HOTWIRE® DSL ROUTERS

USER'S GUIDE

Document No. 6371-A2-GB20-10

August 2000

PARADYNE®

Notice

Warranty, Sales, Service, and Training Information

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

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

Document Feedback

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

Trademarks

Contents

3 Configuring the DSL Router

4 DSL Router Configuration Examples

5 Monitoring the DSL Router

6 Diagnostics and Troubleshooting

A Command Line Interface

B Configuration Defaults & Command Line Shortcuts

C Traps & MIBs

D DSL Router Terminal Emulation

Index

About This Guide

Document Purpose and Intended Audience

This guide describes how to configure and operate Hotwire DSL routers. This document addresses the use of the following Hotwire DSL Router models:

- Hotwire 6301/6302 IDSL Router
- Hotwire 6341/6342 Symmetric DSL Router
- Hotwire 6371 RADSL Router

This document is intended for administrators and operators who maintain the endpoints at customer premises. A basic understanding of internetworking protocols and their features is assumed. Specifically, you should have familiarity with the following internetworking concepts:

- TCP/IP applications
- IP and subnet addressing
- IP routing
- Bridging

It is also assumed that you have already installed a Hotwire DSL Router. If not, refer to *Product-Related Documents* on page vii for installation documents.

Document Summary

Section	Description
Chapter 1	*Introduction to Hotwire DSL Routers.* Provides an overview of the Hotwire DSL Routers.
Chapter 2	*Accessing the DSL Router.* Describes the Hotwire DSL Routers access control and provides instructions on how to log in and log out of the system.
Chapter 3	*Configuring the DSL Router.* Describes the DSL router interfaces, Domain Types, IP Routing, and network considerations.
Chapter 4	*DSL Router Configuration Examples.* Presents several common DSL router configuration examples.
Chapter 5	*Monitoring the DSL Router.* Describes operator programs that monitor the Hotwire system.
Chapter 6	*Diagnostics and Troubleshooting.* Describes common Hotwire operational problems and solutions. Contains SysLog information.
Appendix A	*Command Line Interface.* Provides explanation of the DSL router's Command Line Interface and command syntax with examples.
Appendix B	*Configuration Defaults & Command Line Shortcuts.* Provides a list of all configuration options with factory default settings and a list of all command line shortcuts with the abbreviated command line input.
Appendix C	*Traps & MIBs.* Summarizes the MIBs and SNMP traps supported by the DSL routers.
Appendix D	*DSL Router Terminal Emulation.* Provides configuration setup procedures for two common text file programs.
Index	Lists key terms, acronyms, concepts, and sections in alphabetical order.

A master glossary of terms and acronyms used in Paradyne documents is available on the Web at **www.paradyne.com**. Select *Library* → *Technical Manuals* → *Technical Glossary.*

Product-Related Documents

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

Document Number	Document Title
6301-A2-GN10	*Hotwire 6301/6302 IDSL Routers Installation Instructions*
6341-A2-GN10	*Hotwire 6341/6342 Symmetric DSL Routers Installation Instructions*
6371-A2-GN10	*Hotwire 6371 RADSL Router Installation Instructions*
8000-A2-GB22	*Hotwire Management Communications Controller (MCC) Card, IP Conservative, User's Guide*
8000-A2-GB26	*Hotwire IP MVL, RADSL, IDSL, and SDSL Cards, Models 8310/8312/8314, 8510/8373/8374, 8303/8304, and 8343/8344, User's Guide*

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

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

Document Conventions

The following syntax is used throughout this document.

Syntax	Translation
[ ]	Square brackets represent an optional element.
{ }	Braces represent a required entry.
|	Vertical bar separates mutually exclusive elements.
Italics	Entry is a variable to be supplied by the operator.
Bold	Enter (type) as shown.
x.x.x.x	32-bit IP address and mask information where *x* is an 8-bit weighted decimal notation.
xx:xx:xx:xx:xx:xx	MAC address information where *x* is a hexadecimal notation.

Introduction to Hotwire DSL Routers

1

What is a Hotwire DSL Router?

The Hotwire® DSL (Digital Subscriber Line) Router operates as an IP router connecting a DSL link to an Ethernet network. This system provides high-speed access to the Internet or a corporate network over a traditional twisted-pair copper telephone line to the end user.

DSL Technologies Supported

Paradyne's Hotwire DSL network supports the following types of technologies:

- Hotwire IDSL (ISDN DSL) products provide IDSL multirate symmetric packet transport and can operate over a connection with an ISDN repeater or digital facilities. Data rates of 64 kbps, 128 kbps, or 144 kbps can be configured.
- Hotwire RADSL (Rate Adaptive DSL) products are applicable for both asymmetric and symmetric applications. The 1 Mbps symmetric operation is ideal for traditional business applications while the 7 Mbps downstream with 1.1 Mbps upstream asymmetric operation provides added bandwidth for corporate Internet access. RADSL products can also save line costs by optionally supporting simultaneous data and voice over the same line.
- Hotwire SDSL (Symmetric DSL) packet-based products provide high-speed symmetric DSL services with bandwidth for business applications. These products are configurable from 144 kbps up to 2.3 Mbps. This gives service providers the opportunity to sell multiple services with a single product.

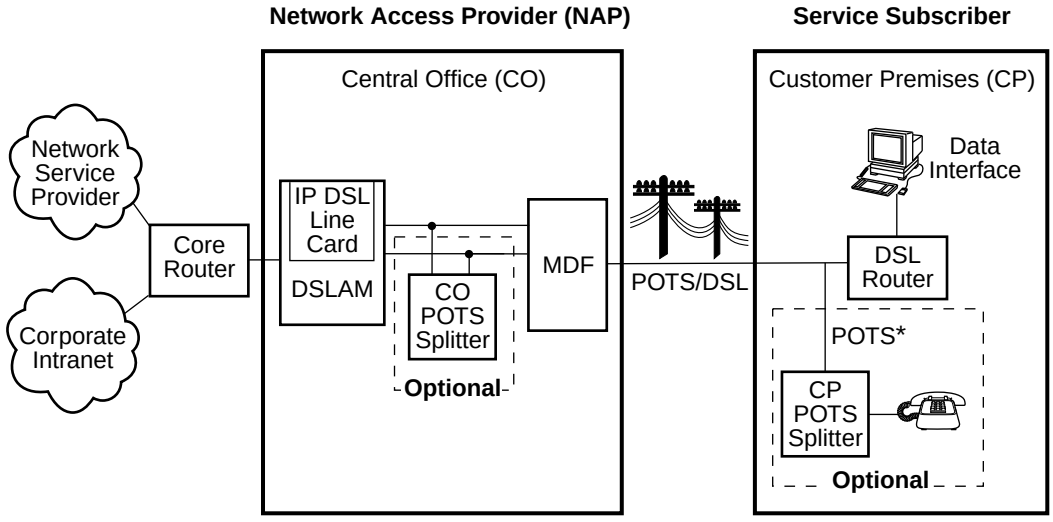
Typical DSL Router System

DSL is a local loop technology that uses standard twisted-pair copper wire to support high-speed access over a single pair of twisted copper wires. DSL applications are point-to-point, requiring DSL devices at the central site and at the end-user site.

The Hotwire DSL routers interoperate with the following types of Hotwire IP DSL cards (at the DSLAM/GranDSLAM chassis) to deliver applications at high speeds in support of packet services over a DSL link:

- The Hotwire 8303 or 8304 IP IDSL Cards interoperate with two Hotwire IDSL Routers:
  - — Hotwire 6301 IDSL Router with one Ethernet port
  - — Hotwire 6302 IDSL Router with a 4-port Ethernet hub
- The Hotwire 8343 or 8344 SDSL Cards interoperate with two Hotwire Symmetric DSL Routers:
  - — Hotwire 6341 SDSL Router with one Ethernet port
  - — Hotwire 6342 SDSL Router with a 4-port Ethernet hub
- The Hotwire 8510, 8373, and 8374 IP RADSL Cards interoperate with the Hotwire 6371 RADSL Router with one Ethernet port

The following illustration shows a typical Hotwire system with a Hotwire DSL Router. All Hotwire DSL routers transport data. The Hotwire 6371 RADSL Router can transport data and POTS simultaneously.



Hotwire DSL Router Features

The Hotwire DSL routers contain the following features.

- **IP routing with**:
  - — NAT (Network Address Translation)
  - — NAPT (Network Address Port Translation)
  - — DHCP Server (Dynamic Host Configuration Protocol) and DHCP Relay Agent
  - — A full set of IP filters
  - — SNMP Set/Get capability
- **High-speed Internet or intranet access.**
- **Diagnostics.** Provides the capability to diagnose device and network problems and perform tests.
- **Device and Test Monitoring.** Provides the capability of tracking and evaluating the unit's operation.
- **Remote Firmware Download.** Provides easy setup and activation of firmware upgrades from a remote location.
- **Security.** Provides multiple levels of security, which prevents unauthorized access to the DSL router.
- **Console Terminal Interface.** Provides an interface for:
  - — Configuring and managing the DSL router.
  - — Remote terminal access via Telnet.
  - — Management from an NMS using SNMP.

Service Subscriber

The Service Subscriber is the user (or set of users) that has contracted to receive networking services (e.g., Internet access, remote LAN access) for the end-user system from an NSP (Network Service Provider). Service subscribers may be:

- Residential users connected to public network services (e.g., the Internet)
- Work-at-home users connected to their corporate intranet LAN
- Commercial users at corporate locations (e.g., branch offices) connected to other corporate locations or connected to public network services

The Hotwire DSL Router must be installed at the customer premises to provide the end user with access to any of the above services.

NOTE:

If you would like more information on DSL-based services, applications, and network deployment, refer to Paradyne's *The DSL Sourcebook.* The book may be downloaded or ordered through Paradyne's World Wide Web site at **www.paradyne.com/library**.

Accessing the DSL Router

2

Access Control to the DSL Router

The Hotwire DSL Router can be managed from an NMS using SNMP or from the command line interface. There are two methods to access the command line interface:

- Local access at the DSL router through the Console port, or
- Access by a Telnet session (controlled through the management interface at the Hotwire chassis).

When a local console connection is first established, a login prompt appears. The Hotwire DSL Router accepts only one login session at a time. The DSL Router is configured at the factory with a default login ID and password. However, to provide login security to the DSL system, configure a new login ID and password.

Levels of Access

There is one login ID and two levels of privileges on the Hotwire DSL system. Your user account can be configured with one user name and different passwords for:

- **Administrator**. The Administrator has two levels of access to the DSL router.
  - — Administrator, non-configuration mode: Provides read-only capabilities. This is the same level of access as Operator.
  - — Administrator, configuration mode: Provides complete write access to the DSL router. However, MIB sets are done from the NMS vs. the command line.
- **Operator**. The Operator has read-only access to display device information with no modification permission and no access to management functions.

Refer to Appendix A, *Command Line Interface*, for access level details for each command line entry.

Changing Access Session Levels

- You can change the Administrator access level by entering:

  `admin enable`

  This command provides Administrator access level privileges. The DSL router will respond with a prompt to enter the password for Administrator access.

- You can end the Administrator access level by entering:

  `admin disable`

  This command results in ending the Administrator access level session. No password is needed.

  Entering **`exit`** has the same results. Refer to *Exiting from the System* on page 2-5 for further details on ending a session.

The Operator and Administrator have the same Login ID with different passwords for their access level. To determine the level of access for a session, refer to *Determining the Current Access Level* on page 2-4.

Local Console Access

The DSL router ships with the local console enabled. After login, the local console can be disabled with the command **`console disable`**. After saving this change and ending the session, there is no local access through the console port. Any access must be through a Telnet session or the NMS.

NOTE:

Entering **`console disable`** results in NO local access to the DSL router. If you attempt to log in, you will receive an error message.

To determine via a Telnet session if a console is enabled, enter:

`show console`

The display returned for the show console command will be:

- **`console enabled`** – Command line management at the console is available, or
- **`console disabled`** – No command line management is available at the console.

For steps to set up the new user's login, refer to *Setting Up the New User's Login* on page 2-3.

Setting Up the New User's Login

The DSL router will provide the login prompt when the local console connection is first established. When the login prompt appears, a locally connected console defaults to Console Enabled with Operator access only.

▶ Procedure

For first-time access to the Hotwire DSL Router's command line interface:

1. At the initial **`login>`** prompt, type the default login ID **`paradyne`** and press Enter.
2. At the **`password>`** prompt (for Operator), type the default password **`abc123`** and press Enter.

