default interface for the DELHW-UA Default Gateway. The default interface is the channel which is set up to handle SNMP traps sent to an IP station that is not on the same subnet as the DELHW-UA in an IP routed environment. The default setting for this field is NONE DEFINED. To set the default interface for the Default Gateway of the DELHW-UA , refer to Setting the Default Interface.

1.4.1 Setting the System Date

The DELHW-UA is year 2000 compliant so that the System Date field can be set beyond the year 1999. To set the system date, perform the following steps:

1. Use the arrow keys to highlight the **System Date** field.

2. Enter the date in an MM/DD/YYYY format.

When entering the date in the system date field, you do not need to add separators between month, day, and year numbers, as long as the entire entry uses eight decimal numbers. For example, to set the date to 03/17/1997, type “03171997” in the System Date field.

3. Press ENTER to set the system date.

4. Use the arrow keys to highlight the **SAVE** command at the bottom of the screen and press ENTER.

If the date entered was a valid format, the Event Message field at the top of the screen displays “SAVED OK”. If the entry was not valid, Local Management does not alter the current value and refreshes the System Date field with the previous value.

1.4.2 Setting the System Time

To set the system time, perform the following steps:

1. Use the arrow keys to highlight the **System Time** field.
2. Enter the time in a 24-hour format, HH:MM:SS.

When entering the time in the system time field, you do not need to add separators between hours, minutes, and seconds, as long as each entry uses two decimal numbers. For example, to set the time to 6:45 a.m., type “064500” in the System Time field.

3. Press ENTER to set the system time.
4. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and press ENTER. If the time entered was a valid format, the Event Message field at the top of the screen displays “SAVED OK”. If the entry was not valid, Local Management does not alter the current value and refreshes the System Time field with the previous value.

1.4.3 Setting the Host IP Address

To set the host IP address, perform the following steps:

1. Use the arrow keys to highlight the **Host IP Address** field.
2. Enter the IP address using Decimal Dotted Notation (DDN) format.

   For example: 168.192.25.17
3. Press ENTER. If the IP address entered was a valid format, the cursor returns to the beginning of the Host IP Address field. If the entry was not valid, the Event Message field displays “INVALID IP ADDRESS OR FORMAT ENTERED”. Local Management does not alter the

current value and refreshes the Host IP Address field with the previous value.

4. Use the arrow keys to highlight the **SAVE** command field.

5. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.

1.4.4 Setting the Subnet Mask

Subnets are logical divisions of the network. To change the Subnet Mask from its default value, perform the following steps:

1. Use the arrow keys to highlight the **Subnet Mask** field.

2. Enter the Subnet Mask using Dotted Decimal Notation (DDN) format. Values for each decimal can be from 0 to 255.

   For example: 255.255.0.0

3. Press ENTER. If the Subnet Mask entered was a valid format, the cursor returns to the beginning of the Subnet Mask field. If the entry was not valid, the Event Message field displays “INVALID SUBNET MASK OR FORMAT ENTERED”. Local Management does not alter the current value and refreshes the Subnet Mask field with the previous value.

4. Use the arrow keys to highlight the **SAVE** command field.

5. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.

1.4.5 Setting the Default Gateway

To set the Default Gateway, perform the following steps:

1. Use the arrow keys to highlight the **Default Gateway** field.

2. Enter the IP address of the Default Gateway using DDN format.

   For example: 168.192.79.121

3. Press ENTER. If the Default Gateway address entered was a valid format, the cursor returns to the beginning of the Default Gateway field. If the entry was not valid, the Event Message field displays

“INVALID DEFAULT GATEWAY OR FORMAT ENTERED”. Local Management does not alter the current value and refreshes the Default Gateway field with the previous value.

4. Use the arrow keys to highlight the **SAVE** command field.
5. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.

1.4.6 Setting the Default Interface

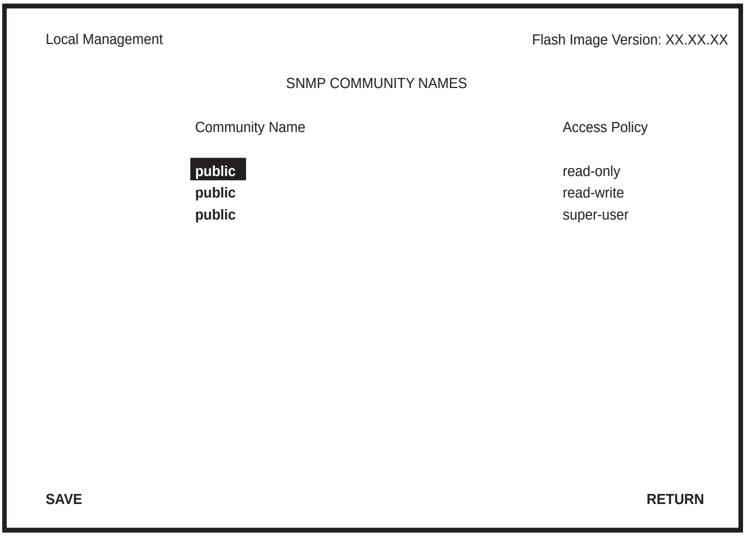
To set the default interface, perform the following steps:

1. Use the arrow keys to highlight the **Default Interface** field.
2. Enter the interface number for the Default Gateway in this field.
3. Press ENTER. If the interface entered was a valid format, the cursor returns to the beginning of the Subnet Mask field. If the entry was not valid, the Event Message field displays “PERMISSIBLE RANGE: 1...1”. Local Management does not alter the current value and refreshes the Default Interface field with the previous value.
4. Use the arrow keys to highlight the **SAVE** command field.
5. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.

1.5 SNMP COMMUNITY NAMES SCREEN

This section explains how to assign community names. Community names allow you to control Local Management access by establishing three passwords. Each password controls a different level of access to DELHW-UA Local Management.

Access the SNMP Community Names screen, shown in Figure 1-8, from the Setup Menu screen by using the arrow keys to highlight the **SNMPCommunity Names** option and pressing ENTER. The SNMP Community Names screen displays.



```
Local Management                                          Flash Image Version: XX.XX.XX

                              SNMP COMMUNITY NAMES

                Community Name                            Access Policy

                public                                    read-only
                public                                    read-write
                public                                    super-user
```

2012_05

Figure 1-8 SNMP Community Names Screen

1.5.1 Community Name Access Policy

To perform any operations on the SNMP Community Names screen, you must have used the superuser community name at the User Password prompt when initiating the Local Management session. The default community name for each access level is *public. If you wish to use the default, you can type public, or just* press ENTER.

The following explains each of the SNMP Community Names screen fields:

Community Name

Displays the user-defined names through which a user accesses the DELHW-UA Local Management. Any community name entered here acts as a password to Local Management.

Access Policy

Indicates the access status accorded each community name. Possible status conditions are:

- **read-only -** This access level allows reading of device parameters not including community names.
- **read-write -** This access level allows editing of some device configuration parameters not including changing or viewing community names.
- **superuser -** This access level allows full management privileges.

1.5.2 Setting SNMP Community Names

To set a community name, perform the following steps:

If you edit the super-user community name, be certain you do not forget it. If you do, you cannot perform Local Management functions without returning the device to its factory default configurations. This effectively erases any configuration work you have done.

1. Use the arrow keys to highlight the community name you want to change.

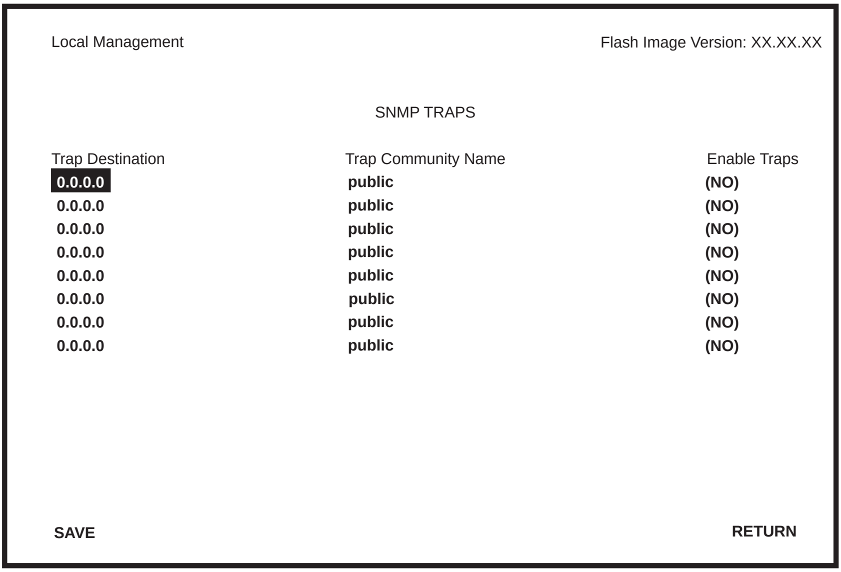
2. Type the new community name and press ENTER. The old community name is replaced by the new community name.

3. Use the arrow keys to highlight the **SAVE** command field.

4. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.

1.6 SNMP TRAPS SCREEN

The SNMP Traps screen, shown in Figure 1-9, allows the user to configure the DELHW-UA to send traps to as many as eight remote management workstations. SNMP traps are messages about network events and device operational statistics. Access the SNMP Traps screen from the Setup Menu screen by using the arrow keys to highlight the **SNMP Traps** option and pressing ENTER. The SNMP Traps screen displays.



```
Local Management                                           Flash Image Version: XX.XX.XX

                                  SNMP TRAPS

Trap Destination             Trap Community Name                      Enable Traps
0.0.0.0                      public                                   (NO)
0.0.0.0                      public                                   (NO)
0.0.0.0                      public                                   (NO)
0.0.0.0                      public                                   (NO)
0.0.0.0                      public                                   (NO)
0.0.0.0                      public                                   (NO)
0.0.0.0                      public                                   (NO)
0.0.0.0                      public                                   (NO)




SAVE                                                                  RETURN
```

2012_06

Figure 1-9 SNMP Traps Screen

1.6.1 Trap Table Screen Fields

The following definitions explain each of the SNMP Traps screen fields:

Trap Destination

Use this field to enter the IP address of the management workstation designated to receive SNMP traps from the DELHW-UA.

Trap Community Name

Use this field to enter the community name of the management workstation with the associated IP address. The community name indicates the "access level" of traps that will be forwarded to the Trap destination.

Enable Traps

Use this field to enable the transmission of SNMP traps to the management workstation.

1.6.2 Setting the SNMP Trap Destination

Each management workstation designated to receive SNMP traps from the DELHW-UA must have a valid IP address and community name. To set and enable SNMP trap destination, perform the following steps:

1. Use the arrow keys to highlight the **Trap Destination** field that you want to modify.
2. Type the IP address of the management workstation designated to receive SNMP traps from the DELHW-UA. This address must be entered in DDN format.

   For example: 168.192.25.17
3. Press ENTER. If the IP address entered was a valid format, the cursor returns to the beginning of the Trap Destination IP address field. If the entry was not valid, the Event Message field displays "INVALID IP ADDRESS OR FORMAT ENTERED". Local Management does not alter the current value and refreshes the Trap Destination IP address field with the previous value.
4. Use the arrow keys to highlight the **Trap Community Name** field (on the same row as the Trap Destination field).
5. Type the community name of the management workstation. The community name indicates the "access level" of traps that will be forwarded to the Trap destination.
6. Press ENTER.
7. Use the arrow keys to highlight the **Enable Traps** field (on the same row as the Trap Destination and Trap Community Name you have just configured). The default setting for this field is **NO**.

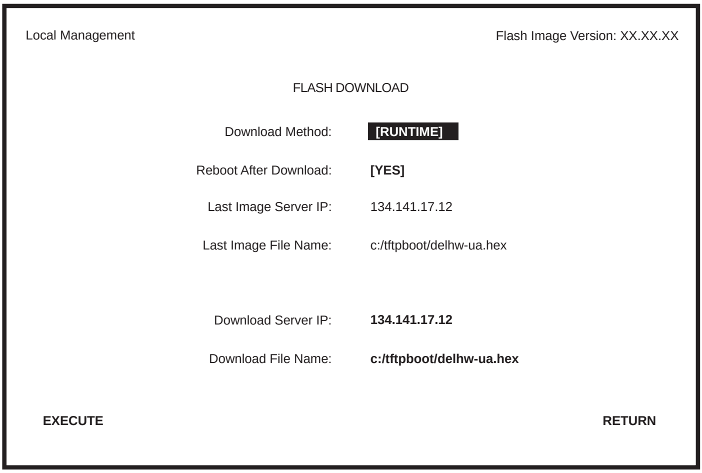
8. Press the SPACE bar or BACKSPACE to set the field to **YES**.
9. Use the arrow keys to highlight the **SAVE** command field.
10. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.
11. Repeat this procedure as necessary to set each Trap Destination.

1.7 FLASH DOWNLOAD SCREEN

The Flash Download screen (Figure 1-10) allows you to download a firmware image from a TFTP server to the DELHW-UA.

Access the Flash Download screen from the Setup Menu screen by using the arrow keys to highlight the **Flash Download** option and pressing ENTER. The Flash Download screen, shown in Figure 1-10, displays.

Flash download operations require a properly named download file and a properly configured download server.



```
Local Management                                  Flash Image Version: XX.XX.XX

                              FLASH DOWNLOAD

              Download Method:   [RUNTIME]

        Reboot After Download:   [YES]

         Last Image Server IP:   134.141.17.12

        Last Image File Name:    c:/tftpboot/delhw-ua.hex


          Download Server IP:    134.141.17.12

          Download File Name:    c:/tftpboot/delhw-ua.hex


  EXECUTE                                                          RETURN
```

2012_07

Figure 1-10 Flash Download Screen

The following definitions explain each of the Flash Download screen fields.

Download Method

Use this field to select the method you wish to use to download the firmware image to the DELHW-UA.

- **Reboot After Download —** This field displays when the **RUNTIME** Download Method is chosen. Selecting **YES** forces the DELHW-UA to reboot and use the new firmware image immediately. Selecting **NO** allows the DELHW-UA to continue using the existing firmware image without interrupting network operation.
- **Commit to Flash —** This field displays when the **BOOTPROM** Download Method is chosen. Selecting **YES** allows the DELHW-UA to continue using the existing firmware image without interrupting network operation and selecting **NO** allows the DELHW-UA to reboot and use the new firmware image immediately.
- **TFTP Gateway Server IP —** This field displays when the **BOOTPROM** Download Method is chosen. Use this field to enter the IP address of the TFTP Gateway Server.

Last Image Server IP

Displays the IP address of the last server used to download a firmware image to the DELHW-UA.

Last Image File Name

Displays the file name of the last firmware image downloaded to the DELHW-UA.

Download Server IP

Use this field to type in the IP address of the server from which you wish to download the firmware image.

Download File Name

Use this field to type in the file name of the firmware image you wish to download to the DELHW-UA.