   The login ID and password fields are validated together.
3. At the system identity of **`CUSTOMER>`** prompt, type **`admin enable`** and press Enter.
4. At the **`password>`** prompt (for Administrator), type the default password **`abc123`** and press Enter.
5. The system identity will change to the Administrator display mode of **`CUSTOMER#>`**. Type **`configure terminal`** and press Enter.
6. The system identity will change to the Administrator configuration mode of **`CUSTOMER - CONFIG#>`**.
7. To change the login ID, enter text to replace the default of paradyne:

   `name` *your new login ID*

   NOTE:

   The Login ID and Password fields are NOT case-sensitive.
8. Enter a new password and specify the level:

   `password` *level password*

   Example: type **`password operator 238clrd3`** and press Enter.

   Both the Login ID and the Password fields are 1–31 printable alphanumeric ASCII characters in the ASCII hex range of 0x21–0x7E. No spaces are allowed. The following table lists the invalid characters.

Invalid Characters	Value	ASCII Hex Translation
#	Number sign	0x23
$	Dollar sign	0x24
%	Percentage	0x25
&	Ampersand	0x26

9. At the prompt, enter the new Administrator-level password to replace abc123:

   `password admin` *new password* and press Enter

   `save` and press Enter

   NOTE:

   Any input during an Administrator configuration session must be saved while still in configuration mode.

For more information regarding the system identity, refer to *Determining the Current Access Level,* below.

If you are denied access during a Telnet session, the session stops and an error is logged. If you accessing the DSL router locally and a Telnet session is active, you will receive a message:

```
Local console disabled by conflict
```

Telnet Access

The Telnet access defaults to Administrator level. If the login is at the Operator level, then Operator level access is available. Telnet access is always enabled.

Determining the Current Access Level

The command line prompt displays the access level. The factory default for System identity is **`CUSTOMER>`**. You can set your own system identity name to replace CUSTOMER. See the example below.

If the prompt format appears as . . .	Then the DSL router access level is . . .	And if you entered a System identity of PARADYNE, the prompt displays . . .
CUSTOMER>	Operator, display mode	PARADYNE>
CUSTOMER #>	Administrator, display mode	PARADYNE #>
CUSTOMER – CONFIG#>	Administrator, configuration mode	PARADYNE – CONFIG#>

Determining the Available Commands

To determine the commands available at the current login access level, enter:

- **`help`** or
- **?** (question mark)
- the command without any parameters

Using the List Command

The list command displays a sequence of commands, in the form of ASCII strings, that would have the effect of setting all configuration settings to the current values. (The two passwords are not output.)

To determine the commands available, enter the Administrator configuration mode and enter either:

- **`list`**

  Displays the output in on-screen page mode. In on-screen page mode, the user interface displays 23 lines of information. When the 24th line is reached, **`More...`** is displayed. Pressing any key will display the next page.

- **`list config`**

  Displays the output in scroll mode as a text file. Scroll mode captures and displays all command strings in a text file for use with a terminal emulation program. Refer to Appendix D, *DSL Router Terminal Emulation*.

Changing the System Identity

▶ Procedure

To change the System Identity from the factory default of CUSTOMER>:

1. Login and enter the ADMIN-configuration mode.
2. At the CUSTOMER-CONFIG#> prompt, type the new System identity (no spaces allowed), press Enter, type **`save`**, and press Enter.

   `system identity` *new system identity*

   For example:

   `system identity PARADYNE` and press Enter

   `save` and press Enter
3. In this example, after saving the entry and ending the configuration mode, the System identity will display:

   `PARADYNE #>`

   The System identity is the same as the MIB entry of sysName. The sysContact and SysLocation MIB entries are not displayed.

Exiting from the System

You can manually log out of the system, or let the system automatically log you out. The DSL router will log you out immediately if you disconnect the Console cable. Any unsaved configuration input will be lost.

Manually Logging Out

To log out, there are two commands: logout and exit.

▶ Procedure

To log out of the Hotwire DSL Router command line session or Telnet session:

1. At the **>** prompt, type **`logout`** and press Enter.
2. The system ends the session immediately. Any configuration updates must be saved before exiting or the updates will be lost.

▶ Procedure

To exit the Hotwire DSL Router's current access level:

1. At the **>** prompt, type **`exit`** and press Enter. If there are any unsaved configuration changes, you will be prompted to save changes before exiting.
2. The exit command has the following effect:

If you are accessing the DSL router . . .	Then . . .
At the Local console and logged in at the Administrator level, configuration mode	You are placed at the Operator level and any configuration updates must be saved or the updates will be lost.
At the Local console and logged in at the Administrator level, non-configuration mode	You are placed at the Operator level.
At the Local console and logged in at the Operator level	The Exit command responds exactly like the Logout command.
Via a Telnet session and logged in at any access level	Entering either of the following ends the Telnet session immediately: ■ Exit ■ Ctrl +] (right bracket)

Automatically Logging Out

The DSL router has an automatic timeout feature that logs you out of the system after five minutes of inactivity. Any input that is not saved is lost. You will need to log back in.

At the console, press Enter to display the **`login>`** prompt to log back in. The **`autologout {enable | disable}`** command default is enabled. Unsaved configuration input is lost.

When autologout is:

- Enabled, the current configuration is retained through a power recycle.
- Disabled, the system inactivity timer is disabled.

Configuring the DSL Router

3

Overview of DSL Router Configuration

The Hotwire DSL Routers support various customer premises distribution networks that contain IP forwarding devices or routers, in addition to locally attached hosts or subnets. The Hotwire DSL Router has an IP Routing Table that contains IP address and subnet mask information.

The DSL router supports Internet Protocol as specified in RFC 791 and Internet Control Message Protocol (ICMP) as specified in RFCs 792 and 950. The DSL router acts as a router (or gateway) as defined in RFC 791.

For more information on supported RFCs, refer to Appendix C, *Traps & MIBs*.

Interfaces for the DSL Router

The Hotwire DSL Router has two interfaces:

- **DSL Interface**

  The Hotwire DSL Router interface type is determined by the model number:

  — 6301 and 6302 are Hotwire IDSL Routers

  — 6341 and 6342 are Hotwire SDSL Routers

  — 6371 is a Hotwire RADSL Router

  The DSL interface has a unique MAC address assigned before shipping.

- **Ethernet Interface**
  - — All DSL routers have an Ethernet interface with a unique MAC address assigned before shipping.
  - — The Ethernet interface is a 10/100BaseT interface that automatically negotiates the rate. If all attached Ethernet devices support 100BaseT, the DSL router will default to 100BaseT. Otherwise, the DSL router operates at 10BaseT.
  - — The DSL router can be configured for either DIX format or IEEE 802.3 format. When the DSL router is configured to use IEEE 802.3 format, the DSL router uses SNAP encapsulation as specified in RFC 1042.
  - — The Hotwire 6302 IDSL and the 6342 SDSL Routers each have a hub configuration with four Ethernet connectors. The hub acts as a bit-level repeater. There is logically one Ethernet communications interface and one single collision domain.
  - — The DSL router only accepts frames on the Ethernet interface with its own MAC address or a broadcast or multicast MAC address.

Ethernet and DSL Interface Identifiers

The following are the naming conventions used for the Hotwire DSL Router interfaces:

- **eth1** (or **e0**) – Ethernet interface name.
- **dsl1** (or **d0**) – DSL interface name.

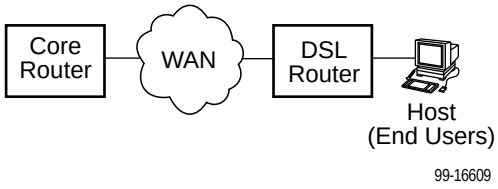
Service Domain IP Address Assignments

- Multiple Service Domains can be defined using network addresses and subnet masks.
- For both the DSL interface and the Ethernet interface, four Service Domain IP Addresses and subnet masks can be defined.

Numbered DSL Interface

In this scenario, the hosts attached to the DSL router's Ethernet interface are on a different logical network than the core router. The DSL router is the next hop router for the hosts. The upstream next hop router for the DSL router is the core router.

Simplified Network Topology



The hosts can be assigned IP addresses on the network attached to the DSL router's Ethernet interface. The upstream next hop router is assigned an address on a different logical network than the hosts.

Actions required to configure the DSL router interfaces in this scenario:

- Assign IP address to Ethernet interface: eth1
- Assign IP address to DSL interface: dsl1
- Assign upstream next hop router

Unnumbered DSL Interface

In this LAN extension application scenario, the hosts connected to a corporate network for virtual office connection or teleworkers want to look like they are on the same network as the core router. The core router will be the next hop router for the hosts.

Actions required to configure the DSL router interfaces in this scenario:

- Assign IP address to Ethernet interface: eth1
- Specify the DSL interface as unnumbered: dsl1
- Assign upstream next hop router
- Enable Proxy ARP for both the eth1 and dsl1 interfaces
- Disable scoping on the DSL card at the DSLAM/GranDSLAM chassis

IP Routing

The DSL router uses destination-based routing for downstream traffic. An IP Routing Table is maintained to specify how to forward IP datagrams downstream. The DSL router is capable of supporting 32 entries in the IP Routing Table. This table can be viewed by both Operator and Administrator access levels.

The DSL router uses source-based forwarding for upstream traffic to ensure that packets are forwarded to the upstream router specified for the configured Service Domain.

Refer to Chapter 4, *DSL Router Configuration Examples*, for further details.

Network Considerations

The DSL routers can be configured to function in a variety of network environments. The following sections provide descriptions of some of the DSL router features:

- *Address Resolution Protocol (ARP)*
- *Proxy ARP*
- *Network Address Translation (NAT)*
  - *Basic NAT*
  - *Network Address Port Translation (NAPT)*
  - *IP Options Processing*
  - *Applications Supported by NAT*
- *Dynamic Host Configuration Protocol (DHCP) Server*
- *DHCP Relay Agent*
- *Security*
  - *IP Filtering*
  - *Land Bug/Smurf Attack Prevention*
- *Routed vs. Bridged PDUs*

Address Resolution Protocol (ARP)

Address Resolution Protocol, as specified in RFC 826, is supported in the DSL router. The DSL router provides for a total of 265 ARP table entries. The timeout for completed and uncompleted ARP table entries is configurable.

NOTE:

The DSL router does not process ARP requests and ARP responses on its DSL interface when it is configured to support RFC 1483 PDU routing (Standard mode). See *Routed vs. Bridged PDUs* on page 3-10 for more information. The operating mode (Standard or VNET) can be changed from the DSL card without requiring any reconfiguration of the DSL router. If any static ARP entries have been configured, they will remain in the database and can be displayed with the **`show arp`** command. You can create static ARP entries regardless of the current operating mode.

The Command Line Interface provides the ability to:

- Create up to 64 static ARP table entries to be retained across power cycles.
- Display the ARP table.
- Delete ARP table entries.
- Display and delete automatically added static ARP table entries by the DHCP server and relay functions. Refer to *Dynamic Host Configuration Protocol (DHCP) Server* on page 3-7.

Proxy ARP

The DSL router supports Proxy ARP. Proxy ARP responses are based on the IP Routing table contents. The IP Routing table must have an entry for every host that is reachable on the Ethernet interface, including hosts for which the DSL router will not forward packets because of IP filters. If an ARP request is received on one interface for an IP address that is reachable on the other interface, the DSL router will respond with its own MAC address.

NOTE:

The Proxy ARP option is not available on the DSL interface when the DSL router is configured to support RFC 1483 PDU routing. See *Routed vs. Bridged PDUs* on page 3-10 for more information.

The Command Line Interface provides the ability to enable and disable Proxy ARP for each interface.

NOTES:

— When Basic NAT is enabled, the DSL interface (dsl1) must have Proxy ARP enabled if the dsl1 interface address is part of the Basic NAT global IP network address.

— Proxy ARP and NAPT cannot be enabled at the same time.

Network Address Translation (NAT)

Network Address Translation is used when a private network's internal IP addresses cannot be used outside the private network. The IP addresses may be restricted for privacy reasons or they may not be valid public IP addresses.

The DSL router provides NAT as described in *RFC 1631 The IP Network Address Translator (NAT)*. NAT allows the private (local) hosts to transparently access public (global) external IP addresses.

Two variations of traditional NAT are supported:

- Basic NAT
- Network Address Port Translation (NAPT)

NOTE:

Basic NAT and NAPT cannot be enabled at the same time.

Basic NAT

Basic NAT allows hosts in a private network to transparently access the external network by using a block of public addresses. Static mapping enables access to selected local hosts from the outside. Basic NAT is often used in a large organization with a large network setup for internal use and the need for occasional external access.