1.7.1 Selecting a Flash Download Method

1. Use the arrow keys to highlight the **Download Method** field.

2. Press the SPACE bar or BACKSPACE to select a flash download method.

- If you select **RUNTIME**, the **Reboot After Download** field displays.
- If you select **BOOTPROM**, the **Commit to Flash** field and the **TFTP Gateway Server IP** field display.

1.7.1.1 RUNTIME Download

If you select **RUNTIME Download**, perform the following steps:

1. Use the arrow keys to highlight the **Reboot After Download** field.

2. Press the SPACE bar or BACKSPACE to select one of the following:

- **YES**, if you want the DELHW-UA to reboot and use the new firmware image immediately.
- **NO**, if you want the DELHW-UA to continue using the existing firmware image without interrupting network operation. The DELHW-UA stores the new firmware image in flash memory. When you reset the DELHW-UA, it boots from flash memory using the new image.

3. Use the arrow keys to highlight the **Download Server IP** field.

4. Type the IP address of the download server and press ENTER.

5. Use the arrow keys to highlight the **Download File Name** field.

6. Type the complete path and filename of the new image file to be downloaded. You must include all directories and subdirectories involved in accessing the file. Type the new entry over the previous entry.

7. Press ENTER.

8. Use the arrow keys to highlight the **EXECUTE** command located at the bottom of the Flash Download screen.

9. Press ENTER to begin the download. The DELHW-UA attempts to download the file using the IP address, filename, and path provided. This file is assigned to the Flash memory of the DELHW-UA.

1.7.1.2 BOOTPROM Download

If you select a **BOOTPROM Download**, perform the following steps:

1. Use the arrow keys to highlight the **Commit to Flash** field.

2. Press the SPACE bar or BACKSPACE to select one of the following:

- **YES**, if you want the DELHW-UA to continue using the existing firmware image without interrupting network operation. The DELHW-UA stores the new firmware image in flash memory. When you reset the DELHW-UA, it boots from flash memory using the new image.
- **NO**, if you want the DELHW-UA to reboot and use the new firmware image immediately.

3. Use the arrow keys to highlight the **Download Server IP** field.

4. Type the IP address of the download server and press ENTER.

5. Use the arrow keys to highlight the **Download File Name** field.

6. Type the complete path and filename of the new image file to be downloaded. You must include all directories and subdirectories involved in accessing the file. Type the new entry over the previous entry.

7. Press ENTER.

8. Use the arrow keys to highlight the **TFTP Gateway Server IP** field.

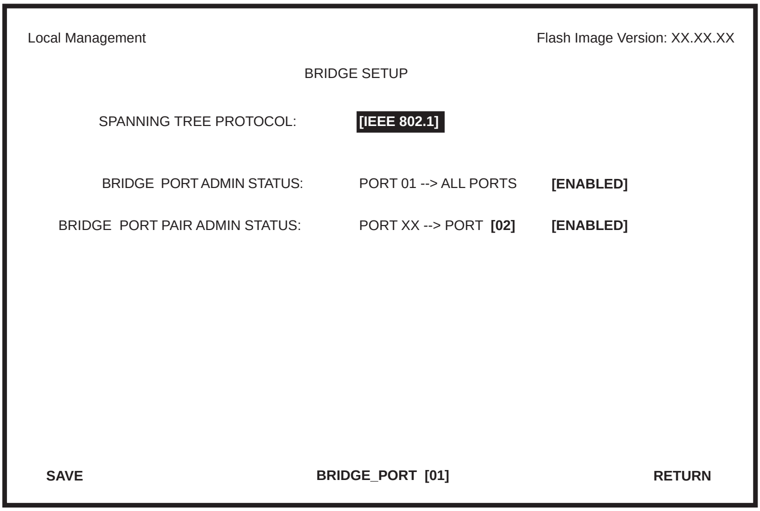
9. Enter the IP address of the TFTP gateway server.

10. Use the arrow keys to highlight the **EXECUTE** command located at the bottom of the Flash Download screen. The DELHW-UA attempts to download the file using the IP address, filename, and path provided. This file is assigned to the Flash memory of the DELHW-UA.

1.8 BRIDGE SETUP SCREEN

The Bridge Setup screen enables you to select a Spanning Tree protocol and enable/disable bridge ports.

Access the Bridge Setup screen, shown in Figure 1-11, by using the arrow keys to highlight the **Bridge Setup** option and pressing ENTER. The Bridge Setup screen displays.



```
Local Management                                                    Flash Image Version: XX.XX.XX

                                     BRIDGE SETUP

          SPANNING TREE PROTOCOL:             [IEEE 802.1]

          BRIDGE  PORT ADMIN STATUS:          PORT 01 --> ALL PORTS      [ENABLED]

     BRIDGE  PORT PAIR ADMIN STATUS:          PORT XX --> PORT  [02]     [ENABLED]






   SAVE                              BRIDGE_PORT  [01]                              RETURN
```

2012_08

Figure 1-11 Bridge Setup Screen

1.8.1 Bridge Setup Screen Fields

The following list describes each of the Bridge Setup screen fields:

Spanning Tree Protocol

Use this field to select a Spanning Tree protocol. Possible selections for this field are IEEE 802.1, DEC, or NONE.

Bridge Port Admin Status

Use this field to enable or disable individual DELHW-UA bridge ports. Possible selections for this field are ENABLED or DISABLED.

Bridge Port Pair Admin Status

Use this field to enable or disable bridging between bridge port pairs. For example, you can enable Port 1 to bridge traffic to all ports except Port 2.

Bridge_Port X

Use this command field to select the DELHW-UA bridge port you want to configure.

1.8.2 Selecting a Spanning Tree Protocol

To select the Spanning Tree protocol to be used by the DELHW-UA, perform the following steps:

1. Use the arrow keys to highlight the **SPANNING TREE PROTOCOL** field.

2. Press the SPACE bar or BACKSPACE to select **[IEEE 802.1]**, **[DEC]**, or **[NONE]**.

3. Use the arrow keys to highlight the **SAVE** command field.

4. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.

1.8.3 Selecting the Bridge Port Administrative Status

To select the bridge port administrative status, perform the following steps:

1. Use the arrow keys to highlight the **[BRIDGE_PORT *XX*]** field at the bottom of the Bridge Setup screen.

2. Press the SPACE bar or BACKSPACE to select the bridge port you want to configure. The selected bridge port displays in the **Bridge Port Admin Status** field.

3. Use the arrow keys to highlight the **BRIDGE PORT ADMIN STATUS: PORT X - - > ALL PORTS [ENABLED]** field.

4. Press the SPACE bar or BACKSPACE to select **ENABLE** or **DISABLE**.

For example, the following bridge setup indicates that bridge port 01 is configured to bridge traffic to all ports:

BRIDGE PORT ADMIN STATUS: PORT **01 - -** > ALL PORTS **[ENABLED]**

5. Use the arrow keys to highlight the **SAVE** command field.
6. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.

1.8.4 Selecting the Bridge Port Pair Administrative Status

To select the bridge port pair administrative status, perform the following steps:

1. Use the arrow keys to highlight the **[BRIDGE_PORT *XX*]** field at the bottom of the Bridge Setup screen.
2. Press the SPACE bar or BACKSPACE to select the bridge port you want to configure. The selected bridge port displays in the **Bridge Port Pair Admin Status** field.
3. Use the arrow keys to highlight the **BRIDGE PORT PAIR ADMIN STATUS: PORT X - -> PORT [Y]** field.
4. Press the SPACE bar or BACKSPACE to select the port you want to enable or disable bridge traffic.
5. Use the arrow keys to highlight the **BRIDGE PORT PAIR ADMIN STATUS: PORT X - -> PORT [Y] [ENABLED]** field.
6. Press the SPACE bar or BACKSPACE to select **ENABLE** or **DISABLE**.

   For example, the following bridge setup indicates that bridge port 01 is configured NOT to bridge traffic to bridge port 02:

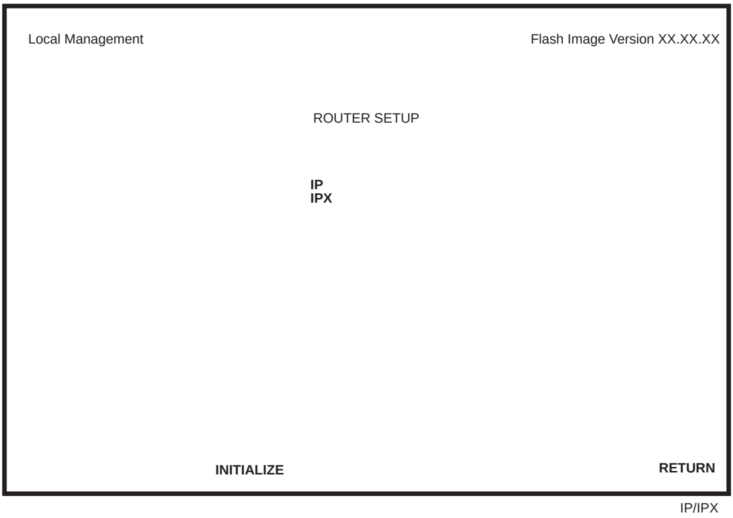
   BRIDGE PORT PAIR ADMIN STATUS: PORT **01 - -** > PORT **[02] [DISABLED]**

7. Use the arrow keys to highlight the **SAVE** command field.
8. Press ENTER. The Event Message field at the top of the screen displays “SAVED OK”.

1.9 ROUTER SETUP SCREEN

The Router Setup screen allows you to choose either IP or IPX routing for your DELHW-UA.

Access the Router Setup screen, shown in Figure 1-12, by using the arrow keys to highlight the **ROUTER SETUP** menu item in the Setup Menu and pressing ENTER. The Router Setup screen displays.



Local Management

Flash Image Version XX.XX.XX

ROUTER SETUP

IP
IPX

Figure 1-12 Router Setup Screen

1.9.1 Router Setup Fields

The following list describes the Router Setup fields.

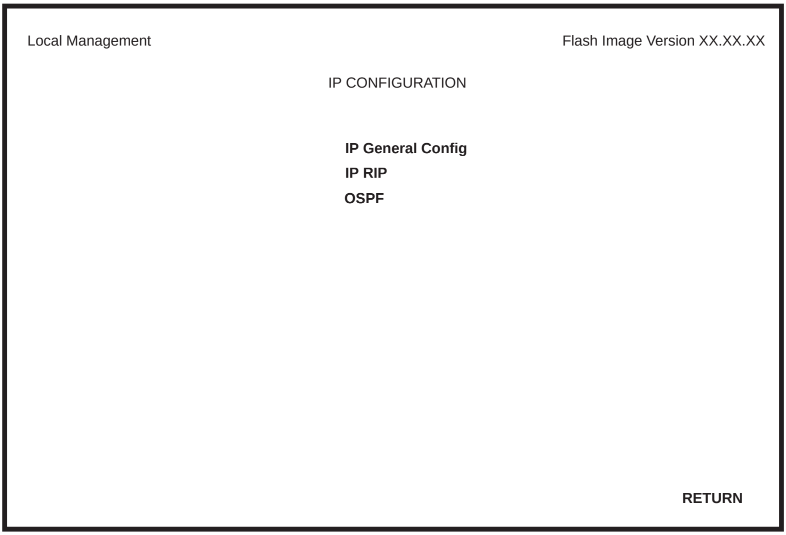
IP
Use this field to access the IP Configuration screen to configure the DELHW-UA for IP routing.

IPX
Use this field to access the IPX Configuration screen to configure the DELHW-UA for IPX routing.

1.10 IP CONFIGURATION SCREEN

The IP Configuration screen enables you to access the IP General Config and IP RIP screens to configure the DELHW-UA for IP Routing and enable RIP on the DELHW-UA.

Access the IP Configuration screen, shown in Figure 1-13, by using the arrow keys to highlight the **IP** menu item on the Router Setup screen and pressing ENTER. The IP Configuration screen displays.



2012_09

Figure 1-13 IP Configuration Screen

1.10.1 IP Configuration Screen Fields

The following list describes each of the IP Configuration screen fields.

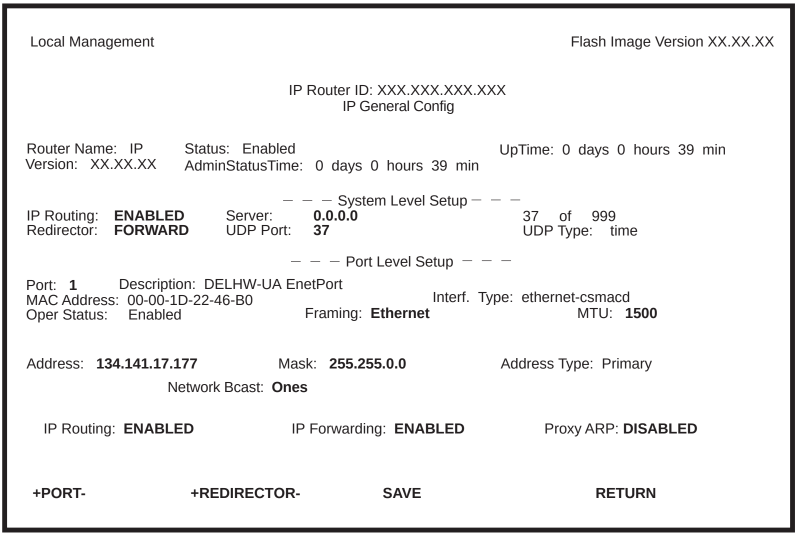
IP General Config
Use this field to access the IP General Config screen and configure the DELHW-UA for IP routing.

IP RIP
Use this field to access the IP RIP screen and enable Routing Information Protocol (RIP) routing on the DELHW-UA.

1.10.2 IP General Config Screen

The IP General Config screen allows you to configure the DELHW-UA for IP routing.

Access the IP General Config screen by using the arrow keys to highlight the **IP General Config** menu item and pressing ENTER. The IP General Config screen shown in Figure 1-14 displays.



```
 Local Management                                                       Flash Image Version XX.XX.XX

                                    IP Router ID: XXX.XXX.XXX.XXX
                                          IP General Config

 Router Name:   IP       Status:   Enabled                              UpTime:  0  days  0  hours  39  min
 Version:   XX.XX.XX     AdminStatusTime:   0  days  0  hours  39  min

                                   — — — System Level Setup — — —
 IP Routing:   ENABLED       Server:        0.0.0.0                          37    of    999
 Redirector:   FORWARD       UDP Port:      37                               UDP Type:    time

                                    — — — Port Level Setup — — —
 Port:   1         Description:  DELHW-UA EnetPort
 MAC Address:  00-00-1D-22-46-B0                        Interf.  Type:  ethernet-csmacd
 Oper Status:     Enabled               Framing:  Ethernet                   MTU:   1500


 Address:   134.141.17.177            Mask:   255.255.0.0              Address Type:  Primary
                         Network Bcast:  Ones

   IP Routing:  ENABLED                 IP Forwarding:  ENABLED              Proxy ARP: DISABLED


  +PORT-                 +REDIRECTOR-            SAVE                          RETURN
```

2012_11

Figure 1-14 IP General Config Screen

1.10.3 IP General Configuration Status Fields

The following list describes each of the IP General Config status fields. The status fields are for informational purposes only and cannot be modified.