Basic NAT provides a one-to-one mapping by translating a range of assigned public IP addresses to a similar-sized pool of private addresses (typically from the 10.*x.x.x* address space). Each local host currently communicating with a external host appears to have an unique IP address. Up to 256 IP addresses can be allocated for use with Basic NAT.

Network Address Port Translation (NAPT)

NAPT allows multiple clients in a local network to simultaneously access remote networks using a single IP address. This benefits telecommuters and SOHO (Small Office/Home Office) users that have multiple clients in an office running TCP/UDP applications. NAPT is sometimes referred to as PAT (Port Address Translation).

NAPT provides a many-to-one mapping and uses one public address to interface numerous private users to an external network. All hosts on the global side view all hosts on the local side as one Internet host. The local hosts continue to use their corporate or private addresses. When the hosts are communicating with each other, the translation is based on the IP address and the IP port numbers used by TCP/IP applications.

IP Options Processing

The NAT and NAPT functions handle and process the IP datagrams with options set as described below. No command is available to set IP options.

The DSL Router does not process (and drops) any IP datagrams with the following IP options:

- Loose source and record route (type 131)
- Strict source and record route (type 133)
- Security (type 130)
- Stream ID (type 136)

The DSL Router does process IP datagrams with the following IP options, but does not provide its IP address or timestamp information in the response message:

- Record route (type 7)
- Timestamp (type 68)

Applications Supported by NAT

The DSL routers support the following applications and protocols:

- FTP
- HTTP
- NetMeeting
- Ping
- RealPlayer
- Telnet
- TFTP

Dynamic Host Configuration Protocol (DHCP) Server

The DSL router provides a DHCP Server feature as specified in RFC 2131, Dynamic Host Configuration Protocol, and RFC 2132, DHCP Option and BOOTP Vendor Extensions. DHCP is the protocol used for automatic IP address assignment.

DHCP setup considerations:

- The range of IP addresses to be used by the DHCP server must be configured. The maximum number of clients is 256.
- The DHCP server must be enabled.

- When the DHCP IP address range is changed, all binding entries, automatically added routes, and ARP table entries for the clients configured with the old address range are removed.
- When the DHCP Server is enabled, there can be only one service domain (Ethernet interface) configured.
- The IP address for the next hop router that is provided to the hosts in the DHCP reply must be configured.
- The subnet mask can be configured along with the IP address range (optional).
- The DHCP server domain name can be configured (optional).
- The Domain Name Server (DNS) IP address can be configured (optional).
- The minimum and maximum lease time settings can be configured.

For additional information, refer to Chapter 4, *DSL Router Configuration Examples*.

DHCP Relay Agent

The DSL router provides the capability of serving as a DHCP Relay Agent, as specified in RFC 2131, Dynamic Host Configuration Protocol. The DSL router provides the capability to enable and disable the DHCP Relay Agent and to configure the IP address of the DHCP server to which the DHCP requests are to be forwarded.

The DHCP server assigns an IP address to the end-user system. When DHCP Relay is enabled, it is possible to limit the number of DHCP clients. The DSL router's IP Routing table and ARP table are automatically updated. The DHCP relay agent in the DSL router should be used when there is a DHCP server upstream in the service domain. DHCP relay agent setup considerations:

- DHCP server IP address must be configured.
- DHCP relay must be enabled.
- The number of DHCP clients can be limited to 1—256.
- DHCP server and DHCP relay functions cannot be enabled at the same time.
- NAT and DHCP relay cannot be enabled at the same time.

Security

The DSL router offers security via the following:

- **IP Filtering** – Can be enabled or disabled.
- **Land Bug/Smurf Attack Prevention** – Always present.

IP Filtering

NOTE:

All Hotwire DSL Router filters are configured on the Hotwire DSL card.

By default, filtering is disabled on the Hotwire DSL card for the DSL router. If enabled, filtering provides security advantages on LANs by restricting traffic on the network and hosts based on the IP source and/or destination addresses.

IP packets can be filtered based on:

- Destination IP Address
- IP Protocol Type
- Source and Destination Port Number (if applicable)
- Source IP Address
- TCP Filter (prevents the receipt of downstream TCP connect requests)

NOTE:

If the Source IP Address filter is enabled on the Hotwire card and an IP address is assigned to the DSL interface, there must also be an entry configured in the Hotwire Client Table for the DSL interface's IP address.

For more information about IP filtering, see the *Hotwire MVL, RADSL, IDSL, and SDSL Cards, Models 8310/8312, 8510/8373/8374, 8303/8304, and 8343/8344, User's Guide.*

Land Bug/Smurf Attack Prevention

Land Bug and Smurf Attack prevention are enhanced firewall features provided by the DSL Router:

- **Land Bug** – The DSL router drops all packets received on its DSL interface or Ethernet interface when the source IP address is the same as the destination IP address. This prevents the device from being kept busy by constantly responding to itself.
- **Smurf Attack** – The DSL Router will not forward directed broadcasts on its DSL and Ethernet interfaces, nor will it send an ICMP echo reply to the broadcast address. This ensures that a legitimate user will be able to use the network connection even if ICMP echo/reply (smurf) packets are sent to the broadcast address.

Routed vs. Bridged PDUs

The DSL router supports both the VNET model and the 1483 Routed model (derived from RFC 1483) for the transportation of PDUs (Protocol Data Units) from the DSL router to the router in the core network. When operating in Standard mode, the DSL router supports both routed and bridged PDUs. When operating in VNET mode, the DSL router supports bridged PDUs only.

NOTE:

Standard mode vs. VNET mode is configured on the DSL card at the DSLAM/GranDSLAM chassis.

Both ends of the network (e.g., the DSL router and the DSL line card or the core router) must be configured to operate the same way (i.e., routed or bridged).

If Using This Network Model . . .	Then These DSL Cards Can Be Used . . .
1483 Routed or Bridged (Standard Mode)	Model 8303 24-port IDSL Model 8344 24-port SDSL Model 8374 12-port RADSL
1483 Bridged (VNET Mode)	Models 8303/8304 24-port IDSL Models 8343/8344 24-port SDSL Models 8373/8374 12-port RADSL Model 8510 12-port RADSL

The following diagram illustrates the 1483 Routed model (Standard mode) in the network.

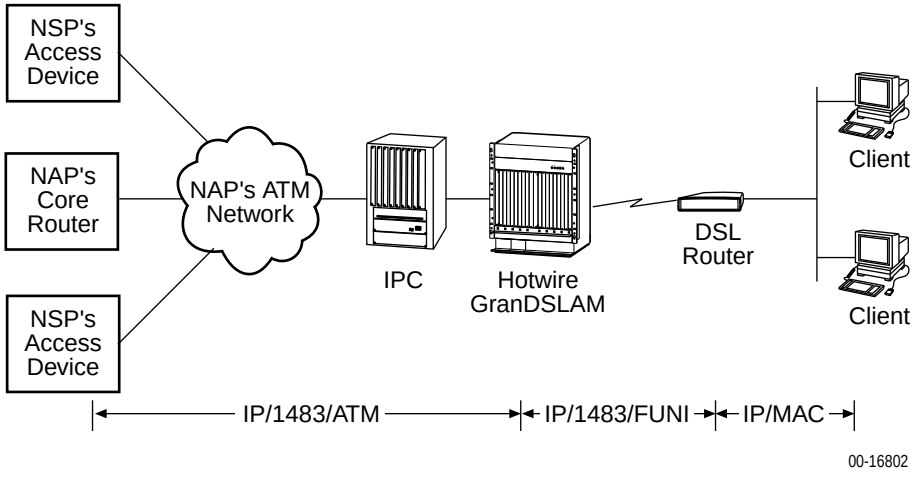


Figure 3-1. 1483 Routed Network Model (Standard mode)

DSL Router Configuration Examples

4

Configuration Examples

The Hotwire DSL Router configuration examples include only a few of the possible scenarios. This chapter covers some of the common configurations. The command syntax will vary based on your network setup.

Configuration commands require the access level of Administrator-Config and changes need to be saved while in configuration mode to take effect. Refer to Chapter 2, *Accessing the DSL Router*.

The Hotwire DSL Router configuration examples include:

- Basic
- Basic NAT
- NAPT
- Unnumbered DSL Interface with Proxy ARP
- DHCP Relay with Proxy ARP
- DHCP Server with Basic NAT
- Downstream Router

Refer to Appendix A, *Command Line Interface,* for specific commands and syntax.

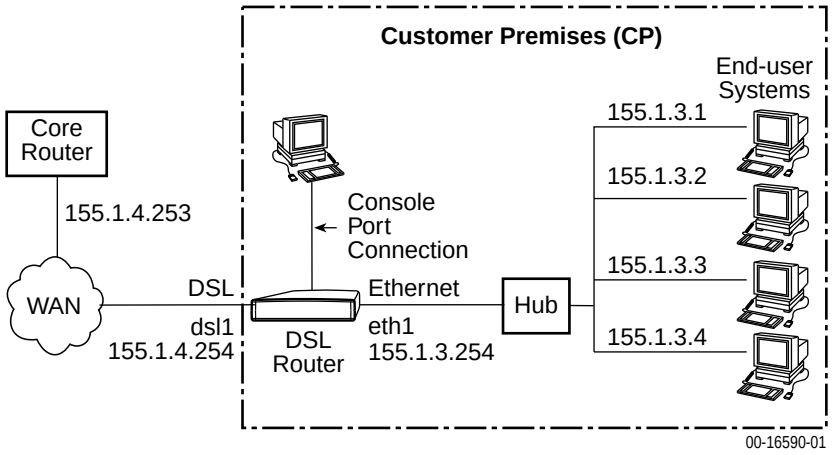
Refer to Appendix B, *Configuration Defaults & Command Line Shortcuts*, for specific command default settings and abbreviated command line syntax.

NOTES:

— The examples in this chapter are provided to illustrate some of the features of the Hotwire DSL Routers. Not all possible feature configurations are covered in the examples.

— The IP addresses used in the examples are for illustrative purposes only. These addresses are not intended for use when configuring your local network.

Basic Configuration Example



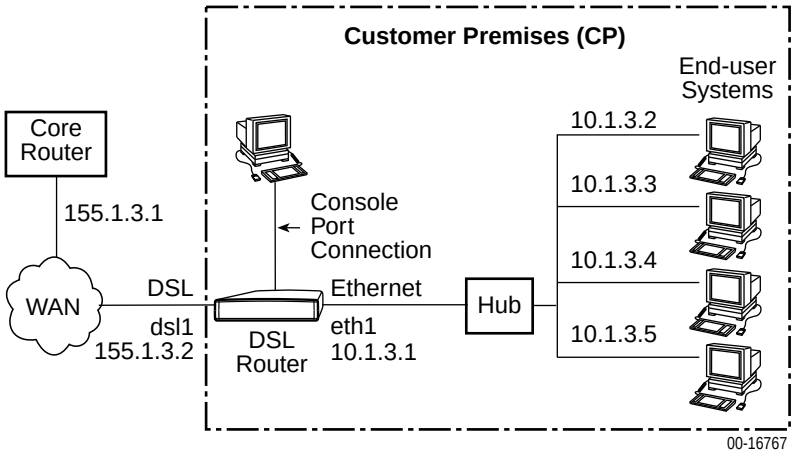
In this basic example:

- There are multiple clients with statically assigned public IP addresses configured on the Ethernet side of the DSL router.
- The IP addresses of the clients are contained within the subnet specified by the configured Ethernet IP address and subnet mask.
- The next hop router (default gateway) of the clients is the Ethernet interface (eth1) of the DSL router.
- The next hop router for downstream forwarding from the core router is the DSL interface (dsl1) of the DSL router.