Router Name
Displays the type of routing used.

Status
Displays the status of IP Routing.

UpTime
Displays the amount of time elapsed since the last time the DELHW-UA was rebooted.

Version
Displays the IP Routing version number used on the DELHW-UA.

AdminStatusTime
Displays the amount of time elapsed since an IP address was assigned to the DELHW-UA.

UDP Type
Displays the User Datagram Protocol (UDP) Service to which the selected UDP Port number corresponds.

Description
Describes the selected Port.

MAC Address
Displays the physical (MAC) address of the DELHW-UA.

Interf. Type
Displays the type of interface used by the specified port.

Oper Status
Displays the operational status of the selected port.

1.10.4 IP General Configuration Fields

This section provides a general overview of the procedures required to configure the DELHW-UA. The following list describes each of the modifiable IP General Config Screen fields.

+PORT-
Use this field to select the routing port you wish to configure.

+REDIRECTOR-
Use this field to toggle through a list of commonly used UDP port numbers. UDP port numbers are associated with the relay agent functionality of the router.

Framing

Use this field to select the format of the frame in which IP packets are encapsulated for transmission.

MTU

Use this field to set the Maximum Transmission Unit (MTU).

IP Routing

Use this field to enable IP Routing Services.

IP Forwarding

Use this field to enable IP Forwarding.

Proxy ARP

Use this field to enable Proxy Address Resolution Protocol (ARP).

Address

Use this field to assign an IP address to the port that you wish to configure.

Mask

Use this field to set the Subnet Mask for the port that you wish to configure.

1.10.4.1 Selecting a Port for Configuration

Routing Services allows you to choose the ports that you want to configure for IP routing. To select a router port to configure for IP routing, complete the following steps:

1. Use the arrow keys to highlight the **PORT** option.

2. Type in the number of the port that you want to configure for IP routing and then press ENTER.

You can type in the port number, or you can use the +**PORT**- option at the bottom of the screen to scroll through the list of the ports on your device. To use the +**PORT-** option, use the arrow keys to highlight the + (to go forward), or the **-** (to go backward), and then press **ENTER** to scroll through the available ports in the direction you have selected. You can also use the **+** and **-** keys to scroll through the available ports.

If you type in an invalid port number, the error message “PORT NUMBER IS OUT OF RANGE” displays. Perform steps 1 and 2 again.

1.10.4.2 Entering the IP Address and Subnet Mask

All IP hosts must have an IP Address for each network interface. These addresses identify each network connection.

To enter the IP address for a router port, complete the following steps:

1. Use the arrow keys to highlight the **ADDRESS** option.

2. Type in the IP address and then press ENTER.

Once an IP address is entered, the default Subnet Mask automatically enters into the Mask field. To to change the default Subnet Mask for a router port, complete the following steps:

1. Use the arrow keys to highlight the **MASK** option.

2. Type in the Subnet Mask for the IP address that you have assigned.

1.10.4.3 Selecting the Frame Type for a Port

On each port, Frame Type specifies the format of the frame in which IP packets are encapsulated for transmission. The Frame Type options available for each router port are dependent on the type of media supported by that router port.

To select the Frame Type for a port, complete the following steps:

1. Use the arrow keys to highlight the **Framing** option.

2. Use the ENTER key to toggle the entry to the correct Frame Type for the port.

3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and then press ENTER. The message “SAVED OK” displays.

1.10.4.4 Setting the Maximum Transmission Unit (MTU)

The Maximum Transmission Unit specifies the maximum packet size for all IP packets that are transmitted.

To select the MTU for a port, complete the following steps:

1. Use the arrow keys to highlight the **MTU** option under Port Level Setup.
2. Enter an MTU value for the media used.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen, then press ENTER. The message “SAVED OK” displays.

1.10.4.5 Enabling IP Routing Services on a Port

The ability to switch IP Routing Services on and off on a port-by-port basis, provides great flexibility. On the same device, some ports can be routing IP traffic while other ports are bridging it. As you are in transition from a bridged network to a routed network, this flexibility allows you to implement IP routing and test your routing configuration on a port-by-port basis. If necessary, you can temporarily disable the IP routing on any port without losing your configuration, or you can temporarily switch from IP routing back to bridging.

To enable IP Routing Services on a router port, complete the following steps:

1. Use the arrow keys to highlight the **IP Routing** option under Port Level Setup.
2. Use the ENTER key to toggle the entry to **ENABLED**.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen, and then press ENTER. The message “SAVED OK” displays.

1.10.4.6 Enabling IP Forwarding on a Port

By default, IP Forwarding is disabled on each router port. Your device cannot begin forwarding IP data packets on any router port until you enable IP Forwarding on that port.

To enable IP Forwarding on a router port, complete the following steps:

1. Use the arrow keys to highlight the **IP Forwarding** option.
2. Use the ENTER key to toggle the entry to **ENABLED**.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and then press ENTER. The message “SAVED OK” displays.

1.10.4.7 Configuring the UDP Broadcast Redirector

To locate a server that can provide a particular network service, many IP hosts rely on the use of LAN broadcasts to send UDP service requests. The UDP port number contained in the broadcast request packet identifies the service being requested. Table 1-3 shows the port numbers and their corresponding requested services.

Table 1-3 UDP Port Numbers

UDP Port #	UDP Services
37	Time
42	Host Name Server
53	Domain Name Server
65	TACACS-Database Service
67	Bootstrap Protocol/Dynamic Host Control Protocol Server
68	Bootstrap Protocol/Dynamic Host Control Protocol Client
69	Trivial File Transfer
137	NETBIOS Name Server
138	NETBIOS Datagram Server
111	Sunrpc (NIS)

The UDP Broadcast Redirector enables you to configure any Routing Services enabled device to forward the UDP packets that it receives as LAN broadcasts, directly to the appropriate server. UDP service requests that are sent as LAN broadcasts by clients of applications such as Host Name, Domain Name, and Bootstrap servers, can be redirected to any server on any network segment.

To configure the UDP Broadcast Redirector, complete the following steps:

1. Use the arrow keys to highlight the **UDP Port** option under System Level Setup.
2. Enter the UDP port number of the UDP service request packets that you want to redirect (refer to Table 1-3) and then press ENTER.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and then press ENTER. The message “SAVED OK” displays.

You can type in the UDP port number, or you can use the +**REDIRECTOR**- option at the bottom of the screen to scroll through a list of commonly used UDP port numbers. To use the +**REDIRECTOR**- option, use the arrow keys to highlight the + (to go forward), or the - (to go backward), and then press the **ENTER** key to scroll in the direction that you selected.

The entry for the UDP Port option reflects the UDP port number that is currently selected. The entry for UDP Type names the UDP service to which that port number corresponds.

1.10.4.8 Enabling Proxy ARP on a Port

By default, Proxy Address Resolution Protocol (ARP) is disabled on all ports, and IP Routing Services respond only to ARP requests addressed to its own IP address.

For one IP host to communicate with another IP host, knowledge of the target host’s MAC address must be known. To learn this MAC address, the IP host sends an ARP request packet as a LAN broadcast with the destination IP address of the target IP host. All hosts receive this broadcast and the one host that matches the target IP address responds with its MAC-layer address.

However, because each subnet constitutes a separate broadcast domain and LAN broadcasts are not forwarded across routers, ARP does not work beyond a host’s local network or subnetwork. One of the primary purposes of a router is to confine LAN broadcast traffic to each local network or subnetwork.

A proxy ARP response is generated when the following occurs:

- Proxy ARP is enabled on a router port.
- An ARP request is received as a LAN broadcast (looking for the MAC-layer address of an IP host on another network segment).
- An entry exists in the IP Forwarding Table for the destination host’s network.

Enabling Proxy ARP on a router port allows IP hosts to dynamically obtain the MAC-layer address of other IP hosts attached to different networks or subnetworks by using broadcast ARP request packets. With Proxy ARP enabled, IP hosts are not required to maintain knowledge of specific subnetworks.

To enable Proxy ARP on a router port, complete the following steps:

1. Use the arrow keys to highlight the **Proxy ARP** option.
2. Use the ENTER key to toggle the entry to **ENABLED**.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen, and then press ENTER. The message “SAVED OK” displays.

1.10.4.9 Configuring the Network Broadcast Type on a Port

IP Routing Services recognizes and accepts network broadcasts, IP packets with the host portion of the IP address as either all 1’s or all 0’s. Other networking devices only recognize all 0’s as a network broadcast.

To configure IP Routing Services to send network broadcasts addressed to all 0’s, complete the following steps:

1. Use the arrow keys to highlight the **Network Bcast** option.
2. Use the ENTER key to toggle the entry to **ZEROS**.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and then press ENTER. The message “SAVED OK” displays.

1.10.5 Enabling the RIP Routing Protocol on a Port

Routing Information Protocol (RIP) is a widely implemented routing protocol that is used extensively on IP internetworks. IP Routing Services uses the RIP routing protocol to send and gather information about the internetwork topology. This information is used to construct and maintain a database called RIP Route Table, which contains the addresses of the available routes to all the networks and hosts that RIP has learned.

Enabling the RIP routing protocol allows IP Routing Services to build and maintain a dynamic database of route information. The best routes learned by the RIP routing protocol are added to the IP Forwarding Table to forward IP packets. The ability to switch the RIP routing protocol on and off on a port-by-port basis provides great flexibility. On the same device, some router ports can be running the RIP routing protocol while other router ports are not. If necessary, you can temporarily disable the RIP routing protocol on any port without affecting the rest of your configuration.

To enable RIP Routing, complete the following steps:

1. From the IP Configuration screen, highlight **IP RIP** and then press ENTER.

   The IP RIP Configuration screen, shown in Figure 1-15, displays.

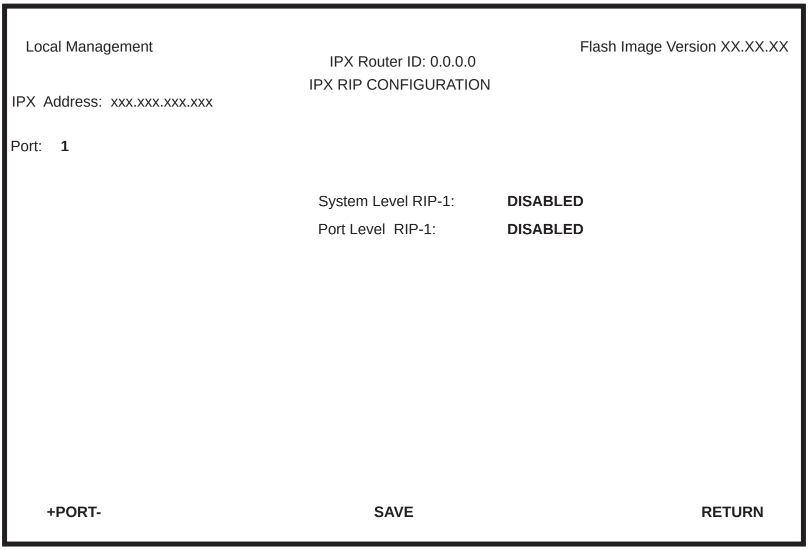
2. Use the arrow keys to highlight the **System Level RIP-1** option.

3. Use the ENTER key to toggle the entry to **ENABLED**.

4. Use the arrow keys to highlight the **Port Level RIP-1** option.

5. Use the ENTER key to toggle the entry to **ENABLED**.

6. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen, and then press ENTER. The message “SAVED OK” displays.



```
Local Management                                              Flash Image Version XX.XX.XX
                                IPX Router ID: 0.0.0.0
                               IPX RIP CONFIGURATION
IPX  Address:  xxx.xxx.xxx.xxx

Port:    1

                                System Level RIP-1:          DISABLED
                                Port Level  RIP-1:           DISABLED
```

Figure 1-15 IP RIP Configuration Screen

1.10.6 IP OSPF Configuration

OSPF (Open Shortest Path First) is a Link-State Protocol. OSPF distributes routing information between routers belonging to a single Autonomous System (AS). In an Autonomous System, routers exchange routing information through a common routing protocol.

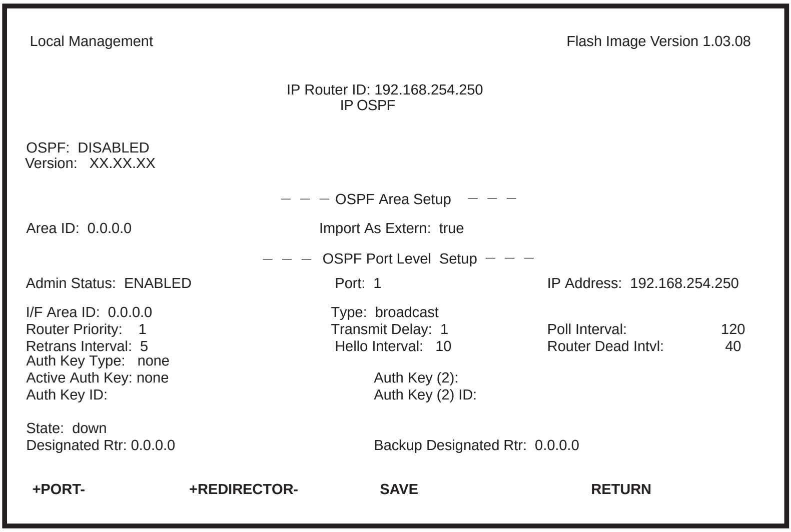
An Autonomous System may contain one or more networks, but each network within the AS may or may not support subnetting. Every OSPF routing domain must have a “Backbone”. An OSPF backbone distributes routing information between areas in an OSPF routing domain. The backbone of an OSPF routing domain is an OSPF area possessing an area ID of 0.0.0.0. Because OSPF protocol only broadcasts link state updates when topology has changed, it is considered “quiet” when compared to RIP protocol, which has to periodically send a portion, or all of its routing table to its neighbors.

Convergence (the time it takes to recalculate routing tables) under OSPF protocol is instantaneous and not periodic because of the use of IP Multicast to send the link-state updates. Updates are only sent when routing changes occur instead of periodically, ensuring better use of available bandwidth.

OSPF employs “flooding” to exchange link-states with other routers. Any change in routing information is flooded to all routers in the network. The use of “areas” puts a boundary on the explosion of link-state updates. All routers within an area will have the exact link-state database.

To enable OSPF complete the following steps:

1. From the Router Select screen, select **IP** and hit ENTER. The IP Configuration screen displays.
2. From the IP Configuration screen, use the arrow keys to select **IP OSPF**. Hit ENTER, and the IP OSPF Configuration screen shown in Figure 1-16, displays.



```
Local Management                                                         Flash Image Version 1.03.08

                                       IP Router ID: 192.168.254.250
                                                IP OSPF

OSPF:  DISABLED
Version:   XX.XX.XX

                                    — — — OSPF Area Setup   — — —

Area ID:  0.0.0.0                          Import As Extern:  true

                                  — — —  OSPF Port Level  Setup — — —
Admin Status:  ENABLED                         Port:  1                     IP Address:  192.168.254.250

I/F Area ID:  0.0.0.0                         Type:  broadcast
Router Priority:    1                         Transmit Delay:  1            Poll Interval:              120
Retrans Interval:  5                           Hello Interval:   10         Router Dead Intvl:           40
Auth Key Type:   none
Active Auth Key: none                              Auth Key (2):
Auth Key ID:                                       Auth Key (2) ID:

State:  down
Designated Rtr: 0.0.0.0                            Backup Designated Rtr:  0.0.0.0

 +PORT-               +REDIRECTOR-            SAVE                      RETURN
```

ipospfconfig

Figure 1-16 IP OSPF Configuration Screen

3. Use the arrow keys to select **OSPF: Disabled**. Hit ENTER. The selection will toggle to **Enabled**.
4. Use the arrow keys to select **Area ID: 0.0.0.0**. Enter the Area ID number in dotted decimal format (000.000.000.000). When you have finished entering the area ID number, use the arrow keys to select

Admin Status:. If Admin Status is Disabled, hit ENTER to toggle the status to **Enabled**. Use the arrow keys to select **Port:**. Type the port number you wish to use. Hit ENTER, and the port will be changed to the number that you typed.

5. Use the arrow keys to select **I/F Area ID**. Enter the I/F Area ID in dotted decimal notation (000.000.000.000). When you have finished, use the arrow keys to select **Router Priority**.

6. Type in the number representing the router priority you desire. When you have finished, use the arrow keys to select **Retrans Interval**. Enter the number of seconds of delay between retransmission of link-state advertisements. When you have finished, use the arrow keys to select **Transmit Delay**.

7. Type the number of seconds you wish to set for transmit delay. Transmit delay represents the estimated number of seconds it takes to transmit a link-state update packet over this interface. Link-state advertisements contained in the Link-state update packet will have their age incremented by this amount before transmission. This value must take into account transmission and propagation delays. When you have finished, use the arrow keys to select **Hello Interval**.

8. Type the number of seconds that you wish to use for the Hello Interval. The Hello Interval is the length of time in seconds between Hello packets that the router sends on this interface, advertised in Hello packets sent out of this interface. When you have finished use the arrow keys to select **Poll Interval**.

9. Type the number of seconds that you wish to use for Poll Interval. If a neighboring router has become inactive (Hello packets have not been sent for [router dead] seconds, it may be necessary to send Hello packets to the dead neighbor. The packets will be sent at a reduced rate [Poll Interval}, which should be much larger than the Hello Interval. A typical Poll Interval for an X.25 network is 120 seconds. When you have finished, use the arrow keys to select **Router Dead Interval**.

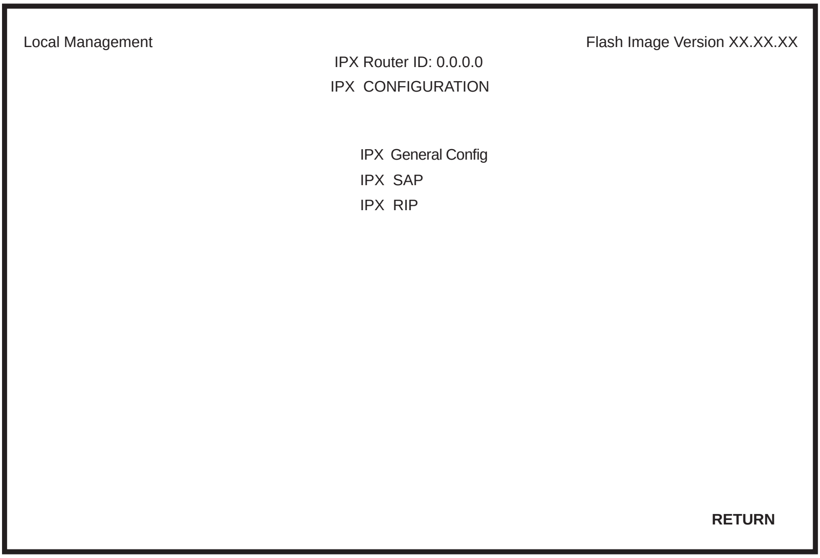
10. Type the number of seconds that you wish to use for Router Dead Interval. Router Dead Interval is the number of seconds before the router’s neighbors will declare it down, when they stop hearing the router’s Hello packets. When you have finished entering the Router

Dead Interval, use the arrow keys to select **SAVE**. Hit ENTER. The event message field at the top of the screen displays “SAVED OK”.

1.11 IPX CONFIGURATION SCREEN

The IPX Configuration screen enables you to access the IPX General Config, IPX RIP, and IPX SAP screens to configure the DELHW-UA for IPX Routing and enable RIP routing or Source Advertisement Protocol (SAP) routing on the DELHW-UA.

Access the IPX Configuration screen, shown in Figure 1-17, by using the arrow keys to highlight the **IPX** menu item on the Router Setup and pressing ENTER. The IPX Configuration screen displays.



```
Local Management                                           Flash Image Version XX.XX.XX
                              IPX Router ID: 0.0.0.0
                              IPX  CONFIGURATION


                                IPX  General Config
                                IPX  SAP
                                IPX  RIP





                                                                          RETURN
```

Figure 1-17 IPX Configuration Screen

1.11.1 IPX Configuration Fields

The following list describes each of the IPX Configuration screen fields.

IPX General Config
Use this field to access the IPX General Config screen and configure the DELHW-UA for IP routing.

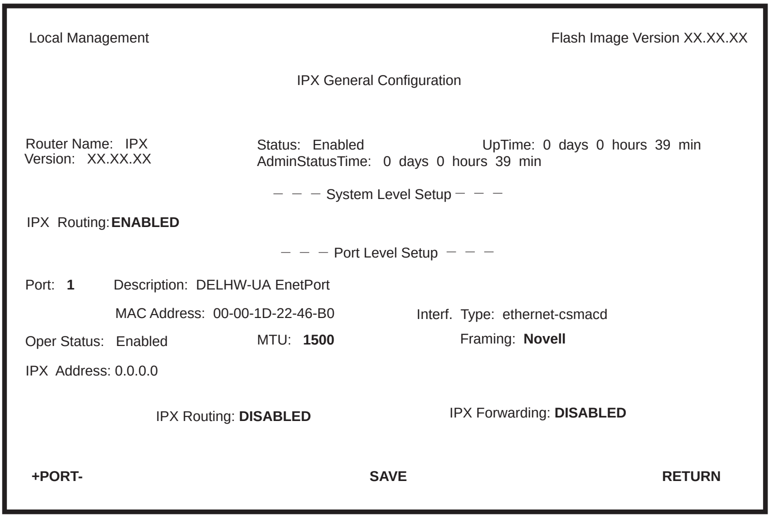
IPX SAP
Use this field to access the IPX SAP screen and enable Source Advertisement Protocol (SAP) routing.

IPX RIP
Use this field to access the IPX RIP screen and enable the Routing Information Protocol (RIP).

1.11.2 IPX General Configuration Screen

The IPX General Configuration screen allows you to configure the DELHW-UA for IPX routing.

To access the IPX General Configuration screen, use the arrow keys to highlight the **IPX General Config** menu item and press ENTER. The IPX General Configuration screen shown in Figure 1-18 displays.



```
 Local Management                                          Flash Image Version XX.XX.XX

                              IPX General Configuration


 Router Name:  IPX          Status:  Enabled             UpTime:  0  days  0  hours  39  min
 Version:   XX.XX.XX        AdminStatusTime:  0  days  0  hours  39  min

                         – – – System Level Setup – – –
 IPX  Routing: ENABLED
                         – – – Port Level Setup – – –
 Port:  1      Description:  DELHW-UA EnetPort

               MAC Address:  00-00-1D-22-46-B0        Interf.  Type:  ethernet-csmacd

 Oper Status:  Enabled          MTU:  1500                  Framing:  Novell

 IPX  Address: 0.0.0.0

            IPX Routing: DISABLED               IPX Forwarding: DISABLED


  +PORT-                              SAVE                                 RETURN
```

Figure 1-18 IPX General Configuration Screen

1.11.3 IPX General Configuration Status Fields

The following list describes each of the IPX General Config status fields. The status fields are for informational purposes only and cannot be modified.

Router Name
Displays the type of routing used.

Status
Displays the status of IP Routing.

UpTime
Displays the amount of time elapsed since the last time the DELHW-UA was rebooted.

Version
The version number of the IP Routing used on the DELHW-UA.

AdminStatusTime
Displays the amount of time elapsed since an IP address was assigned to the DELHW-UA.

Description
Describes the selected Port.

MAC Address
Displays the physical (MAC) address of the DELHW-UA.

Interf. Type
Displays the type of interface used by the specified port.

Oper Status
Displays the operational status of the selected port.

1.11.4 IPX General Configuration Fields

This section provides a general overview of the procedures required to configure the DELHW-UA. The following list describes each of the IPX General Config fields.

+PORT-
Use this field to select the routing port that you wish to configure.

Framing
Use this field to select the format of the Frame in which IPX packets are encapsulated for transmission.

MTU
Use this field to set the Maximum Transmission Unit (MTU).

IPX Routing
Use this field to enable IP Routing Services.

IPX Forwarding
Use this field to enable IP Forwarding.

IPX Address
Use this field to assign an IP Address to the port that you wish to configure.

1.11.4.1 Selecting a Port for Configuration

Routing Services allows you to choose the ports that you want to configure for IPX routing. To select a router port to configure for IPX routing, complete the following steps:

1. Use the arrow keys to highlight the **PORT** option.
2. Type in the number of the port that you want to configure for IPX routing, then press ENTER.

You can type in the port number, or you can use the +**PORT-** option at the bottom of the screen to scroll through the list of the ports on your device. To use the +**PORT-** option, use the arrow keys to highlight the + (to go forward), or the **-** (to go backward), and then press **ENTER** to scroll through the available ports in the direction you have selected. You can also use the **+** and **-** keys to scroll through the available ports.

If you type in an invalid port number the error message: “PORT NUMBER IS OUT OF RANGE” displays. Perform steps 1 and 2 again.

1.11.4.2 Entering the IPX Address

All IPX hosts must have an IPX Address for each network interface. These addresses identify each network connection.

To enter the IPX Address for a router port, complete the following steps:

1. Use the arrow keys to highlight the **IPX ADDRESS** option.

2. Type in the IPX Address in Dotted Decimal Notation (DDN) format and then press ENTER.

1.11.4.3 Selecting the Frame Type for a Port

On each port, Frame Type specifies the format of the frame in which IPX packets are encapsulated for transmission. The Frame Type options available for each router port are dependent on the type of media supported by that router port.

To select the Frame Type for a port, complete the following steps:

1. Use the arrow keys to highlight the **Framing** option.

2. Use the ENTER key to toggle the entry to the correct Frame Type for the port.

3. Use the arrow keys to highlight the **SAVE command field** at the bottom of the screen and then press ENTER. The message “SAVED OK” displays.

1.11.4.4 Setting the Maximum Transmission Unit (MTU)

The Maximum Transmission Unit specifies the maximum packet size for all IPX packets that are transmitted.

To select the MTU for a port, complete the following steps:

1. Use the arrow keys to highlight the **MTU** option under Port Level Setup.

2. Enter an MTU value for the media used.

3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and then press ENTER. The message “SAVED OK” displays.

1.11.4.5 Enabling IPX Routing Services on a Port

The ability to switch IPX Routing Services on and off on a port-by-port basis provides great flexibility. On the same device, some ports can be routing IPX traffic while other ports are bridging it. As you are in transition from a bridged network to a routed network, this flexibility allows you to implement IPX routing and test your routing configuration on a port-by-port basis. If necessary, you can temporarily disable IPX routing on any port without losing your configuration, or you can temporarily switch from IPX routing back to bridging.

To enable IPX Routing Services on a router port, complete the following steps:

1. Use the arrow keys to highlight the **IPX Routing** option under Port Level Setup.
2. Use the ENTER key to toggle the entry to **ENABLED**.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and then press ENTER. The message “SAVED OK” displays.

1.11.4.6 Enabling IPX Forwarding on a Port

By default, IPX Forwarding is disabled on each router port. Your device cannot begin forwarding IPX data packets on any router port until you enable IPX Forwarding on that port.

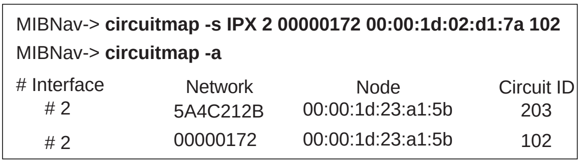
To enable IPX Forwarding on a router port, complete the following steps:

1. Use the arrow keys to highlight the **IPX Forwarding** option.
2. Use the ENTER key to toggle the entry to **ENABLED**.
3. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen and then press ENTER. The message “SAVED OK” displays.

1.11.5 IPX Routing over Frame Relay

An additional step is required when routing IPX over Frame Relay. This step requires that entries are created in the IPX Host Map. The IPX Host Map is a database of remote IPX hosts that are defined generally by the WAN Network number and MAC Address, and more specifically by the Interface Number and Data Link Connection Identifier (DLCI). The IPX Host Map helps a routing decision by determining which circuit a packet should be forwarded to in a point to multi-point Frame Relay connection.

Figure 1-19 shows how IPX Host Map entries are entered using the circuitmap command. The circuitmap command is accessed from the **MIB Navigator Screen**. Refer to **Chapter 2** for more information on the circuitmap command.



```
MIBNav-> circuitmap -s IPX 2 00000172 00:00:1d:02:d1:7a 102
MIBNav-> circuitmap -a
# Interface          Network          Node            Circuit ID
     # 2            5A4C212B     00:00:1d:23:a1:5b        203
     # 2            00000172     00:00:1d:23:a1:5b        102
```

Figure 1-19 Circuitmap Command

The circuitmap command contains the following fields:

#Interface
An entry must be created for each remote Router connected via the Frame Relay interface.

Network
The Network is the IPX Network number associated with the Frame Relay network.

Node
The Node is the MAC address of the remote router on the other end of the WAN link.

Circuit ID
The Circuit ID is the DLCI identifying the virtual circuit connection to the Telco.

1.11.6 Enabling the IPX SAP Routing Protocol on a Port

IPX Source Advertisement Protocol (SAP) is used by IPX to exchange information about Novell service providing nodes, such as file servers and print servers that are available. IPX SAP builds and maintains a database, the Service Advertisement Table, containing the addresses and routes to specific service providing nodes, and advertises this information over the network.