The command line syntax for this example is:

```
ifn address eth1  155.1.3.254  255.255.255.0
ifn address dsl1  155.1.4.254  255.255.255.0
ip route create upstream  eth1  155.1.4.253
```

Basic NAT Configuration Example



NAT Mapping Public IP Addresses	Private IP Addresses
192.128.1.1	10.1.3.2
192.128.1.2	10.1.3.3
192.128.1.3	10.1.3.4
192.128.1.4	10.1.3.5

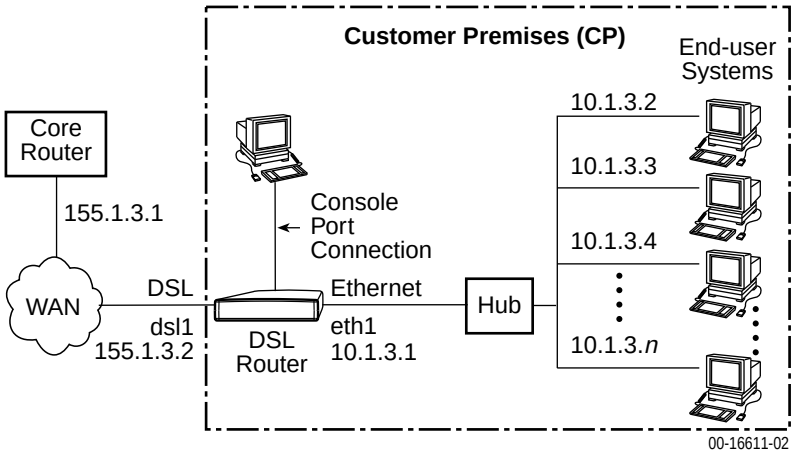
In this Basic NAT example:

- NAT is used for one-to-one mapping of addresses.
- There are four private IP addresses configured on the Ethernet side of the DSL router with NAT static mappings to four public IP addresses.
- The Ethernet interface (eth1) is in the private address space and the DSL interface is in public address space.
- The next hop router (default gateway) for the clients is the Ethernet IP address of the DSL router, 10.1.3.1.

  The command line syntax for this example is:

```
ifn address eth1:1  10.1.3.1  255.255.255.248
ifn address dsl1  155.1.3.2  255.255.255.0
ip route create upstream eth1 155.1.3.1
nat basic address  192.128.1.0
nat basic map  192.128.1.1  10.1.3.2  10.1.3.5
nat basic enable
```

NAPT Configuration Example



NAPT Mapping Public IP Addresses	Private IP Addresses
155.1.3.2 Port 23	10.1.3.4
155.1.3.2 Port 23	10.1.3.2
155.1.3.2 Port 23	10.1.3.3
155.1.3.2 Port *n*	10.1.3.*n*

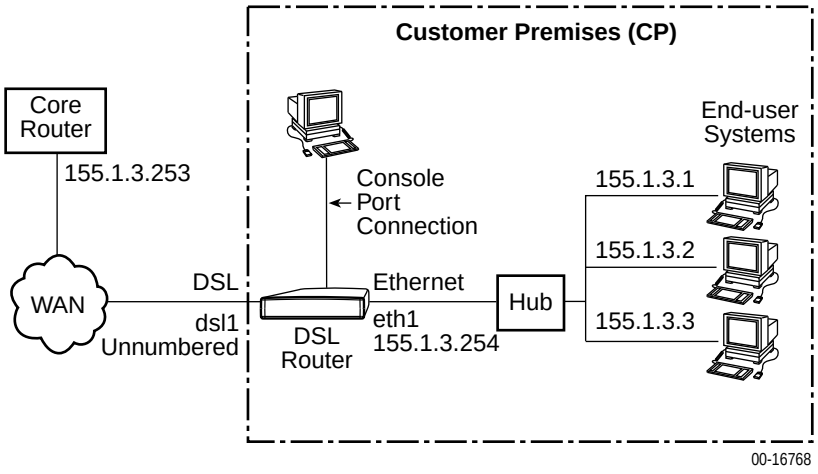
In this NAPT example:

- The DSL router is configured for NAPT using a single public IP address.
- When using NAPT, the DSL interface (dsl1) must be numbered because the Ethernet interface will be configured within the private address space.
- NAPT static mapping is configured for a server (Telnet port 23) on the Ethernet interface but publicly available.

  The command line syntax for this example is:

```
ifn address eth1  10.1.3.1  255.255.255.0
ifn address dsl1  155.1.3.2  255.255.255.0
ip route create upstream eth1 155.1.3.1
nat napt address  155.1.3.2
nat napt map tcp  10.1.3.4  23
nat napt enable
```

Unnumbered DSL Interface with Proxy ARP Configuration Example



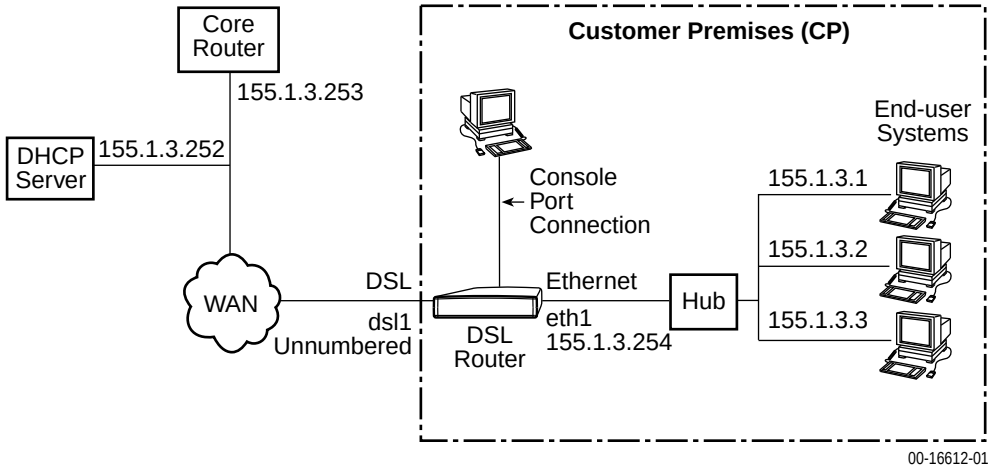
In this Unnumbered DSL Interface with Proxy ARP example:

- The clients are statically configured and use the core router as the next hop router (default gateway) in order to create the LAN extension configuration.
- The DSL interface is unnumbered.
- The DSL line is configured (at the DSLAM/GranDSLAM chassis) for VNET mode.
- Proxy ARP and NAPT cannot be enabled at the same time.
- If Basic NAT was enabled, the DSL interface (dsl1) must have Proxy ARP enabled if the dsl1 interface address is part of the Basic NAT global IP network address.
- The clients, the DSL router's Ethernet interface, and the core router interface are all on the same logical network.

  The command line syntax for this example is:

```
ifn address eth1  155.1.3.254  255.255.255.0
ifn address dsl1 unnumbered
ip route create upstream eth1 155.1.3.253
proxy arp eth1 enable
proxy arp dsl1 enable
```

DHCP Relay with Proxy ARP Configuration Example



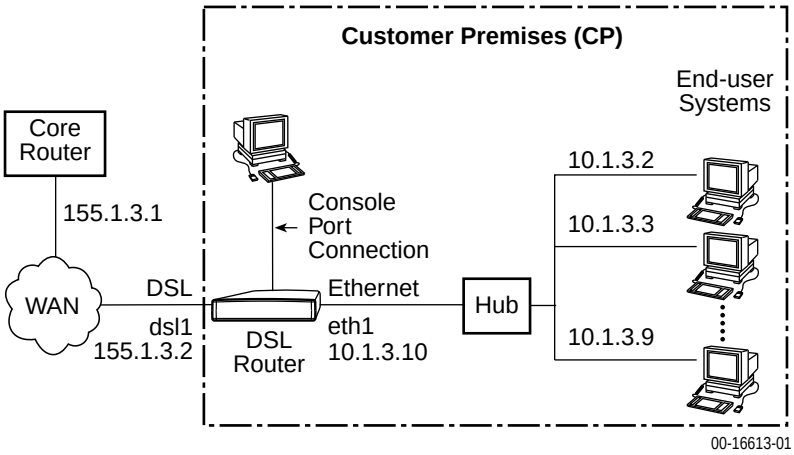
In this DHCP Relay with Proxy ARP example:

- The clients are using dynamic IP address assignment and use the core router as the next hop router (default gateway) in order to create the LAN extension configuration.
- The DSL line is configured (at the DSLAM/GranDSLAM chassis) for VNET mode.
- The DSL interface (dsl1) is unnumbered.
- The clients, the Ethernet interface (eth1), and the core router interface are all on the same logical network.
- IP Scoping must be disabled at the DSL card.
- The DSL router is configured as a DHCP relay.

  The command line syntax for this example is:

```
ifn address eth1  155.1.3.254  255.255.255.0
ifn address dsl1 unnumbered
ip route create upstream eth1 155.1.3.253
proxy arp eth1 enable
proxy arp dsl1 enable
dhcp relay enable
dhcp relay address 155.1.3.252
```

DHCP Server with Basic NAT Configuration Example



Public IP Addresses for Basic NAT	Private IP Addresses
192.128.1.1	10.1.3.2
192.128.1.2	10.1.3.3
...	...
192.128.1.8	10.1.3.9

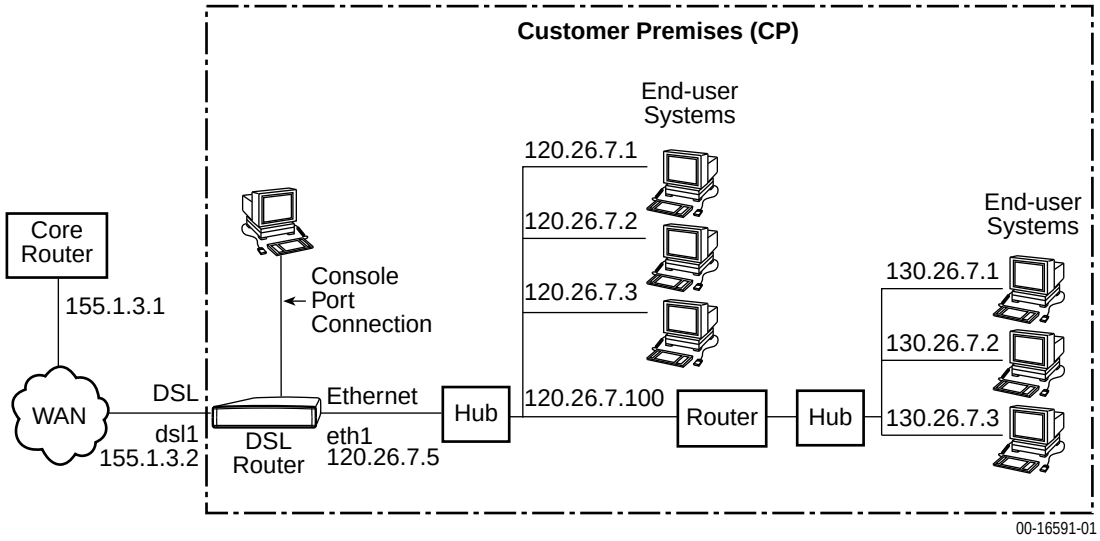
In this DHCP Server with Basic NAT example:

- The clients are using dynamic IP address assignment and use the Ethernet interface (eth1) of the DSL router as the next hop router (default gateway).
- The DSL interface (dsl1) must be numbered.
- The DSL router is configured as the DHCP server giving the private IP addresses to the clients.
- The Ethernet interface is in private address space. NAT is used for one-to-one mapping of addresses.

  The command line syntax for this example is:

```
ifn address eth1  10.1.3.10  255.255.255.240
ifn address dsl1  155.1.3.2  255.255.255.0
ip route create upstream eth1 155.1.3.1
nat basic address  192.128.1.0
nat basic enable
dhcp server addresses  10.1.3.2  10.1.3.9
dhcp server router  10.1.3.10
dhcp server enable
```

Downstream Router Configuration Example



In this downstream router example:

- There are clients statically configured and connected to the DSL router.
- There are also clients connected behind a downstream router.
- The DSL interface (dsl1) is numbered.

The command line syntax for this example is:

```
ifn address eth1  120.26.7.5  255.255.255.0
ifn address dsl1  155.1.3.2  255.255.255.0
ip route create upstream eth1  155.1.3.1
ip route create 130.26.7.0  255.255.255.0 120.26.7.100
```

Monitoring the DSL Router

5

What to Monitor

This chapter presents information on how to access and monitor the Hotwire DSL Router's status and performance statistics. You can monitor DSL router operations by viewing:

- LEDs on the DSL router's front panel.
- DSL Router Interfaces Status, including DSL and Ethernet LED status.
- DSL Router Statistics, including DSL Service Domain, DSL Management Domain, Ethernet, and IP statistics.
- DSL Router SNMP traps.

Detecting Problems

The DSL router can detect and report problem conditions and the user can perform diagnostic tests. The DSL router offers a number of indicators to alert you to possible problems:

- LEDs provide status. Refer to *Status LEDs* in the Hotwire DSL Router Installation Instructions for LED indications and troubleshooting of the hardware installation.
- Status messages for both the Ethernet and DSL links. Refer to *Status of Interfaces* on page 5-2.
- Network performance statistics for both the Ethernet and DSL links. Refer to *Interface Statistics* on page 5-3.
- Current status of DSL Router SNMP traps, if enabled. Refer to Appendix C, *Traps & MIBs*.