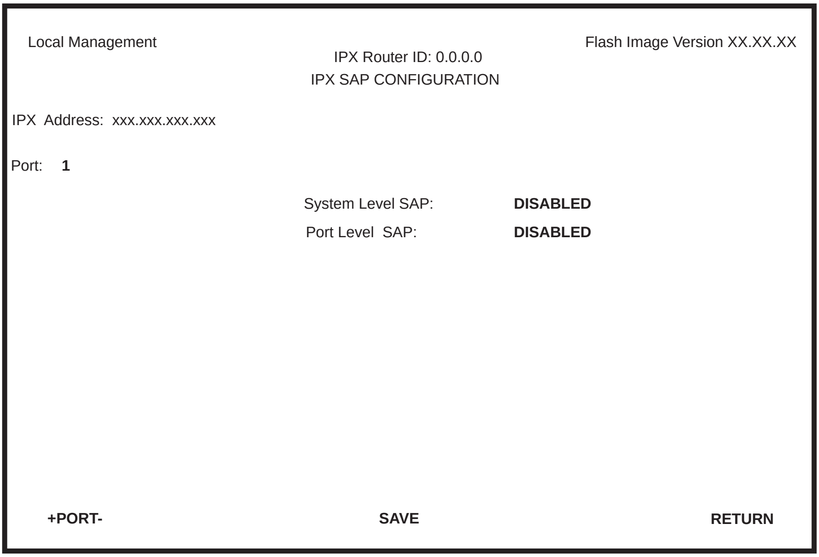
Each router running IPX SAP gathers this LAN based information from the locally connected network segments and adds it to its Service Advertisement Table. Each table contains the Novell Network Number and type of services available on all Novell servers known to the IPX SAP. IPX routing services uses this information to provide internetworked NetWare clients with access to these services.

To enable SAP Routing, complete the following steps:

1. From the IPX Configuration screen, highlight **IPX SAP** and then press ENTER.

   The IPX SAP Configuration screen, shown in Figure 1-20, displays.

2. Use the arrow keys to highlight the **Port** option.
3. Type in the number of the port that you wish to enable SAP routing, then press ENTER.
4. Use the arrow keys to highlight the **Port Level SAP** option.
5. Use the ENTER key to toggle the entry to **ENABLED**. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen, and then press ENTER. The message “SAVED OK” displays.



```
Local Management                                        Flash Image Version XX.XX.XX
                              IPX Router ID: 0.0.0.0
                              IPX SAP CONFIGURATION

IPX  Address:  xxx.xxx.xxx.xxx

Port:    1

                              System Level SAP:         DISABLED
                              Port Level  SAP:          DISABLED
```

Figure 1-20 IPX SAP Configuration Screen

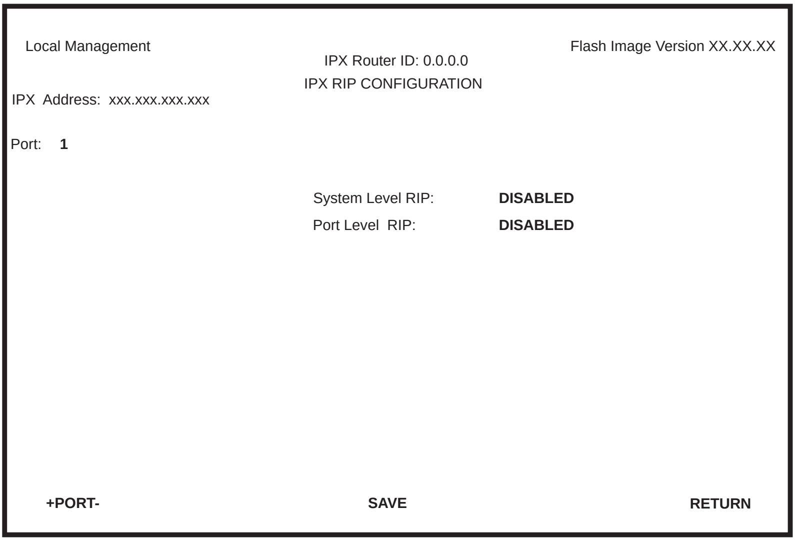
1.11.7 Enabling RIP on a Port

IPX RIP (Routing Information Protocol) is a widely implemented routing protocol that is used extensively on IPX intermediations. IPX Routing Services uses the RIP to send and gather information about the internetwork topology. This information is used to construct and maintain a database, called the RIP Route Table, containing the addresses and available routes to all the networks and hosts that RIP has learned.

Enabling RIP allows IPX Routing Services to build and maintain a dynamic database of route information. The best routes learned by RIP are added to the IPX Forwarding Table to be used to forward IPX packets. The ability to switch RIP on and off on a port-by-port basis provides great flexibility. On the same device, some router ports can be running RIP while other router ports are not. If necessary, you can temporarily disable RIP on any port without affecting the rest of your configuration.

To enable RIP Routing, complete the following steps:

1. From the IPX Configuration screen, highlight **IPX RIP** and then press ENTER. The IPX RIP Configuration screen, shown in Figure 1-21, displays.
2. Use the arrow keys to highlight the **Port** option.
3. Type in the number of the port that you wish to enable RIP routing and then press ENTER.
4. Use the arrow keys to highlight the **Port Level RIP** option.
5. Use the ENTER key to toggle the entry to **ENABLED**. Use the arrow keys to highlight the **SAVE** command field at the bottom of the screen, and then press ENTER. The message “SAVED OK” displays.



```
 Local Management                                          Flash Image Version XX.XX.XX
                                    IPX Router ID: 0.0.0.0
                                  IPX RIP CONFIGURATION
IPX  Address:  xxx.xxx.xxx.xxx

Port:    1


                                   System Level RIP:          DISABLED
                                   Port Level  RIP:           DISABLED







    +PORT-                               SAVE                                 RETURN
```

Figure 1-21   IPX RIP Configuration Screen

CHAPTER 2

MIB NAVIGATOR

This chapter explains how to use the MIB Navigator utility. The MIB Navigator allows access to a command set from which you can configure and manage your DELHW-UA.

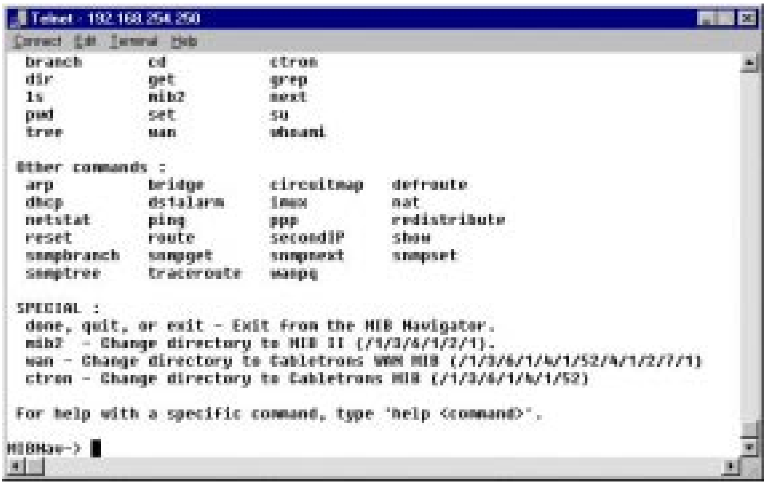
2.1 CHAPTER ORGANIZATION

The following list summarizes the organization of this chapter:

- **MIB Navigator Screen** – describes the MIB Navigator screen and explains how to access it.
- **MIB Navigator Command Set Overview** – describes the types of commands available to the MIB Navigator.
- **Navigation Commands** – explains the commands used to navigate through the MIB Navigator.
- **Other Commands** – explains other commands that allow you to access and manage network devices connected to the device running the MIB Navigator.
- **Special Commands** – explains the special commands that allow you to exit from the MIB Navigator.
- **PPP Security Command** – explains how to list and set security on an interface basis.
- **ISDN Configuration Commands** – explains how to set up primary and backup configurations.

2.2 MIB NAVIGATOR SCREEN

Access the MIB Navigator screen from the Main Menu screen using Local Management (refer to the **Accessing Local Management** section in **Chapter 1** of this guide). Using the arrow keys, highlight the **MIB NAVIGATOR** menu item, then press ENTER. At the MIB Navigator cursor, type **Help** and press ENTER. The MIB Navigator Help screen shown in Figure 2-1 displays.



```
  branch       cd           ctron
  dir          get          grep
  ls           mib2         next
  pwd          set          su
  tree         wan          whoami

 Other commands :
  arp          bridge       circuitmap   defroute
  dhcp         dslalarm     imux         nat
  netstat      ping         ppp          redistribute
  reset        route        secondIP     show
  snmpbranch   snmpget      snmpnext     snmpset
  snmptree     traceroute   wanpq

 SPECIAL :
  done, quit, or exit - Exit from the MIB Navigator.
  mib2  - Change directory to MIB II (/1/3/6/1/2/1).
  wan - Change directory to Cabletrons WAN MIB (/1/3/6/1/4/1/52/4/1/2/7/1)
  ctron - Change directory to Cabletrons MIB (/1/3/6/1/4/1/52)

 For help with a specific command, type 'help <command>'.

MIBNav->
```

Figure 2-1 MIB Navigator Help Screen

2.2.1 Managing Device MIBs

The MIB Navigator lets you manage objects in the DELHW-UA Management Information Bases (MIBs). MIBs are databases of objects used for managing the device and determining the device’s configuration. The commands within the MIB Navigator enable you to view and modify a device’s objects.

The MIB Navigator views the MIB tree hierarchy as a directory. Figure 2-2 shows the MIB tree hierarchy. Each layer is numerically encoded, so that every branch group and leaf object in the MIB is identified by a corresponding number, known as an Object Identifier (OID). This allows the MIB Navigator to navigate through the MIB and access the manageable leaf objects.

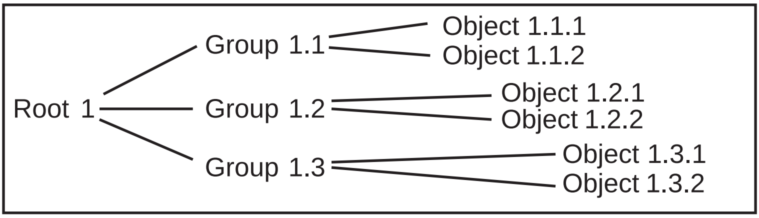


Figure 2-2 Hierarchical MIB Tree Structure

Often an ASCII name is assigned to the OID of a leaf object, making it more readable. To identify the value for the object “ipForwarding” you use the OID (/1/3/6/1/2/1/4/1), or its ASCII name (/iso/org/dod/internet/mgmt/mib-2/ip/ipForwarding).

2.3 MIB NAVIGATOR COMMAND SET OVERVIEW

Use the help command for an on-line description of each MIB Navigator command. For example **MIB Nav-> help branch** provides help information for the branch command.

The MIB Navigator command set provides the following commands:

Navigation Commands

Navigation commands allow you to access and manage the MIB for the device running the MIB Navigator. Some of these commands also provide user community-string information. The commands are as follows:

```
branch          cd          ctron
dir             get         grep
ls              mib2        next
```

pwd
set
su
tree
wan
whoami
help

Other Commands

Other commands allow you to access and manage network devices connected to the device running the MIB Navigator. The commands are as follows:

arp
bridge
circuitmap
defroute
dhcp
ds1alarm
fr
imux
nat
netstat
ping
ppp
redistribute
reset
route
secondIP
show
snmpbranch
snmpget
snmpnext
snmpset
snmptree
traceroute
wanpq

Special Commands

Special Commands allow you to exit from the MIB Navigator. The commands are as follows:

done
quit
exit

2.3.1 Conventions for MIB Navigator Commands

This manual uses the following conventions for denoting commands:

- Information keyed by the user is shown in this helvetica font.
- In the examples, information keyed in by the user is indicated by **bold font**.
- Command arguments are indicated by two types of brackets:
  - required arguments are enclosed by [ ].
  - optional arguments are enclosed by < >.

MIB Navigator command conventions are as follows:

- To abort the output or interrupt a process the escape character is ^C (where ^ indicates the Control key).

- A slash (/) preceding an OID issues that command from the root directory regardless of where you are in the MIB. If no slash precedes the OID the command issues from your current MIB location.
- Dot notation (1.1.1.1) is equivalent to slash notation (1/1/1/1). Use slash notation with the navigational commands, and the dot notation with the built-in commands that are using SNMP to access and manage network devices.

MIB Navigation Commands are listed in the format shown below:

command:

Syntax: This entry provides the format that the MIB Navigator command requires. It indicates where arguments, if any, must be specified.

Description: This entry briefly describes the command and its uses.

Options: This entry lists any additional fields which may be added to the command and their format.

Example: This entry shows an example of the command.

2.4 NAVIGATION COMMANDS

The following MIB Navigation commands allow you to move from MIB object to MIB object within the MIB tree.

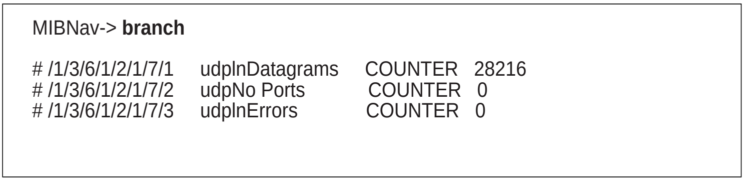
branch:

Syntax: branch [path]

Description: The branch command displays all of the leaves in the MIB tree below a specified path. The information displayed includes the pathname, the object ASCII name, the type of object (i.e., integer, counter, time tick, etc.), and the current value of each leaf object.

Options: Not Applicable

Example:



```
MIBNav-> branch

# /1/3/6/1/2/1/7/1    udplnDatagrams    COUNTER   28216
# /1/3/6/1/2/1/7/2    udpNo Ports        COUNTER   0
# /1/3/6/1/2/1/7/3    udplnErrors        COUNTER   0
```

cd:

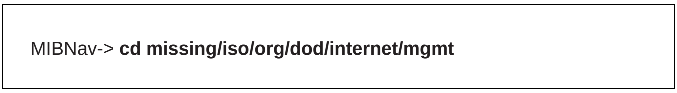
Syntax: cd [path] or cd <option>

Description: The cd command allows you to change directories within a MIB subtree (branch). The path specified must be valid, or the MIB Navigator will not perform the cd operation.

Options: .. Moves you one subtree above the current one.

/ Moves you to the root.

Example:



```
MIBNav-> cd missing/iso/org/dod/internet/mgmt
```

051457

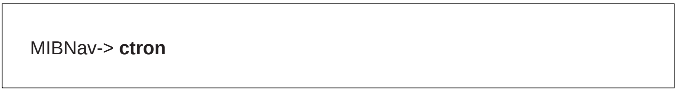
ctron:

Syntax: ctron

Description: The ctron command allows you to change directories to the Cabletron MIB (1.3.6.1.4.1.52) without keying in the path.

Options: Not Applicable

Example:



```
MIBNav-> ctron
```

051458

dir:

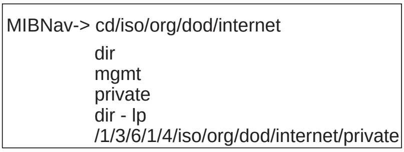
Syntax: dir [- 1pdm] [PATH]

Description: The dir command lists the contents of the directory sub-tree specified. If no [directory-path] is specified, the contents of the current directory are displayed. The display options are as follows:

-1 Displays the OID value along with the ASCII name of the leaf object.
-p Lists all the entries along with the path name of the leaf object.
-d Lists only the directory entries in the tree.
-m Displays one screen at a time.

Options: Not Applicable

Example:



```
MIBNav-> cd/iso/org/dod/internet
            dir
            mgmt
            private
            dir - lp
            /1/3/6/1/4/iso/org/dod/internet/private
```

dir

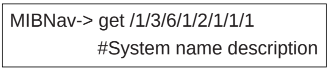
get:

Syntax: get <PATH>

Description: Returns the value of a managed object. This is only valid for “leaf” entries in the MIB tree (or managed objects in the MIB).

Options: Not Applicable

Example:



```
MIBNav-> get /1/3/6/1/2/1/1/1
            #System name description
```

get

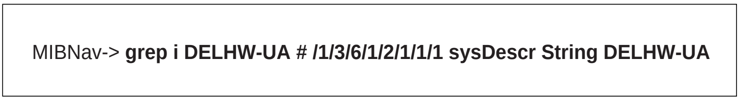
grep:

Syntax: grep <option> string

Description: Allows you to search the MIB tree for a specific character string. All leafs in the MIB tree are searched.

Options: -m Displays on the terminal one screen at a time.
-i Ignores case when searching for string.

Example:



```
MIBNav-> grep i DELHW-UA # /1/3/6/1/2/1/1/1 sysDescr String DELHW-UA
```

051478

ls:

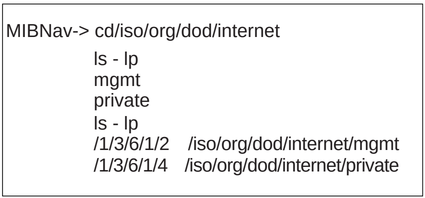
Syntax: ls [-1pdm] [PATH]

Description: Lists the contents of the directory sub-tree specified. If no [directory-path] is specified, the contents of the current directory are displayed. The display options are as follows:

-1 Displays the OID value along with the ASCII name of the leaf object.
-p Lists all the entries along with the path name of the leaf object.
-d Lists only the directory entries in the tree.
-m Displays one screen at a time.

Options: Not Applicable

Example:



```
MIBNav-> cd/iso/org/dod/internet
            ls - lp
            mgmt
            private
            ls - lp
            /1/3/6/1/2    /iso/org/dod/internet/mgmt
            /1/3/6/1/4   /iso/org/dod/internet/private
```

ls

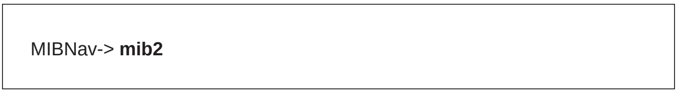
mib2:

Syntax: mib2

Description: The mib2 command allows you to move directly to the MIB II subtree (1.3.6.1.2.1) without entering the entire path.

Options: Not Applicable

Example:



```
MIBNav-> mib2
```

051460

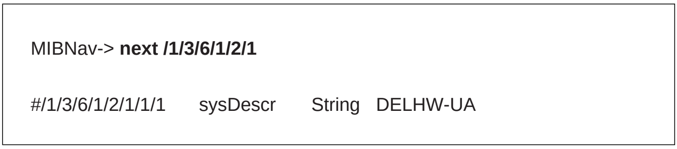
next:

Syntax: next [path]

Description: The next command enables you to determine the next leaf in the specified path within the managed device’s MIB.

Options: Not Applicable

Example:



```
MIBNav-> next /1/3/6/1/2/1

#/1/3/6/1/2/1/1/1      sysDescr      String   DELHW-UA
```

051461

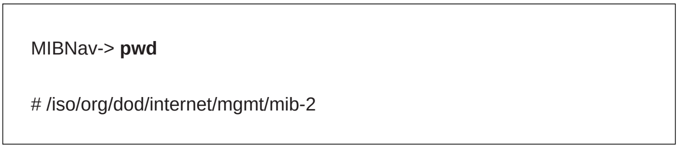
pwd:

Syntax: pwd

Description: The pwd command displays the full pathname for the directory in which you are currently working. The directory is displayed in ASCII format.

Options: Not Applicable

Example:



```
MIBNav-> pwd

# /iso/org/dod/internet/mgmt/mib-2
```

051462

set:

Syntax: set <OID> <value>

Description: The set command enables you to set the value of a managed object. This command is valid only for leaf entries in the current MIB tree, or for managed objects in the MIB.

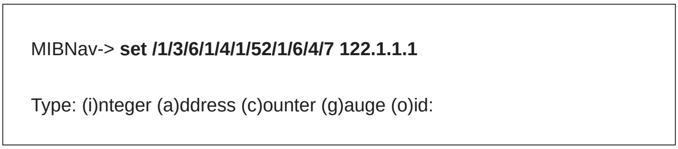
If the leaf specified does not exist for the given path, MIB Navigator asks for a value. The following lists possible value types:

(i)nteger - number
(c)ounter - number

(g)auge - number
(t)ime ticks - number
o(p)aque - “value” (with quotation marks)
(s)tring - “value” (with quotation marks)
(o)id - OID number with dotted punctuation
(a)ddress - IP address in DDN format
(m)ac - MAC address in hexadecimal format
(n)ull - no type

Options: Not Applicable

Example:



```
MIBNav-> set /1/3/6/1/4/1/52/1/6/4/7 122.1.1.1

Type: (i)nteger (a)ddress (c)ounter (g)auge (o)id:
```

051463

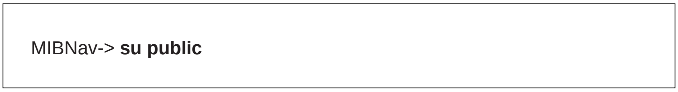
su:

Syntax: su [community name]

Description: The su command enables you to change your community name to allow for different access to the MIB. The community name that you enter allows you either read-only, read-write, or super-user access to that device’s MIBs, depending on the level of security access assigned the password through the SNMP Community Names screen. Refer to the **SNMP Community Names Screen** section in **Chapter 1** for more information about community names.

Options: Not Applicable

Example:



```
MIBNav-> su public
```

051464

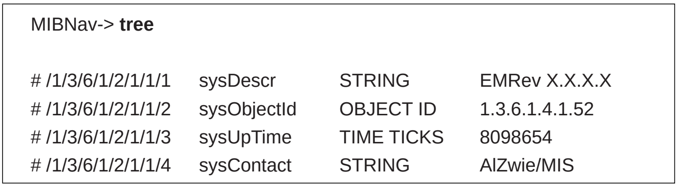
tree:

Syntax: tree

Description: The tree command provides a display of the entire MIB for the device. Leaves and associated values are displayed in columns.

Options: Not Applicable

Example:



```
MIBNav-> tree

# /1/3/6/1/2/1/1/1    sysDescr       STRING         EMRev X.X.X.X
# /1/3/6/1/2/1/1/2    sysObjectId    OBJECT ID      1.3.6.1.4.1.52
# /1/3/6/1/2/1/1/3    sysUpTime      TIME TICKS     8098654
# /1/3/6/1/2/1/1/4    sysContact     STRING         AlZwie/MIS
```

051465

wan:

Syntax: wan

Description: The wan command will change the current directory to Cabletron’s WAN MIB: (/1/3/6/1/4/1/52/4/1/2/7/2).

Options: Not Applicable

whoami:

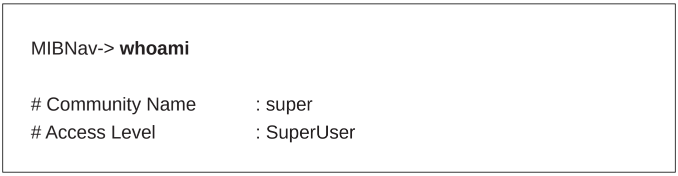
Syntax: whoami

Description: The whoami command displays your community string and access privileges to the

MIB. When using the whoami command, one of these three access levels displays: read-only, read-write, and super-user.

Options: Not Applicable

Example:



```
MIBNav-> whoami

# Community Name          : super
# Access Level            : SuperUser
```

051466

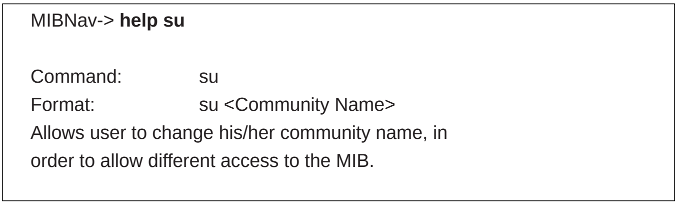
help:

Syntax: help <command>

Description: The help command provides general help on how to use the MIB Navigator or how to use a particular MIB Navigator command.

Options: A particular MIB Navigator command.

Example:



```
MIBNav-> help su

Command:          su
Format:           su <Community Name>
Allows user to change his/her community name, in
order to allow different access to the MIB.
```

051459

2.5 OTHER COMMANDS

The Other commands listed in this section activate functions on the LM managed device or devices being accessed through MIB Navigation.

arp:

Syntax: arp <options>

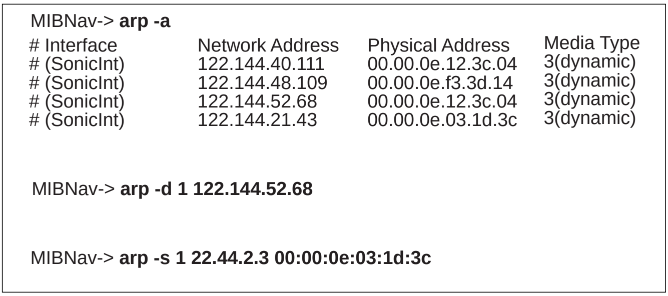
Description: The arp command provides access to the ARP (Address Resolution Protocol) cache, enabling you to view cache data, delete entries, or add a static route. Super-user access is required to delete an entry or add a static route.

Each ARP cache entry lists the network *interface* that the device is connected to, the device's *network address* or IP address, the device's *physical address* or MAC address, and the *media type* of connection to the device. Media types are displayed as numbers, which stand for the following states:

1 - Other
2 - Invalid entry (cannot ping device, timed out, etc.)
3 - Dynamic route entry
4 - Static route entry (not subject to change)

Options: -a Views cache data.
-d Deletes an IP address entry.
Requires additional arguments: <Interface Number> <IP address>
-s Adds a static entry.
Requires additional arguments: <Interface Number> <IP address> <MAC address>

Example:



```
MIBNav-> arp -a
# Interface          Network Address      Physical Address      Media Type
# (SonicInt)         122.144.40.111       00.00.0e.12.3c.04     3(dynamic)
# (SonicInt)         122.144.48.109       00.00.0e.f3.3d.14     3(dynamic)
# (SonicInt)         122.144.52.68        00.00.0e.12.3c.04     3(dynamic)
# (SonicInt)         122.144.21.43        00.00.0e.03.1d.3c     3(dynamic)


MIBNav-> arp -d 1 122.144.52.68


MIBNav-> arp -s 1 22.44.2.3 00:00:0e:03:1d:3c
```

051467

bridge:

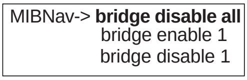
Syntax: bridge <ENABLE/DISABLE> <IFNUM/ALL>

Description: The bridge command allows management of bridging upon one or more interfaces of the device. Bridging may be enabled or disabled at your request, either one at a time or all at once. Specifying a single interface number affects the bridging status of that interface, while specifying ALL affects every interface of the device.

Options: <ENABLE/DISABLE> Enables or disables bridging.

<IFNUM/ALL> Allows you to specify an interface number.

Example:



```
MIBNav-> bridge disable all
             bridge enable 1
             bridge disable 1
```

bridge

circuitmap:

Syntax: circuitmap -a <PROTOCOL>

circuitmap -f <PROTOCOL>

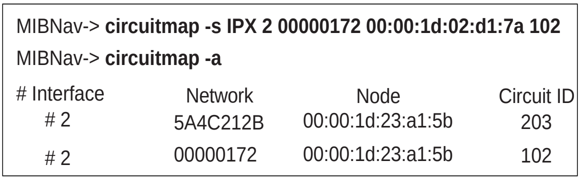
circuitmap -d <PROTOCOL> <INTERFACENUM> <NETADDRESS> <MACADDRESS>

circuitmap -s <PROTOCOL> <INTERFACENUM> <NETADDRESS> <MACADDRESS> <CIRCUIT>

Description: The circuitmap command allows you to view and/or modify a Protocol’s Circuit Map (i.e., address-to-circuit) table for the device.
The device must be initialized after changing the Circuit Map.

Options: -a Shows you the current Host Map information for the device.
-d Allows you to delete an entry from the table.
-s Allows you to insert a static entry into the table.
-f Allows you to flush the table.

Example:



```
MIBNav-> circuitmap -s IPX 2 00000172 00:00:1d:02:d1:7a 102
MIBNav-> circuitmap -a
# Interface       Network          Node            Circuit ID
   # 2           5A4C212B    00:00:1d:23:a1:5b        203
   # 2           00000172    00:00:1d:23:a1:5b        102
```

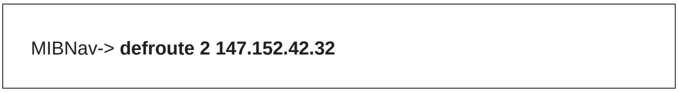
defroute:

Syntax: defroute [interface number] [IP address]

Description: The defroute command allows you to set the default IP route to a managed device through the specified interface.

Options: Not Applicable

Example:



```
MIBNav-> defroute 2 147.152.42.32
```

051469

dhcp:

Syntax: dhcp <options>

Description: The dhcp command provides a status of the Dynamic Host Configuration Protocol feature. It allows you to enable/disable DHCP globally and by interface, and to configure interfaces with server parameters.

Options: dhcp (with no options) Displays DHCP status information.
dhcp enable/disable Enables or disables the DHCP feature globally.

dhcp <IFNUM> enable disable Enables or disables the DHCP feature by interface.

dhcp reclaim <IPADDRESS> Reclaims an IP address so another client can use it.

dhcp <IFNUM> <GATEWAY> <DNSADDRESS> <WINSADDRESS> <DOMAINNAME> The IFNUM is the Ethernet port number. The four configuration parameters can be passed to the hosts (clients). These are the IP address of their default gateway, the IP address of their domain name server, the IP address of their WINS server, and their domain name.

dhcp <IFNUM> <NETADDRESS> <NETMASK> <LOWADDRESS> <HIGHADDRESS> <LEASE> Allows you to specify the lease period for the hosts (clients), from one hour to many years. Selectable on a per port basis only.

<IFNUM> The Ethernet port number.