For additional information regarding diagnostic tests, System Log messages, and troubleshooting, refer to Chapter 6, *Diagnostics and Troubleshooting*.

Status of Interfaces

From the Command Line Interface, the current status of the Ethernet (eth1) Interface and the DSL (dsl1) Interface can be obtained with one command:

```
show interface
```

The information displayed for Ethernet and DSL Interfaces is presented below.

`show interface {eth1 | dsl1}`

Use to request status statistics for the named interface, eth1 or dsl1.

Minimum access level: Operator

eth1 – Ethernet interface

dsl1 – DSL interface

eth1 status – Fields included in the display of Ethernet status: eth1

- **Ethernet Link:** { up | down }
  This is the same status as reflected by the Ethernet LED.
- **MAC address:** *xx:xx:xx:xx:xx:xx*
- **proxy ARP eth1** { enabled | disabled }
- **ifn eth1:1** – ip-addr *x.x.x.x* mask *x.x.x.x* *
- **ifn eth1:2** – ip-addr *x.x.x.x* mask *x.x.x.x*
- **ifn eth1:3** – ip-addr *x.x.x.x* mask *x.x.x.x*
- **ifn eth1:4** – ip-addr *x.x.x.x* mask *x.x.x.x*

dsl1 status – Fields included in the display of DSL status: dsl1

- **DSL Link:** { up | down }
  This is the same status as reflected by the DSL LED.
- **MAC address:** *xx:xx:xx:xx:xx:xx*
- **proxy ARP dsl1** { enabled | disabled }
- **ifn dsl1:1** – ip-addr *x.x.x.x* mask *x.x.x.x* *
- **ifn dsl1:2** – ip-addr *x.x.x.x* mask *x.x.x.x*
- **ifn dsl1:3** – ip-addr *x.x.x.x* mask *x.x.x.x*
- **ifn dsl1:4** – ip-addr *x.x.x.x* mask *x.x.x.x*

* The Primary designation of a numbered interface marks that interface as the one whose IP address is used as a Router ID. If no interface is defined as Primary, the last numbered interface created becomes the Primary IP Address.

Interface Statistics

From the Command Line Interface, statistics are available for DSL, Ethernet, and IP processing. Statistics are available for all three selections, **`eth1`**, **`dsl1`**, and **`ip`**, with one command:

```
show statistics
```

The format of the statistics information display is presented below.

`show statistics [ eth1 | dsl1 | ip ]`
Use to request statistics for the named interface, eth1 or dsl1, or IP processing statistics. Minimum access level: Operator **eth1** – Ethernet interface statistics **dsl1** – DSL interface statistics **ip** – IP processing statistics
Information displayed for **`show statistics eth1`**: – Total Bytes Received . . . . . *nnnn* – Total Bytes Transmitted . . . . . *nnnn* – Total Frames Received . . . . . *nnnn* – Total Frames Transmitted . . . . . *nnnn* – Total Frames Discarded: Each Discard Reason will display with # of frames discarded for each specific Discard Reason. Refer to Table 5-1, Discard Reasons for the Ethernet Interface (eth1).
Information displayed for **`show statistics dsl1`**: ■ Service Domain Statistics (end-user traffic): – Total Bytes Received . . . . . *nnnn* – Total Bytes Transmitted . . . . . *nnnn* – Total Frames Received . . . . . *nnnn* – Total Frames Transmitted . . . . . *nnnn* ■ Management Domain Statistics (management traffic): – Total Bytes Received . . . . . *nnnn* – Total Bytes Transmitted . . . . . *nnnn* – Total Frames Received . . . . . *nnnn* – Total Frames Transmitted . . . . . *nnnn* ■ Total Frames Discarded: This total is for both the Service Domain and the Management Domain. Each Discard Reason will display with # of frames discarded for each specific Discard Reason. Refer to Table 5-2, Discard Reasons for the DSL Interface (dsl1).
Information displayed for **`show statistics ip`**: – Total Packets Received . . . . . *nnnn* – Total Packets Transmitted . . . . . *nnnn* – Total Packets Discarded: Each Discard Reason will display with # of packets discarded for each specific Discard Reason. Refer to Table 5-3, Discard Reasons for IP.

Clearing Statistics

From the Command Line Interface, the statistics can be cleared.

clear statistics [eth1 | dsl1 | ip]
Clears the statistics for the named interface. If no interface is entered, ALL statistics for all interfaces are cleared. Minimum access level: Administrator **eth1** – Ethernet interface statistics **dsl1** – DSL interface statistics **ip** – IP processing statistics Example: **clear statistics eth1**

List of Discard Reasons

The Discard Statistics represents the number of frames or packets discarded. The display includes the reason for the discard. The following tables list discard reasons for:

- Ethernet Interface (Table 5-1)
- DSL Interface (Table 5-2)
- IP (Table 5-3)

Table 5-1. Discard Reasons for the Ethernet Interface (eth1) (1 of 2)

Discard Reasons for the Ethernet Interface (eth1)
Alignment Error
CRC Error
Excessive Collisions
Excessive Defers on TX
FIFO Overflow Error
Frame Length Greater than Max
Late Collision on TX
No Carrier Detect on TX
Parity Error
Receive Buffer Pool Depletion
Receiver Halted

Table 5-1. Discard Reasons for the Ethernet Interface (eth1) (2 of 2)

Discard Reasons for the Ethernet Interface (eth1)
Receiver Missed Frame
Signal Quality Error on TX
Srv Domain Phy TX Queue Overflows
Srv Domain Receive Queue Overflows
Srv Domain Wrpr TX Queue Overflows
TX Halted
TX Parity Error
TX Underflow
Unsupported Encapsulation Protocol
Unsupported SNAP Network Protocol
Unsupported TypeII Network Protocol

Table 5-2. Discard Reasons for the DSL Interface (dsl1) (1 of 2)

Discard Reasons for the DSL Interface (dsl1)
Alignment Error
Mgmt Domain Phy TX Queue Overflows
Mgmt Domain Rcv Queue Overflows
Mgmt Domain TX Link Queue Overflows
Mgmt Domain Wrpr TX Queue Overflows
Receive Aborts
Receive Buffer Pool Depletion
Receive CRC Errors
Receive Frame Too Short or Too Long
Receive Interrupt Errors
Receive Overruns
Receive Unknown Errors
Service Domain Rcv Queue Overflows
Srv Domain Phy TX Queue Overflows
Srv Domain TX Link Down Discards

Table 5-2. Discard Reasons for the DSL Interface (dsl1) (2 of 2)

Discard Reasons for the DSL Interface (dsl1)
Srv Domain Wrpr TX Queue Overflows
Unknown Frame Type Errors
Unrecognized VNID
Unsupported Encapsulation Protocol
Unsupported Network Protocol

Table 5-3. Discard Reasons for IP

Discard Reasons for IP
Bad Port to Destination
Bad Port to Source
DSL Receive Packets Filtered
DSL Transmit Packets Filtered
Ethernet Receive Packets Filtered
Ethernet Transmit Packets Filtered
Fragmentation Failures
ICMP Errors
IP Processing Disabled
No Route to Destination
No Route to Source
No Upstream Route
Other Reassembly Failures
Other Receive Errors
Other Transmit Errors
Packets Pending on ARP Discarded
Reassembly Timeout
TCP Errors
Time to Live Expired
Transport Protocol Not Handled
UDP Errors

Diagnostics and Troubleshooting

6

Diagnostics and Troubleshooting Overview

There are several features available to assist in evaluating the Hotwire DSL Router. The following sections are covered in this chapter:

- Device Restart
- Alarms Inquiry
- System Log
- Ping
- TraceRoute

Device Restart

The DSL router can be restarted locally or remotely. From the Command Line Interface, type **`Restart`** and press Enter.

The DSL router reinitializes itself, performing a power-on self-test and resetting the local System Log (SYSLOG).

Alarms Inquiry

`show alarms`
This command allows the operator to display the list of current alarm conditions, if any. Minimum access level: Operator The possible output lines are: **`Alarm: Management Address Conflict`** **`Alarm: Failed Selftest`** **`Alarm: System Error`** **`No alarm condition is set`** Alarm condition reverts to Normal when the offending problem has been corrected.

System Log

The Hotwire DSL Router can log significant system events (SYSLOG). The SYSLOG can be maintained locally on the DSL router and can also be sent to a remote SYSLOG server, preferably in the management domain. To activate:

- The DSL router must be configured to enable the output of SYSLOG messages via the **`syslog enable`** command. (The Management Controller Card (MCC) has SYSLOG always enabled.)
- An IP address (loopback or remote) must be supplied.
- The SYSLOG can also be captured by a remote SYSLOG server running the UNIX daemon *syslogd* or an equivalent program. It is necessary to know the IP address where the *syslogd* resides and the UDP port number the *syslogd* is using.

  The advantage of using a remote SYSLOG server is that ALL events will be maintained upon restart of the DSL router. The local SYSLOG is cleared upon restart.

Events are classified by severity level and the system administrator can specify the minimum severity to be logged.

`show syslog`
Displays the current status of system as enabled or disabled. If enabled, the severity level, management IP address, and UDP port will be displayed. **syslog** { enabled | disabled } **level** { emer | err | norm | info } **management ip-addr** *x.x.x.x* **port** *nnn*
`syslog {enable | disable}`
Allows the user to enable or disable SYSLOG output. The SYSLOG IP address must be entered (next command) and saved to complete enabling SYSLOG. Minimum access level: Administrator/Config **enable** – Enables SYSLOG output. **disable** – Disables SYSLOG output.
`syslog ip` *ip-addr*
Specifies the IP address for the host to send system log entries to. Minimum access level: Administrator/Config **ip-addr** – The IP address for SYSLOG (typically loopback address of 127.0.0.1).
`syslog port [`*port-number***`]`**
Specifies the UDP port number on the server to which the system events will be sent. Minimum access level: Administrator/Config **port-number** – The UDP port number. Default = 514.

syslog level *level*
Specifies the minimum severity level to be logged. Refer to Table 6-1, SYSLOG Messages, for a list of messages by severity level. Minimum access level: Administrator/Config **level** – The minimum level to be logged. The default is NORM. The choices for severity level (displayed as high severity to low severity) are as follows: EMER – emergency, the system is unusable ERR – error conditions reported NORM – normal or administrative reporting INFO – informational reporting Example: To log EMER and ERR severity levels, enter **syslog level ERR**
show log [*number***]**
Displays the contents of the local system error log. (The 100 most recent SYSLOG entries are kept locally.) The user specifies how many entries they wish to view. Entries are displayed in reverse order from most recent to oldest. **number** – The number of local entries to be seen. Default = 10. Range = 1–100. NOTE: The SYSLOG retained locally will be reset at the DSL router if the restart command is issued. External logs are retained after a DSL router restart.

SYSLOG Events

The following are some of the SYSLOG events that will be reported for defined severity levels.

Table 6-1. SYSLOG Messages (1 of 2)

Level	Description	Event
EMER	Emergency and the system is unusable	Alarm Cleared
		Alarm Set
		System Abort
ERR	Error conditions reported	ARP Table size exceeded
		Executable image in flash invalid
		Frame received in error

Table 6-1. SYSLOG Messages (2 of 2)

Level	Description	Event
NORM	Normal or administrative reporting	Admin enable
		Admin enable failure
		Any configuration change command
		Configuration changes saved
		Download completed
		Download failure
		Login
		Login failure
		Logout
		Statistics cleared
		Switch program LMC message received
		System started
INFO	Informational reporting	ARP table entry created due to packet arrival
		ARP table entry created for DHCP address assignment
		ARP table entry deleted due to time out
		Device information LMC message received
		Packet filter action
		Routing table entry created for DHCP address assignment
		VNID update LMC message received

SYSLOG Message Display

The SYSLOG message displays the following fields:

- Date
- Time
- Severity Level
- DSLAM Slot #/Port #
- System Identifier
- SYSLOG Event Description

This is an example of a SYSLOG message:

```
01/06/00  21:22:38  5  03/01  CUSTOMER  Console logout complete
```

Ping

The Ping program is an IP-based application used to test reachability to a specific IP address by sending an ICMP echo request and waiting for a reply. From the Command Line Interface, Ping can test connectivity upstream or downstream.

ping *dest-ip* **[mgt | -x** *source-ip***] [-l** *bytes***] [-w** *time***] [-i** {**eth1 | dsl1**}**]**
Pings the specified destination IP address. Once Ping starts, the input prompt will not redisplay until either the Ping finishes or the Ping command is aborted with Ctrl-c. Minimum access level: Administrator **dest-ip** – The destination IP address of the device to ping. **mgt** – Specifies that the IP address is in the management domain (through the MCC). Do not use with –x source-ip selection. **source-ip** – The source IP address to be used. The default source address is from the service domain in which the test is being done. The IP address is validated to verify that it is an interface IP address. **bytes** – Bytes of data (l = length). Default = 64 bytes. Range = 0–15,000. **time** – Number of seconds to wait before ending ping attempt. Default = 10 seconds. Range = 0–60. **interface** – The target interface for the command (eth1|dsl1). Do not use with –x source-ip selection. Example: **`ping 135.300.41.8 –l 144 –w 30 -i eth1`**

Ping Test Results

Ping test results display in the following formats.