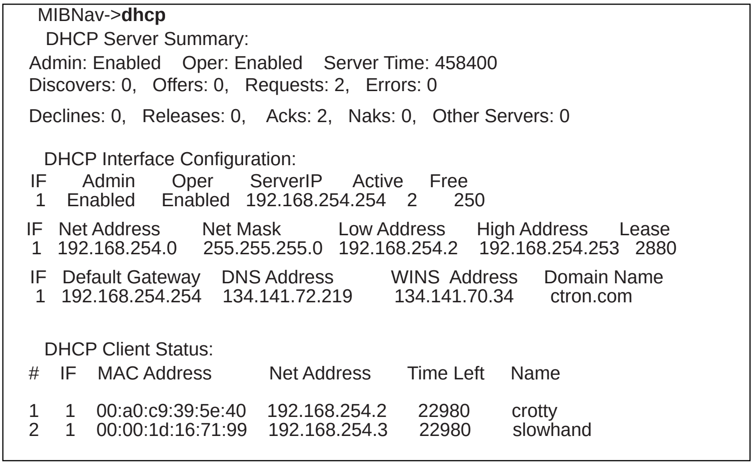
<NETADDRESS> The IP network on which the hosts will reside.

<NETMASK> The subnet mask for the hosts.

<LOWADDRESS> The lowest numerical value of the IP range to be allocated.

<HIGHADDRESS> The highest numerical value of the IP range.

Example:



```
   MIBNav->dhcp
    DHCP Server Summary:
 Admin: Enabled    Oper: Enabled    Server Time: 458400
 Discovers: 0,   Offers: 0,   Requests: 2,   Errors: 0

 Declines: 0,   Releases: 0,    Acks: 2,   Naks: 0,   Other Servers: 0

    DHCP Interface Configuration:
 IF      Admin       Oper       ServerIP      Active     Free
  1    Enabled     Enabled   192.168.254.254    2       250

IF   Net Address       Net Mask          Low Address      High Address      Lease
 1   192.168.254.0     255.255.255.0   192.168.254.2    192.168.254.253   2880

 IF   Default Gateway    DNS Address          WINS  Address     Domain Name
  1   192.168.254.254    134.141.72.219       134.141.70.34      ctron.com


    DHCP Client Status:
 #    IF    MAC Address          Net Address       Time Left     Name

 1     1    00:a0:c9:39:5e:40    192.168.254.2      22980        crotty
 2     1    00:00:1d:16:71:99    192.168.254.3      22980        slowhand
```

dhcp

ds1alarm:

Syntax:

```
ds1alarm
ds1alarm -ea <WANID>
ds1alarm -da <WANID>
ds1alarm -er <WANID>
ds1alarm -dr <WANID>
ds1alarm -et <WANID>
ds1alarm -dt <WANID>
ds1alarm -sec <WANID> <VALUE>
ds1alarm -sei <WANID> <VALUE>
ds1alarm -sbr <WANID> <VALUE>
ds1alarm -sbi <WANID> <VALUE>
```

Description: The command “ds1alarm” with no options displays status information.

Options: <WANID> Is either ALL to apply the command to all DS1 circuits, or it is the specific WAN physical identifier associated with the DS1 circuit.ds1alarm (with no options) displays status information.

ds1alarm -ea Enables the WAN DS1 Alarms Admin.
ds1alarm -da Disables the WAN DS1 Alarms Admin.
ds1alarm -er Enables the WAN DS1 Alarms Auto Recovery Feature.
ds1alarm -dr Disables the WAN DS1 Alarms Auto Recovery Feature.
ds1alarm -et Enables the WAN DS1 Alarms Traps Feature.
ds1alarm -dt Disables the WAN DS1 Alarms Traps Feature.
ds1alarm -sec Sets the Errored Seconds Threshold Count to VALUE.
ds1alarm -sei Sets the Errored Seconds Threshold Interval to VALUE.
ds1alarm -sbr Sets the Bipolar Violations Threshold Rate to VALUE.

ds1alarm -sbi Sets the Bipolar Violations Threshold Interval to VALUE.

fr:

Syntax: fr

Description: The fr command provides status related to Frame Relay and its Control Protocols.

- MGR: This is the physical WPIM for the DLCI
- CKT: This is the virtual port number for the DLCI
- IF: This is the MIB II interface number for the DLCI
- DLCI: This is the circuit DLCI number
- DCP: This is the state of FR Data Compression on this DLCI (on/off)
- STATE: This is the DLCI circuit state (active/invalid/inactive)
- Inactive Reason: This value is empty for active/invalid states. It is filled in if the circuit is inactive. It has the following values:

a. t391 Polling Error: This is a result of a failure in the Synchronous polling between us and the FR switch. If 3 out of any 4 polling cycles fail then both will place the link between us and the FR switch in a “link down” state. This will cause all DLCIs to be set to inactive, and no data placed on the wire (other than polling messages) until the service affecting condition is cleared. This service affecting condition can be the result of a number of things:

- Our STATUS ENQUIRY message never reaches the FR switch, due to: our WAN driver, or our physical WAN connection to the Fr switch dropping the packet for some reason.

- The STATUS RESPONSE message never reaches the FR protocol code, due to: our WAN driver, or our physical WAN connection to the Fr switch, or the FR switch itself dropping the packet for some reason.
- The incorrect LMI type Si selected at our side or the Fr switch side. If they do not match, then polling errors will result.

b. DLCMI Protocol Error: This is a service affecting condition that can/will occur due to any error that has happened between/before the link goes down due to excessive polling errors. If 3 out of 4 errors have not occurred yet, but the circuit was prevented from going active by any one of the FR errors listed in Section, then this will be the condition listed for the inactive reason.

c. Startup/Initialization: This basically means there have been no errors, we are polling correctly with the switch, but for some reason the switch reports to us inactive for that DLCI. Possible reasons for this are:

- The FR DTE bridge/router <-> FR DCE switch on the far side of the WAN cloud is not connected, or has polling error problems. Refer to the remote mibnav/LM screen for CSX products, the Telecommunications/Remote Access Service provider, or other means (remote device console support/protocol analyzer) at the far end to troubleshoot the remote device.

- It may take up to 60 seconds (by default) [t391 (10 by default) seconds x n391 (6 by default) cycles for a circuit to go active, even in a well behaved properly communicating network. This is due to STATUS polling convergence of both FR DCE switches, with both FR DTE bridge/routers.

imux:

Syntax: imux <options>

Description: The imux command lets you balance your LAN traffic between two T1 WAN ports and is used with Point to Point Protocol (PPP). When you select Inverse Multiplexing via QuickSET, bridging, IP routing, and IPX routing functions are all disabled. The WAN device at the other end of the WAN link(s) must be a Cabletron Systems device, capable of receiving the balanced WAN traffic. The imux command with no options displays the status information.

Options:

-ea Enables the Inverse Multiplexer Application.

-da Disables the Inverse Multiplexer Application.

-eg <GROUPID> Enables the Inverse Multiplexer group designated by <GROUPID>.

-dg <GROUPID> Disables the Inverse Multiplexer group designated by <GROUPID>.

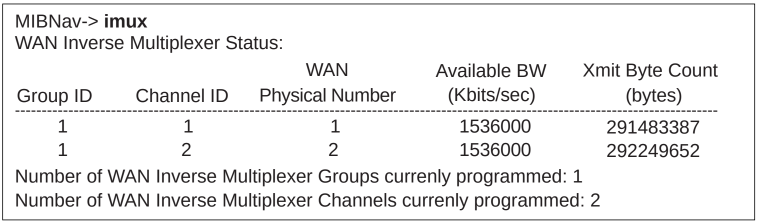
-ac <GROUPID> <INTERFACENUM>
Adds the WAN channel designated by <INTERFACENUM> to the Inverse Multiplexer group designated by <GROUPID>.

-dc <GROUPID> <INTERFACENUM>
Deletes the WAN channel designated by <INTERFACENUM> from the Inverse Multiplexer group designated by <GROUPID>.

<GROUPID> A unique value identifying an element in a sequence of groups that belong to the WAN Inverse Multiplexer Application.

<INTERFACENUM> The MIB II ifIndex value used to represent a WAN channel that has an appropriate datalink protocol associated with it.

Example:



```
MIBNav-> imux
WAN Inverse Multiplexer Status:
                                     WAN            Available BW     Xmit Byte Count
Group ID      Channel ID      Physical Number       (Kbits/sec)         (bytes)
---------------------------------------------------------------------------------------
   1              1                  1                1536000          291483387
   1              2                  2                1536000          292249652
Number of WAN Inverse Multiplexer Groups currenly programmed: 1
Number of WAN Inverse Multiplexer Channels currenly programmed: 2
```

imux

nat:

Syntax: nat <options>

Description: The nat command provides status relating to Network Address Translation. It allows you to assign a private network to an interface, to define an interface through which the internet can be accessed, and to create a public IP address to be used on the internet. It also allows you to assign a host on the private network as a “proxy server” accessible from the internet.

Options: nat (with no options) Displays status information

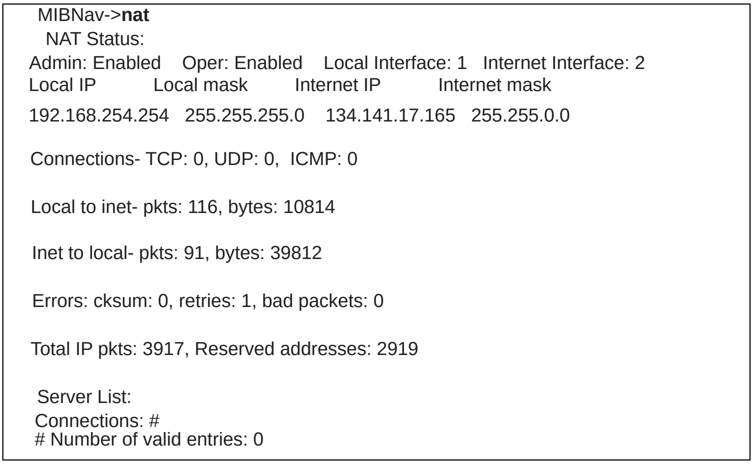
nat enable/disable Enables or disables the NAT feature.

nat config <PRIVATEIFNUM> <PUBLICIFNUM> Selects the local and public interfaces.

nat proxy add <ENTRY_NUMBER> <PRIVATEIP> <PUBLICPORT> <LOCALPORT> <PROTOCOL> Adds a proxy server.

nat proxy delete <ENTRY_NUMBER> Deletes a proxy server.

Example:



```
 MIBNav->nat
   NAT Status:
Admin: Enabled    Oper: Enabled    Local Interface: 1   Internet Interface: 2
Local IP          Local mask        Internet IP          Internet mask
192.168.254.254   255.255.255.0    134.141.17.165   255.255.0.0

Connections- TCP: 0, UDP: 0,  ICMP: 0

Local to inet- pkts: 116, bytes: 10814

Inet to local- pkts: 91, bytes: 39812

Errors: cksum: 0, retries: 1, bad packets: 0

Total IP pkts: 3917, Reserved addresses: 2919

 Server List:
 Connections: #
 # Number of valid entries: 0
```

nat

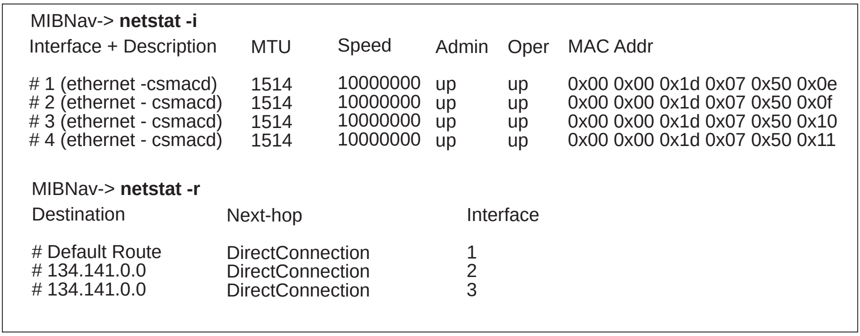
netstat:

Syntax: netstat <option>

Description: The netstat command provides a display of general network statistics for the managed device. The netstat command must be used with one of the two display options.

Options: -i Displays status and capability information for each interface.
-r Displays routing information for each interface.

Example:



```
MIBNav-> netstat -i
Interface + Description   MTU    Speed      Admin   Oper   MAC Addr

# 1 (ethernet -csmacd)    1514   10000000   up      up     0x00 0x00 0x1d 0x07 0x50 0x0e
# 2 (ethernet - csmacd)   1514   10000000   up      up     0x00 0x00 0x1d 0x07 0x50 0x0f
# 3 (ethernet - csmacd)   1514   10000000   up      up     0x00 0x00 0x1d 0x07 0x50 0x10
# 4 (ethernet - csmacd)   1514   10000000   up      up     0x00 0x00 0x1d 0x07 0x50 0x11

MIBNav-> netstat -r
Destination        Next-hop                 Interface

# Default Route    DirectConnection         1
# 134.141.0.0      DirectConnection         2
# 134.141.0.0      DirectConnection         3
```

051470

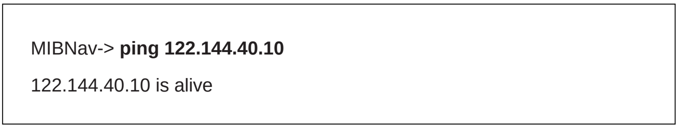
ping:

Syntax: ping [IP address]

Description: The ping command generates an outbound ping request to check the status (alive/not alive) of a device at a specified IP address.

Options: Not Applicable

Example:



```
MIBNav-> ping 122.144.40.10

122.144.40.10 is alive
```

051471

ppp:

Syntax: ppp

Description: The ppp command provides additional status relating to PPP and its Network Control Protocols.

Options: Not Applicable

reset:

Syntax: reset

Description: The reset command allows you to perform a soft reset of the device. You are queried to confirm the reset command to insure against unwanted resets.

The MIB Navigator’s connection to the device is terminated upon execution of this command.

Options: Not Applicable

route:

Syntax: route add <IPADDRESS> <IPADDRESS> <INTERFACENUM>

route add <IPADDRESS> <IPADDRESS> <INTERFACENUM> <METRIC>

route delete <IPADDRESS> <IPADDRESS> <INTERFACENUM>

Description: The route command allows you to add or delete static entries in the IP Forwarding Table for the device. The first address is the destination. The second address is the next hop for the given interface. The metric value is optional. If included, it is used to set the value of **ipForwardingMetric1**. When RIP is used, the metric specifies the distance in hops to the destination.

secondIP:

Syntax: secondIP add <IPADDRESS> <INTERFACENUM>

secondIP delete <IPADDRESS> <INTERFACENUM>

Description: The secondIP command allows you to add or delete secondary IP addresses on the interface.

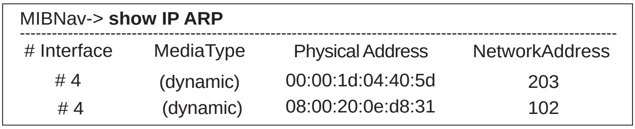
Options: Not Applicable

show:

Syntax: show <PROTOCOL> [TABLE]

Description: The show command displays information concerning various components of the device. Protocols currently supported are IP and IPX. Components of those protocols that are currently supported are ARP caches, route tables, FIB tables, server tables, and interface tables. The number of valid entries in the table is displayed at the end of the table.