- Ping successful:

  `Ping reply [`*x.x.x.x***`]: bytes of data=`***nn***

- Ping timeout:

  `Ping reply [`*x.x.x.x***`]: REQUEST TIMED OUT`**

- ICMP echo response of an unreachable destination:

  `Ping reply [`*x.x.x.x***`]: DESTINATION UNREACHABLE`**

TraceRoute

The TraceRoute program is an IP diagnostic tool that allows you to learn the path a packet takes from the service domain local host to its remote host.

If you are unable to ping a device in a Hotwire network configuration, you may want to run TraceRoute to identify the link (destinations up to 64 hops) between the DSL router and the device that is not forwarding the Ping message.

`traceroute` *dest-ip* **`[-x`** *source-ip***`]`** **`[-l`** *bytes***`]`** **`[-w`** *time***`]`** **`[-h`** *hops***`]`** **`[-i`** {**`eth1 | dsl1`**}**`]`**
Performs TraceRoute to the specified destination IP address. Once TraceRoute starts, the input prompt will not redisplay until either TraceRoute finishes or the TraceRoute command is aborted with Ctrl-c. Minimum access level: Administrator **dest-ip** – The destination IP address for TraceRoute. **source-ip** – The source IP address used. The default source address is from the service domain in which the test is being done. The IP address is validated to verify that it is an interface IP address. **bytes** – Bytes of data (l = length). Default = 64 bytes. Range = 0–15,000. **time** – Time (in seconds) before the TraceRoute is abandoned. Default = 10 seconds. Range = 0–60. **hops** – Decimal number that specifies the maximum number of hops to be tested. Default = 8. Range = 0–128. **interface** – The target interface for the command (eth1 | dsl1). Do not use with the –x source-ip selection. Example: **`traceroute 135.300.41.8 –w 80 -i eth1`**

TraceRoute Test Results

TraceRoute results display in the following format:

`Tracing route to [`*x.x.x.x***`] over a max of`** *nn* **`hops with`** *nnn* **`byte packet`**

Hop #	Round Trip Time			IP Address of Responding System
	Try #1	Try #2	Try #3	
1	<100ms	<100ms	<100ms	*x.x.x.x*
2	<100ms	<100ms	<100ms	*x.x.x.x*
3	<200ms	<200ms	<200ms	*x.x.x.x*
4	<200ms	<200ms	<200ms	*x.x.x.x*

The Hop # is the Time to Live (TTL) value set in the IP packet header. The Round Trip Time contains the time in 100ms intervals for each attempt to reach the destination with the TTL value.

Command Line Interface

A

Command Line Interface Feature

The Hotwire DSL router is managed with text commands from the Command Line Interface. The Command Line Interface can be accessed:

- Locally with an ASCII terminal connected to the Console port, or
- Remotely via a Telnet session.

The Command Line Interface is ASCII character-based and provides the capability to:

- Display the syntax of commands.
- Change the operational characteristics of the DSL router by setting configuration values.
- Restore all configuration values to the initial factory defaults.
- Display DSL router hardware and identification information.
- Display system status, including DSL link status and Ethernet status.
- Display a sequence of commands that would have the effect of setting all configurable parameters to their current value.

Refer to Appendix B, *Configuration Defaults & Command Line Shortcuts*.

Navigation

The Hotwire DSL router uses the following keys (as do most terminal emulation programs):

- **Enter** or **Return** – Accepts the input.
- **Ctrl-c** – Aborts the entry or clears the input line.
- **Down Arrow** – Repeats an entry within the last five entered.
- **Up Arrow** – Displays the last entry.
- **Left Arrow** – Moves the insertion point one space to the left.
- **Right Arrow** – Moves the insertion point one space to the right.

Command Recall

The Hotwire DSL router keeps a history of the last several commands entered on the command line interface. For example, if you press the Up Arrow key, the most recently entered command will appear on the command line, where it can be edited and reentered by pressing Enter. If you press the Up Arrow key again, the next most recent command will appear, etc.

After pressing the Up Arrow key one or more times, pressing the Down Arrow key moves down the list of recent commands, wrapping past the end of the list in either direction.

Commands appearing in the command line can be edited. Use the Left and Right Arrow keys to move the insertion point, enter the new characters or use the Delete key to delete the character just to the left of the insertion point.

Document Conventions

This syntax is used throughout this manual. The Command Line Interface is not case-sensitive, with the exception of the Login ID and Password fields.

Syntax	Translation
[ ]	Square brackets represent an optional element.
{ }	Braces represent a required entry.
|	Vertical bar separates mutually exclusive elements.
Italics	Entry is a variable to be supplied by the operator.
Bold	Enter (type) as shown.
x.x.x.x	32-bit IP address and mask information where *x* is an 8-bit weighted decimal notation.
xx:xx:xx:xx:xx:xx	MAC address information where *x* is a hexadecimal notation.

Command Line Interface Commands

Configuration Control Commands

configure {terminal | factory}
Enables the Administrator configuration mode. Configuration mode will remain in effect until the **exit** or **logout** command has been entered. While in configuration mode, the **show** commands are unavailable. Minimum access level: Administrator **configure terminal** – Configuration mode is in effect and all changes entered by the Administrator are made on top of the current running configuration. When finished entering the commands needed to configure the DSL router, the **save** command must be input to save the configuration changes or the **exit** command can be used to discard the configuration changes and leave the configuration mode. **configure factory** – Causes the configuration mode to be entered and the factory default settings to be loaded. The **save** command must be used to save the configuration factory defaults as the active configuration. CAUTION: All previously set interface IP address assignments, IP route table entries, ARP cache entries, NAT static entries, and DHCP server entries will be purged when the **save** command is executed.
save
Saves configuration changes to the active configuration in NVRAM. No configuration changes are effect until the **save** command is issued. If the **save** command is entered and there are changes that require a reboot of the DSL router, a prompt states that a reset is necessary for changes to take effect and prompts for verification. Minimum access level: Administrator/Config **yes** – Changes are stored and the DSL router resets automatically if interface addresses have been changed. **no** – DSL router is left in configuration mode.

RFC 1483 Encapsulation

1483encap [LLC | VC]
Specifies the method for carrying the routed PDUs. Minimum access level: Administrator/Config **LLC** – LLC encapsulation. Default = LLC. **VC** – VC-based multiplexing.

Ethernet Frame Format

frame [802.3 | DIX]
Specifies the Ethernet frame format that is to be used. Minimum access level: Administrator/Config **format** – 802.3 or DIX. Default = DIX.

Interface and Service Domain IP Address

`ifn address {eth1[:ifn] | dsl1[:ifn]}` *ip-address mask* **`[primary]`**

`ifn {dsl1[:ifn] | eth1[:ifn]} primary`

`ifn address dsl1 unnumbered`

Specifies the IP address associated with either the Ethernet interface or the DSL interface. Up to four (4) IP addresses may be assigned on each interface. An interface address and mask cannot be changed while there is a static route (upstream or downstream) that uses it. Interface IP address ranges must not overlap.

Minimum access level: Administrator/Config

eth1, eth1:1, eth1:2, eth1:3, eth1:4 – Ethernet interface. eth1 is the same as eth1:1.

dsl1, dsl1:1, dsl1:2, dsl1:3, dsl1:4 – DSL interface. dsl1 is the same as dsl1:1.

ip-address – The IP address associated with the specified interface.

mask – Mask for the associated subnet.

primary – The Primary designation of a numbered interface marks that interface as the one whose IP address will be used as the Router ID. (The Router ID is important when the DSL interface is unnumbered.) If no interface is defined as Primary, the last numbered interface created will become the Primary IP Address.

unnumbered – Specifies that the DSL interface is to be unnumbered.

NOTES:
- For each defined Ethernet interface, a corresponding upstream next hop router IP address must be configured for routing of packets received on that interface. See **`ip route create upstream`** command on page A-6 for more details.
- When the eth1 is assigned an IP address, this section also defines the logical network (subnet) containing the locally attached hosts. An IP route table entry will automatically be created to correspond to the subnet defined by the mask.
- When the DSL interface is numbered, multiple logical Ethernet interfaces can be assigned to the same DSL logical interface by configuring the same upstream next hop router.
- The configured DSL logical interfaces must be either all numbered or a single unnumbered interface.
- When NAT is being used, the DSL interface must be numbered. Only one logical interface must be defined for each physical interface, i.e., one IP address to each interface.
- When NAT, DHCP Server, or DHCP Relay is enabled, there can be only one service domain configured.

Examples:
```
ifn address dsl1 135.300.41.8 255.255.255.0
ifn dsl1 primary
```

`delete {eth1[:ifn] | dsl1[:ifn]}`

Deletes any of the assignments that are configured for the interface. Only the specific Ethernet or DSL interface number needs to be specified.

An interface address and mask cannot be deleted while there is a static route (upstream or downstream) that uses it. First, delete the IP route with the **`ip route delete`** command (see IP Routing Table).

Minimum access level: Administrator/Config

eth1, eth1:1, eth1:2, eth1:3, eth1:4 – Ethernet interface. eth1 is the same as eth1:1.

dsl1, dsl1:1, dsl1:2, dsl1:3, dsl1:4 – DSL interface. dsl1 is the same as dsl1:1. Only dsl1 or dsl1:1 are acceptable inputs for an unnumbered interface.

Example: **`delete eth1:4`**

IP Routing Table

`ip route create` *dest-ip dest-mask* **`{next-hop-ip | remote}`**

`ip route delete` *dest-ip dest-mask*

Configures the downstream static routes. Downstream routes cannot be created unless at least one Ethernet interface has been configured. To configure upstream routers, refer to the next set of entries.

create – Create a downstream IP route table entry. To configure a downstream default gateway, enter a destination IP address and a subnet mask of **0.0.0.0**.

delete – Delete a downstream IP route table entry. This will delete an IP route placed in the table by the DHCP server, the DHCP relay, or manually entered static entries.

NOTE: An interface route is created automatically when an address and mask are assigned to an Ethernet interface with the **`ifn address`** command. The Ethernet interface route can be deleted with the **`ip route purge`** or the **`ip route delete`** command. Once deleted, the interface route can be entered manually using **`ip route create`** or a new **`ifn address`** command.

dest-ip – IP address of the destination. The destination IP address must be within the address range of a configured Ethernet interface or the next-hop-ip address must be provided.

dest-mask – IP mask for the destination IP address.

next-hop-ip – IP address of the next hop downstream router used to reach the destination. A next hop with an IP address of 0.0.0.0 specifies a directly reachable client. A nonzero next-hop-ip address must be within the address range of an Ethernet interface.

remote – Indicates that the device specified by the destination IP and destination mask is logically within a local subnet route but is not on the physical Ethernet and resides upstream from the DSL router. A remote route cannot be created unless at least one DSL interface has previously been configured.

Example: Refer to Chapter 4, *DSL Router Configuration Examples*.

`ip route create upstream eth1[:`*`ifn`*`]` *next-hop-ip*

`ip route delete upstream eth1[:`*`ifn`*`]`

Enter or delete upstream IP routing table entries. When the DSL interface is unnumbered, an IP routing table entry will be created automatically with the next hop router as remote. To configure downstream routers, refer to the previous set of entries.

Minimum access level: Administrator/Config

create – Create an upstream IP route table entry.

delete – Delete an upstream IP route table entry.

eth1, eth1:1, eth1:2, eth1:3, eth1:4 – Ethernet interface. eth1 is the same as eth1:1. Specified logical Ethernet interface.

next-hop-ip – IP address of the next hop upstream router used to reach the remote destination or the downstream default gateway.

NOTE: When the DSL interface is numbered, the next hop router IP address must fall into one of the service domain IP subnets configured for the DSL interface.

Example: Refer to Chapter 4, *DSL Router Configuration Examples*.

`ip route purge`

Deletes all IP route table entries, including interface routes and those automatically added by DHCP Server and DHCP Relay agent.

NOTE: An interface route is created automatically when an IP address and mask are assigned to an Ethernet interface with the **`ifn address`** command. The Ethernet interface route can be deleted with the **`ip route purge`** or the **`ip route delete`** command. Once deleted, the interface route can be entered manually using **`ip route create`** or a new **`ifn address`** command.

Minimum access level: Administrator/Config

ARP Table

arp timeout incomplete [*time***]**
Specifies the ARP table timeout value in seconds for incomplete ARP table entries. Default = 5 seconds. Minimum access level: Administrator/Config
arp timeout complete [*time***]**
Specifies the ARP table timeout value in minutes for complete ARP table entries. Default = 20 minutes. Minimum access level: Administrator/Config
arp {create | delete} *ip-address mac-address*
Creates or deletes a single, static ARP table entry. Static ARP entries created with this command are retained across resets/power cycles. Minimum access level: Administrator/Config **create** – Create an ARP table entry. **delete** – Delete an ARP table entry. **ip-address** – The IP address of the ARP entry to be created or deleted. **mac-address** – MAC address (valid for create command). Examples: **arp create 132.53.4.2 00:10:4b:97:6c:44** **arp delete 132.53.4.2**
arp purge
Deletes ALL static and dynamic ARP table entries. Minimum access level: Administrator/Config

Proxy ARP

proxy arp {eth1 | dsl1} [enable | disable]
Enables or disables proxy ARP for the specified interface. Minimum access level: Administrator/Config **eth1** – The Ethernet interface. **dsl1** – The DSL interface. **enable** – Enable Proxy ARP. Default = Enable. **disable** – Disable Proxy ARP. NOTE: Proxy ARP and NAPT cannot be enabled at the same time. When Basic NAT is enabled, Proxy ARP is allowed on the dsl1 interface. Example: **proxy arp dsl1 disable**

NAT

nat basic enable
Enables the one-to-one mapping function of Basic NAT. Enabling Basic NAT automatically disables NAT NAPT. If Basic NAT is enabled, Proxy ARP must be enabled on the dsl1 interface when the dsl1 interface address is part of the Basic NAT global IP network address. Minimum access level: Administrator/Config
nat napt enable
Enables the many-to-one mapping function of NAPT. Enabling NAT NAPT automatically disables Basic NAT. Minimum access level: Administrator/ Config NOTE: Proxy ARP and NAPT cannot be enabled at the same time.
nat basic address *ip-addr* **[***ip-mask***]**
Defines the public IP addresses used in the one-to-one mapping function of Basic NAT Up to 256 addresses can be allocated with Basic NAT. Minimum access level: Administrator/Config **ip-addr ip-mask** – Any valid public IP address/IP mask. Default = 255.255.255.0. Example: **nat basic address 192.128.1.1**
nat napt address *ip-addr*
Defines the public IP addresses used in the public IP address of a single host for use in the many to one mapping function of NAPT. NAPT cannot accept incoming requests, unless a static NAT entry has been configured. Minimum access level: Administrator/Config **ip-addr** – Any valid public IP address. Example: **nat napt address 192.128.1.1**
nat timeout *time*
Specifies the NAT timeout value for mappings set up dynamically. Minimum access level: Administrator/Config **time** – The timeout value in minutes. Default = 20 minutes. Example: **nat timeout 90**
nat napt map {udp | tcp} *server-ip port*
Permits global access to a local server, such as a Web server. Port-based static entries can be configured for NAPT. This allows a global host to access a server behind the DSL router without exposing the local server's IP address. Minimum access level: Administrator/Config **udp, tcp** – Specify the protocol to which the mapping applies. **server-ip** – Enter the IP address of a local server. Only one server of a particular type (FTP, Telnet, SMPT, TFTP, gopher, finger, http, etc.) can be supported at one time. **port** – The destination port number for the specified server. Example: **nat napt map tcp 192.128.1.1 102**

`nat basic map` *public-ip private-ip*
`nat basic map` *lower-public-ip lower-private-ip upper-private-ip*

Statically maps public to private IP addresses for the one-to-one mapping function of Basic NAT. In the first command, a single address pair is mapped. In the second command, a range of IP addresses will be contiguously mapped starting at the pair defined by the *lower-public-ip* and *lower-private-ip* argument.

Minimum access level: Administrator/Config

public-ip – IP address of the public address space which is to be mapped to the IP address of a local host.

private-ip – IP address of a local host which is to be mapped to an IP address in the public IP address space.

lower-public-ip – Lowermost IP address of a range of public addresses which are to be mapped to a range of IP addresses of local hosts.

lower-private-ip – Lowermost IP address of a range of local host IP addresses which are to be mapped to a range of IP addresses in the public IP address space.

upper-private-ip – Uppermost IP address of a range of local IP addresses which are to be mapped to a range of IP addresses of local hosts.

Example: **`nat basic map 192.128.1.1 10.1.3.2`**

`nat basic delete` *private-ip*
`nat basic delete` *lower-private-ip upper-private-ip*

In the first command, the command deletes static mapping entry associated with the specified one-to-one mapping of Basic NAT. In the second command, a range of mappings will be contiguously deleted starting at the pair defined by the *lower-private-ip* and ending with the *upper-private-ip* argument.

Minimum access level: Administrator/Config

private-ip – Statically mapped IP address of the local host.

lower-private-ip – Lowermost IP address of a range of local host IP addresses which are to be deleted.

upper-private-ip – Uppermost IP address of a range of local IP addresses which are to be deleted.

Example: **`nat basic delete 192.128.1.1`**

`nat napt delete {udp | tcp}` *port*

Deletes static mapping entries which identify a local server.

Minimum access level: Administrator/Config

udp, tcp – Specify the protocol used.

port – The port number associated with the *server-ip*.

Example: **`nat napt delete tcp 102`**

nat disable
Disables the currently enabled NAT, either Basic NAT or NAPT. Minimum access level: Administrator/Config
nat purge
Purges all mapping entries. Minimum access level: Administrator/Config

DHCP Server

The DHCP Server can be enabled and disabled. Based on RFC 2131 and RFC 2132, supported options are:

- Domain Name
- Domain Name Server
- Router
- Subnet Mask

dhcp server {enable | disable}
Enables or disables the DHCP server. For the DHCP Server to be enabled, one (and only one) address must be assigned to the Ethernet interface. The DHCP Server and the DHCP Relay Agent cannot be enabled at the same time. Minimum access level: Administrator/Config **enable** – Enable the DHCP Server. **disable** – Disable the DHCP Server. Default = disable. Example: **dhcp server enable**
dhcp server addresses *lower-ip-address upper-ip-address* **[***mask***]**
Specifies the range of IP addresses to be used by the DHCP server. When the DHCP address range is changed, all binding entries, automatically added routes, and ARP entries are removed. Minimum access level: Administrator/Config Example: **dhcp server address 132.53.4.2 132.53.4.250**

dhcp server leasetime *min-lease-time max-lease-time*
Specifies the lease-time settings used by the DHCP server. Minimum access level: Administrator/Config **min-lease-time** – Default = 120 minutes (2 hours) **max-lease-time** – Default = 4320 minutes (72 hours) Example: **dhcp server leasetime 120 320**
dhcp server router *ip-address*
Specifies the router IP address used by the DHCP server. Minimum access level: Administrator/Config Example: **dhcp server router 132.53.4.2**
dhcp server name *domain name*
Specifies the domain name used by the DHCP server. Minimum access level: Administrator/Config Example: **dhcp server name Clearwater7**
dhcp server nameserver *ip-address*
Specifies the DNS IP address used by the DHCP server. Minimum access level: Administrator/Config Example: **dhcp server nameserver 132.53.4.2**

DHCP Relay Agent

dhcp relay {enable | disable}
Enables or disables the DHCP relay agent. The DHCP relay agent will maintain up to 256 DHCP clients. Minimum level access: Administrator/Config **enable** – Enable the DHCP relay. **disable** – Disable the DHCP relay. Default = disable. Example: **dhcp relay enable**
dhcp relay address *ip-address*
Use this command to specify the DHCP server to forward DHCP requests to. Minimum level access: Administrator/Config Example: **dhcp relay address 132.23.4.2**
dhcp relay max *number*
Use this command to specify the maximum number of DHCP clients. Minimum level access: Administrator/Config **number** – 1 — 256 Example: **dhcp relay max 133**

IP Packet Processing

IP multicast {enable | disable}
Enables or disables the forwarding of IP multicast packets. This setting is retained across power cycles. Minimum access level: Administrator **enable** – Enable forwarding of IP multicast packets. **disable** – Disable forwarding of IP multicast packets. Default = disable.
IP processing {enable | disable}
Enables or disables the processing of IP packets in the service domain. This setting is retained across power cycles. Minimum access level: Administrator **enable** – Enable processing of IP packets. Default = enable. **disable** – Disable processing of IP packets.

Traps

trap {disable | enable} *name of trap*
Use this command to enable or disable traps. Default = disable. Minimum access level: Administrator/Config Name of Traps: **all** **authen fail** **ccn** **devfail** **link up** **link down** **selftest** **test start** **test stop** **warmstart** For additional information, refer to Appendix C, *Traps & MIBs*.

Show Command Outputs

show console
Displays: **console enabled** or **console disabled**
show system
Sample **show system** display: May 21 09:53:26 2000 System ID: *xxxxxxxx* Model #: *xxxx*, Serial #: *xxxxxxxxxxxx*, HW-Rev: *xxx* Boot: FW-Version *xxxxxxxx* 2nd Stage Boot: FW-Version *xxxxxxxx* Image 0: FW-Version *xxxxxxxx*, [active] Image 1: FW-Version *xxxxxxxx* DSP: FW-Version *xxx* Selftest Result: [0xxxxx] (if failed) { pass | fail }
show config
Sample **show config** display: **syslog** { enabled | disabled } **eth1 frame** { DIX | 802.3 } **proxy ARP eth1** { enabled | disabled } **proxy ARP dsl1** { enabled | disabled } **NAT disabled** *or* **NAT enabled** { basic NAT | NAPT } **DHCP server** { enabled | disabled } **DHCP relay** { enabled | disabled } **IP multicast** { enabled | disabled } **IP processing** { enabled | disabled } **1483 encapsulation** { LLC | VC Muxing } **autologout** { enabled | disabled }

`show ip route [`*ip-address***`]`**

If an IP address is not provided, the entire table will be displayed with the upstream routes displayed first and the downstream routes next. If the IP address is provided, only the specific entry will be displayed. If the next hop IP address = 0.0.0.0, the host is directly reachable on the Ethernet interface (eth1).

Minimum access level: Operator

Sample **show ip route** display:

source ip-addr	source subnet-mask	nexthop ip-addr	interface
x.x.x.x	*x.x.x.x*	*x.x.x.x*	dsl1

dest ip-addr	dest subnet-mask	nexthop ip-addr	interface
x.x.x.x	*x.x.x.x*	*x.x.x.x*	eth1

`show arp`

Sample **show arp** display:

ip-addr	MAC addr	timeout (min)	status
x.x.x.x	*xx:xx:xx:xx:xx:xx*	*xxxx*	*xxxx*

NOTES: – The timeout value shown is the actual time left for the specific entry.
– The timeout value shown will be Static for configured static entries.
– Status is Complete or Incomplete.

`show arp timeout`

ARP – timeout for complete = 20 min.
timeout for incomplete = 5 sec.

`show nat basic`

Sample **show nat basic** display:

NAT basic – { disabled | enabled }

NAT basic – public network address: *xxx.xxx.xxx.xxx*

NAT basic – public network mask: *xxx.xxx.xxx.xxx*

NAT timeout: *xx* minutes

NAT basic mappings:

public ip	private-ip
x.x.x.x	*x.x.x.x*

show NAT napt

Sample **show NAT napt** display:

NAT NAPT – { disabled | enabled }

NAT NAPT – public IP-address: *x.x.x.x*

NAT timeout: *xx* minutes

NAT NAPT mappings:

private-ip	private-port	mapped-port	protocol
x.x.x.x	*xxxx*	*xxxx*	{ udp | tcp }

show traps

Sample **show traps** display:

warmstart { disabled | enabled }

authen fail { disabled | enabled }

selftest { disabled | enabled }

devfail { disabled | enabled }

test start { disabled | enabled }

test stop { disabled | enabled }

ccn { disabled | enabled }

link up { disabled | enabled }

link down { disabled | enabled }

For additional information, refer to Appendix C, *Traps & MIBs*.

show dhcp server

Displays the DHCP relay's current status and configuration.