Example:



```
MIBNav-> show IP ARP
-----------------------------------------------------------------------------------------------------------
# Interface      MediaType       Physical Address        NetworkAddress
     # 4         (dynamic)       00:00:1d:04:40:5d            203
     # 4         (dynamic)       08:00:20:0e:d8:31            102
```

show

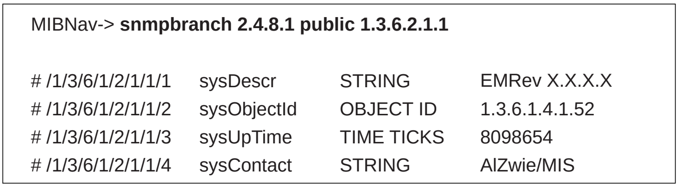
snmpbranch:

Syntax: snmpbranch [IP address] [community name] [OID]

Description: The snmpbranch command enables you to query another SNMP device. The command provides a display of objects that match the specified OID. If no match is made, no object is displayed.

Options: Not Applicable

Example:



```
MIBNav-> snmpbranch 2.4.8.1 public 1.3.6.2.1.1

# /1/3/6/1/2/1/1/1    sysDescr       STRING        EMRev X.X.X.X
# /1/3/6/1/2/1/1/2    sysObjectId    OBJECT ID     1.3.6.1.4.1.52
# /1/3/6/1/2/1/1/3    sysUpTime      TIME TICKS    8098654
# /1/3/6/1/2/1/1/4    sysContact     STRING        AlZwie/MIS
```

051473

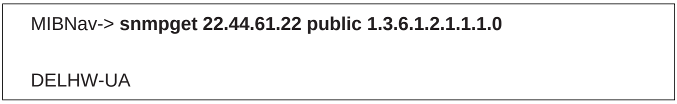
snmpget:

Syntax: snmpget [IP address] [community name] [OID]

Description: The snmpget command enables you to query another SNMP device to obtain a value for a specified object. This command requires the appropriate community string and object id.

Options: Not Applicable

Example:



```
MIBNav-> snmpget 22.44.61.22 public 1.3.6.1.2.1.1.1.0

DELHW-UA
```

051474

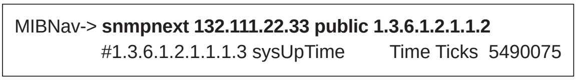
snmpnext:

Syntax: snmpnext [IPADDRESS] [COMMUNITY-STRING] [OBJECT-ID]

Description: The snmpnext command allows you to query another device using SNMP. The next leaf of an object identifier can be retrieved from that device by supplying an appropriate community string and the values of the object identifier.

Options: Not Applicable

Example:



```
MIBNav-> snmpnext 132.111.22.33 public 1.3.6.1.2.1.1.2
           #1.3.6.1.2.1.1.1.3 sysUpTime        Time Ticks  5490075
```

snmpnext

snmpset:

Syntax: snmpset [IP address] [community name]

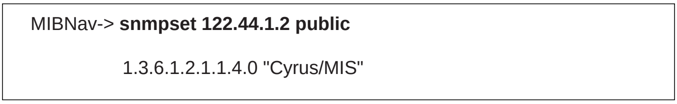
Description: The snmpset command enables you to set the value of an object in other SNMP devices. This command requires the appropriate community string and OID.

When defining a new leaf set, MIB Navigator asks for a value. The following lists possible value types:

(i)nteger - number
(c)ounter - number
(g)auge - number
(t)ime ticks - number
o(p)aque - “value” (with quotation marks)
(s)tring - “value” (with quotation marks)
(o)id - OID number with dotted punctuation
(a)ddress - IP address in DDN format
(m)ac - MAC address in hexadecimal format
(n)ull - no type

Options: Not Applicable

Example:



```
MIBNav-> snmpset 122.44.1.2 public

            1.3.6.1.2.1.1.4.0 "Cyrus/MIS"
```

051475

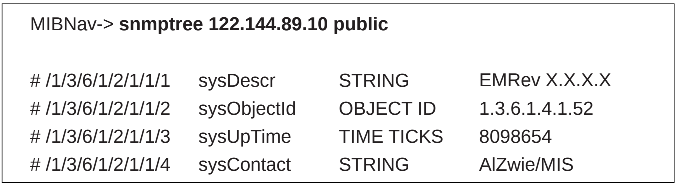
snmptree:

Syntax: snmptree [IP address] [community name]

Description: The snmptree command provides a display of all objects in the device and their corresponding values.

Options: Not Applicable

Example:



```
MIBNav-> snmptree 122.144.89.10 public

# /1/3/6/1/2/1/1/1   sysDescr      STRING       EMRev X.X.X.X
# /1/3/6/1/2/1/1/2   sysObjectId   OBJECT ID    1.3.6.1.4.1.52
# /1/3/6/1/2/1/1/3   sysUpTime     TIME TICKS   8098654
# /1/3/6/1/2/1/1/4   sysContact    STRING       AlZwie/MIS
```

051476

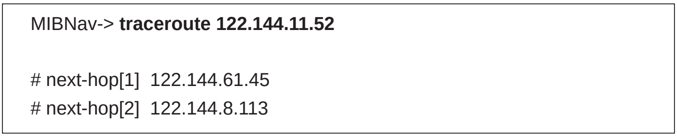
traceroute:

Syntax: traceroute [IP address]

Description: The traceroute command generates a TRACEROUTE request to a specified IP address and provides a display of all next-hop routers in the path to the device. If the device is not reached, the command displays all next-hop routers to the point of failure.

Options: Not Applicable

Example:



```
MIBNav-> traceroute 122.144.11.52

# next-hop[1]  122.144.61.45
# next-hop[2]  122.144.8.113
```

051477

wanpq:

Syntax:

wanpq
wanpq -ea
wanpq -da
wanpq -aip <IPADDRESS>
wanpq -dip <IPADDRESS>

Description:

The wanpq command allows you to configure the WAN Priority Queue database. IPADDRESS is the Internet Protocol (IP) address being added to or removed from the Wide Area Network Priority Queue database.

Options:

wanpq (with no options) Displays status information.
wanpq -ea Enables the WAN Priority Queue Application.
wanpq -da Disables the WAN Priority Queue Application.
wanpq -aip <IPADDRESS> Adds the IP address designated by IPADDRESS to the WAN Priority Queue database.
wanpq -dip <IPADDRESS> Deletes the IP address designated by IPADDRESS from the WAN Priority Queue database.

2.6 SPECIAL COMMANDS

done, quit, exit:

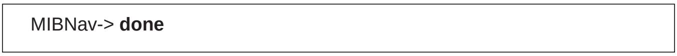
Syntax:

```
done
quit
exit
```

Description: These commands enable you to exit from the MIB Navigator and return to the Main Menu screen.

Options: Not Applicable

Example:



```
MIBNav-> done
```

051472

2.7 PPP SECURITY COMMAND

The following is a new command area for PPP Security.

pppsecurity:

Syntax:

pppsecurity <ifindex#><CHAP><direction><username><secret>

pppsecurity <ifindex#><PAP><direction><peerid><password>

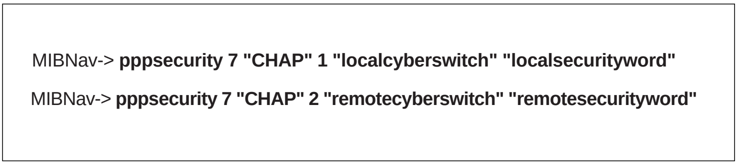
pppsecurity <ifindex#><NONE>

Description: The pppsecurity command allows you to list and set PPP Security on an interface basis.

Options: Not Applicable

Example:

The example below shows the syntax used to set interface 7 to CHAP enabled.



```
MIBNav-> pppsecurity 7 "CHAP" 1 "localcyberswitch" "localsecurityword"
MIBNav-> pppsecurity 7 "CHAP" 2 "remotecyberswitch" "remotesecurityword"
```

051456

2.8 ISDN CONFIGURATION COMMANDS

The following new ISDN configuration commands are used to set up primary and backup configurations.

setbackup:

Syntax:

setbackup <PRIMARYIFNUM> <BACKUPIFNUM><TIMETOCONNECT> <TIMETODISCONNECT> <CONNECTRETRIESNUM> <TIMEBETWEENCONNECTRETRIES> <BACKUPOVERRIDE>

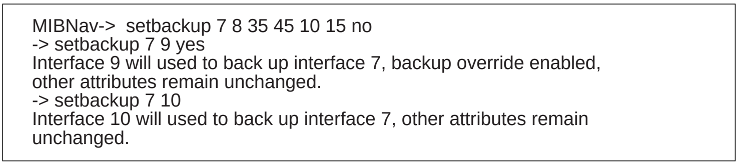
Description:

The setbackup command allows you to configure backup/failover.

Options:

Not Applicable

Example:



```
MIBNav->  setbackup 7 8 35 45 10 15 no
-> setbackup 7 9 yes
Interface 9 will used to back up interface 7, backup override enabled,
other attributes remain unchanged.
-> setbackup 7 10
Interface 10 will used to back up interface 7, other attributes remain
unchanged.
```

051456

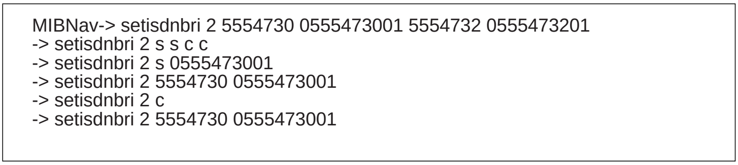
setisdnbri:

Syntax: setisdnbri <WANPORTNUM> <LDN1> <SPID1> <LDN2> <SPID2>

Description: The setisdnbri command allows you to configure BRI.

Options: LDN1, SPID1, LDN2, and SPID2 can be skipped or cleared by entering S/s or C/c respectively. Trailing parameters do not have to be entered.

Example:



```
MIBNav-> setisdnbri 2 5554730 0555473001 5554732 0555473201
-> setisdnbri 2 s s c c
-> setisdnbri 2 s 0555473001
-> setisdnbri 2 5554730 0555473001
-> setisdnbri 2 c
-> setisdnbri 2 5554730 0555473001
```

051456

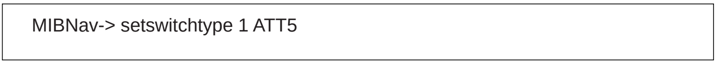
setswitchtype:

Syntax: setswitchtype <WANPORTNUM> <SWITCHTYPE>

Description: The setswitchtype command allows you to set the switch type.

Options: Currently supported switch types are NI1, ATT-4ESS(PRI), ATT-5ESS(BRI), ATT-5ESS(PRI), DMS100(PRI), and DMS100(BRI). Switch type may be set using one of the following: NI1, ATT4, ATT5, DMS100.

Example:



```
MIBNav-> setswitchtype 1 ATT5
```

051456

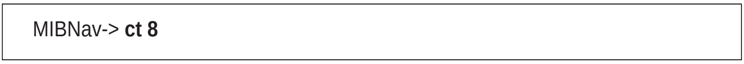
ct:

Syntax: ct <IFNUM>

Description: The ct command allows you to initiate the connection.

Options: Not Applicable

Example:



```
MIBNav-> ct 8
```

051456

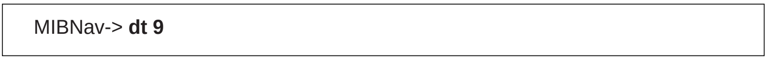
dt:

Syntax: dt <IFNUM>

Description: The dt command allows you to terminate the connection.

Options: Not Applicable

Example:



```
MIBNav-> dt 9
```

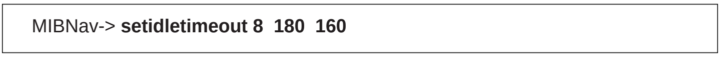
setidletimeout:

Syntax: setidletimeout <IFNUM> <TRANSMITIDLETIMEOUT> <RECEIVEIDLETIMEOUT>

Description: This setidletimeout command allows you to set the idle time out value in seconds in which a packet needs to be transmitted/received before the interface is automatically disconnected.

Options: Not Applicable

Example:



```
MIBNav-> setidletimeout 8  180  160
```

051456

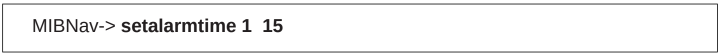
setalarmtime:

Syntax: setalarmtime <WANPORTNUM> <ALARMTIMEOUT>

Description: This setalarmtime command allows you to set the time out value in seconds in which the physical port must remain in a failed state to begin the backup procedure.

Options: Not Applicable

Example:



```
MIBNav-> setalarmtime 1  15
```

051456

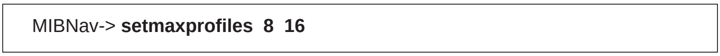
setmaxprofiles:

Syntax: setmaxprofiles <IFNUM> <MAXPROFILESNUM>

Description: This setmaxprofiles command allows you to set the maximum number of profiles for an interface.

Options: Not Applicable

Example:



```
MIBNav-> setmaxprofiles  8  16
```

051456

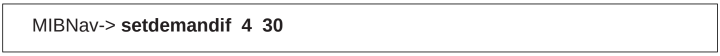
setdemandif:

Syntax: setdemandif <DEMANDIFNUM> <TIMEBETWEENCONNECTRETRIES>

Description: This setdemandif command allows you to set the amount of time between retries to reconnect a primary demand interface which has failed.

Options: Not Applicable

Example:



```
MIBNav-> setdemandif  4  30
```

051456

isdnstat:

Syntax: isdnstat <WANPORTNUM>

Description: This isdnstat command allows you to list the ISDN settings and the Signalling channel status.

Options: Not Applicable

Example:

```
MIBNav-> isdnstat 1
```

CHAPTER 3
ADDITIONAL INFORMATION

This chapter contains the following information:

- Frame relay error information

3.1 FRAME RELAY ERROR TABLE

This table is a standard part of RFC 2115, and provides the following information on a physical interface per physical interface basis:

- The time of the failure: (value of Mib II sysUpTime)
- The type of failure

receiveShort:The frame was not long enough to allow demultiplexing - the address field was incomplete, or for virtual circuits using Multiprotocol over Frame Relay, the protocol identifier was missing or incomplete.

receiveLong:The frame exceeded maximum length configured for this interface.

illegalAddress:address field did not match configured format.

unknownAddress:frame received on a virtual circuit which was not active or administratively disabled.

dlcmiProtoErr:unspecified error occurred when attempting to interpret link maintenance frame.

dlcmiUnknownlE:link maintenance frame contained an Information Element type which is not valid for the configured link maintenance protocol.

dlcmiSequenceErr:link maintenance frame contained a sequence number other than the expected value.

dlcmiUnknownRpt:link maintenance frame contained a Report Type Information Element whose value was not valid for the configured link maintenance protocol.

noErroSinceReset:no errors have been detected since the last cold start or warm start.

- The number of times the interface has gone down due to faults
- The value of sysUpTime when the interface last went down due to errors.

INDEX

digital

9032784 Printed in U.S.A.