Minimum access level: Administrator

Sample **show dhcp server** display:

DHCP server { disabled | enabled }

DHCP server – **router ip-addr**: *x.x.x.x*

DHCP server – **name**: domain name.com

DHCP server – **nameserver ip-addr**: *x.x.x.x*

DHCP server – **address range:**

lower ip-addr *x.x.x.x*
upper ip-addr *x.x.x.x*

DHCP server – **subnet mask:** *x.x.x.x*

DHCP server – **leasetime**:

minimum *xxxx* minutes
maximum *xxxx* minutes

DHCP server bindings:

ip-addr	MAC addr	Leasetime (min.)
x.x.x.x	*xx:xx:xx:xx:xx:xx*	*nnnn*

show DHCP relay
Displays the DHCP relay agent's current status and configuration. Minimum level access: Administrator Sample **show dhcp relay** display: **DHCP relay** – { disabled | enabled } **DHCP relay** – **server ip-addr:** *x.x.x.x* **Maximum number of DHCP relay clients:** *xxx*
show interface **show statistics**
Refer to Chapter 5, *Monitoring the DSL Router.*
show alarms **show syslog** **show log #**
Refer to Chapter 6, *Diagnostics and Troubleshooting.*

Configuration Defaults & Command Line Shortcuts

B

Configuration Default Settings

All configuration options and factory default settings are listed alphabetically in Table B-1, Default Configuration Settings. Refer to Table B-2, Command Line Shortcuts, for abbreviated command line input.

Table B-1. Default Configuration Settings (1 of 2)

Configuration Option	Factory Default Setting
1483 encap	**LLC**
ARP cache entries	**purged**
ARP timeout for complete entries	**20 minutes**
ARP timeout for incomplete entries	**5 seconds**
authen fail (trap)	**disabled**
ccn (trap)	**disabled**
console access locally	**enabled**
devfail (trap)	**disabled**
dsl1 interface IP address (DSL)	**purged**
DHCP relay	**disabled**
DHCP relay address assignment	**purged**
DHCP server	**disabled**
DHCP server address assignment	**purged**
DHCP server max-lease-time	**4320 minutes**
DHCP server min-lease-time	**120 minutes**
DHCP server name assignment	**purged**
DHCP server nameserver assignment	**purged**
DHCP server router assignment	**purged**

Table B-1. Default Configuration Settings (2 of 2)

Configuration Option	Factory Default Setting
Ethernet frame	**DIX**
eth1 interface IP address (Ethernet)	**purged**
IP multicast	**disabled**
IP processing	**enabled**
link up (trap)	**disabled**
link down (trap)	**disabled**
login-ID	**paradyne**
NAT	**disabled**
NAT basic static IP address mappings	**purged**
NAT IP address	**purged**
NAT NAPT static port mappings	**purged**
NAT timeout	**20 minutes**
password	**abc123**
ping data size	**64 bytes**
ping time-out	**10 seconds**
proxy ARP	**disabled**
selftest (trap)	**disabled**
system identity string	**customer**
syslog IP address	**purged**
syslog level	**norm**
syslog messages	**purged**
syslog port	**514**
syslog status	**disabled**
test start (trap)	**disabled**
test stop (trap)	**disabled**
traceroute data size	**64 bytes**
traceroute time-out	**10 seconds**
traceroute max number of hops	**8**
warmstart (trap)	**disabled**

Command Line Input Shortcuts

Text in **bold** is the minimum input for each command line entry.

Table B-2. Command Line Input Shortcuts (1 of 3)

1483encap [**llc** | **vc**]
admin {**dis**able | **ena**ble}
arp create <ip–addr> <mac–addr>
arp delete <ip–addr>
arp timeout **co**mplete [<time>]
arp timeout **in**complete [<time>]
arp purge
autologout {**dis**able | **en**able}
configure {**fac**tory | **ter**minal}
console {**dis**able | **ena**ble}
clear **sta**tistics [**dsl1** | **eth1** | **ip**]
delete {**dsl1**[**:ifn**] | **eth1**[**:ifn**]}
dhcp **rel**ay {**dis**able | **ena**ble}
dhcp **rel**ay **add**ress <ip–addr>
dhcp **ser**ver {**dis**able | **ena**ble}
dhcp **ser**ver **add**ress <lower–ip> <upper–ip> [<ip–mask>]
dhcp **ser**ver **lea**setime <min–time> <max–time>
dhcp **ser**ver **nam**e <name>
dhcp **ser**ver **names**erver <ip–addr>
dhcp **ser**ver **rou**ter <ip–addr>
exit
frame [**dix** | **802**.3]
help
ifn address {**dsl1**[**:ifn**] | **eth1**[**:ifn**]} <ip–addr> <ip–mask> [primary]
ifn address **dsl1 un**numbered
ifn {**dsl1**[**:ifn**] | **eth1**[**:ifn**]} primary
ip multicast {**dis**able | **ena**ble}
ip processing {**dis**able | **ena**ble}
ip route **cre**ate <dest–ip> <dest–mask> <next–hop–ip>

Table B-2. Command Line Input Shortcuts (2 of 3)

ip route **cre**ate <dest–ip> <dest–mask> **rem**ote
ip route **cre**ate **up**stream **eth1**[**:ifn**] <next–hop–ip>
ip route **del**ete <dest–ip> <dest mask>
ip route **del**ete **up**stream **eth1**[**:ifn**]
ip route **pur**ge
list [**conf**ig]
logout
name <name>
nat basic **add**ress <ip–addr> [<ip–mask>]
nat basic **del**ete <private–ip>
nat basic **del**ete <lower–private–ip> <upper–private–ip>
nat basic **ena**ble
nat basic **map** <public–ip> <private–ip>
nat basic **map** <lower–public–ip> <lower–private–ip> <upper–private–ip>
nat disable
nat napt **add**ress <ip–addr>
nat napt **del**ete {**udp** | **tcp**} <port>
nat napt **ena**ble
nat napt **map** {**udp** | **tcp**} <server–ip> <port>
nat purge
nat timeout <time>
password {**adm**in | **ope**rator} <password>
ping <dest–ip> [**mgt** | **–x** <source-ip>] [**–l** <bytes>] [**–w** <time>] [**–i** {eth1 | dsl1}]
proxy arp {**dsl1** | **eth1**} [**dis**able | **ena**ble]
restart
save
show **ala**rms
show **arp** [<ip–addr>]
show **arp tim**eout
show **conf**ig
show **con**sole

Table B-2. Command Line Input Shortcuts (3 of 3)

show **dhc**p {**rel**ay | **ser**ver}
show **int**erface {**dsl1** | **eth1**}
show **ip rou**te [<ip–addr>]
show **log** [<number of entries>]
show **nat** {**bas**ic | **nap**t}
show **sta**tistics [**dsl1** | **eth1** | **ip**]
show **sys**log
show **sys**tem
syslog {**dis**able | **ena**ble}
syslog **ip** <ip–addr>
syslog **lev**el {**eme**r | **err** | **nor**m | **inf**o | **deb**ug}
syslog **por**t <port>
system **id**entity <identity>
traceroute <dest–ip> [**–x** <src–ip>] [**–l** <bytes>] [**–w** <time>] [**–h** <hops>] [**–i** {eth1 | dsl1}]
trap {**dis**able | **ena**ble} *name of trap*

Traps & MIBs

C

SNMP Overview

The Simple Network Management Protocol (SNMP) is an application-level protocol used in network management to gather information from network devices. Each DSL router runs an SNMP agent that collects data. The network management station in the NAP domain can exercise all the management functions remotely from the Network Operations Center (NOC).

There is no discovery of the DSL router, and it does not appear on the Management Domain map. SNMP security is configured on the MCC card and all SNMP requests to the DSL router are authenticated at the MCC. The MCC is the destination for all traps originated by the DSL router.

See the *Hotwire Management Communications Controller (MCC) Card, IP Conservative, User's Guide* for more information on SNMP.

NOTE:

There are several SNMP Sets that result in resetting the DSL router. When this happens, the NMS that sent the Set command may not receive a response from the DSL router and will time out. This is not an error.

Traps Overview

Traps inform the NMS of an alert occurring in the system (e.g. threshold exceeded). Traps are sent at the start and completion of a test or alarm condition. The MCC is the destination for all traps originated by the DSL router. These traps are then rebuilt with the trap destination information stored on the MCC and forwarded to the appropriate trap managers.

Traps are configured via a Telnet session, terminal session, or via SNMP, and are based on community names. Traps are included in the MIB II, Entity and Hotwire Enterprise MIB definitions. MIBs can be accessed through the Paradyne Web site at **www.paradyne.com**. Select *Technical Support* → *MIBS.*

The DSL system can send traps to three IP addressable destinations per community (for a total of 12 destinations).

DSL Router Traps

The table below lists the traps supported by the DSL router. All traps are defined with a severity of Critical, Major, Minor, Warning, or Normal. By default, all traps are initially disabled.

Table C-1. DSL Router Traps

Trap Event(Trap #)	Severity	Description	MIB	Variable Binding*
authenticationFailure	Minor	The authenticationFailure trap signifies an event where access has been attempted and failed. There are several conditions that can cause an Authentication Failure trap, such as three failed attempts to login.	hot_sys.mib (Hotwire System MIB)	IfIndex (RFC 1573)
cCN(7)	Warning	The configuration has changed via the user interface or an SNMP Manager. The trap is sent immediately, providing there has been no CCN trap for 30 minutes. This suppresses the sending of numerous traps when multiple changes are made in a short period of time.	hot_sys.mib (Hotwire System MIB)	IfIndex (RFC 1573)
deviceFailure(2)	Major	An internal device failure has been detected by the operating software for the DSL router.	hot_sys.mib (Hotwire System MIB)	IfIndex (RFC 1573) devFailureStatus (pdn_HealthAndStatus)
devSelfTestFailure(1)	Minor	A hardware failure of the unit was detected as part of the unit's selftest. This trap is generated after the unit has completed initialization.	hot_xdsl.mib (Hotwire xDSL interface)	IfIndex (RFC 1573) devSelfTestResults (pdn_HealthAndStatus)
diagApplTestStart(2)	Normal	At least one test has been started on an interface; e.g., Ping, TraceRoute.	hot_xdsl.mib (Hotwire xDSL interface)	IfIndex (RFC 1573) applTestID applTestType
diagApplTestStop(102)	Normal	This indicates that a test has completed on an interface.	hot_xdsl.mib (Hotwire xDSL interface)	IfIndex (RFC 1573) applTestId (pdn_diag) applTestType (pdn_diag) applTestStatus
LinkDown(3)	Normal	Informational.	IfIndex (RFC 1573)	IfIndex (RFC 1573)
LinkUp(4)	Normal	Informational.	ifIndex (RFC 1213)	IfIndex (RFC 1573)
WarmStart	Normal	The Warm Start trap signifies that the unit has just re-initialized itself. This trap is sent after the unit has been reset (either with a reset command or the result of a power disruption).	MIB II (RFC 1213)	IfIndex (RFC 1573)
* All traps have the Super Overloaded ifIndex as a variable-binding (as a minimum).				

MIBs Overview

The Hotwire DSL system supports standard as well as Paradyne Enterprise MIBs. Various configuration, status, and statistical data within the SNMP agent is accessible from the NMS. The content of an SNMP agent's MIBs is defined by various Internet Request for Comments (RFC) documents.

The following sections provide brief descriptions about supported MIBs. Complete, up-to-date details about the content of all DSL MIBs are available on the Paradyne Web site at **www.paradyne.com**. Select *Technical Support → MIBs.*

Standard MIBs

Standard MIBs supported consist of the following:

- RFC 1213: MIB II
- RFC 1573: Evolution of the Interfaces Group
- RFC 2096: IP Forwarding Table MIB
- RFC 2665: Ethernet-Like MIB

MIB II (RFC 1213)

The objects defined by MIB II (RFC 1213) are organized into ten groups:

- **System Group** – fully supported. Refer to *System Group*
- **Interfaces Group** – refer to *Interfaces Group (RFC 1573)* and *Extension to Interfaces Table (RFC 1573)*
- **Address Translation Group** – not supported.
- **IP Group** – refer to *IP Group (RFC 1213)* and *IP CIDR Route Group (RFC 2096)*
- **ICMP Group** – fully supported.
- **TCP Group** – fully supported.
- **UDP Group** – fully supported.
- **EGP Group** – not supported.
- **Transmission Group** – refer to *Transmission Group.*
- **SNMP Group** – refer to *SNMP Group.*

System Group

System Group objects are fully supported by the DSL router, as shown in Table C-2.

NOTE:

The System Name, System Contact, and System Location objects can be configured via the port card **(A-F)**. Values will display in Monitoring **(B-E)**. However, the DSL router uses and displays the SNMP information set via the System Group.

Table C-2. System Group Objects

Object	Description	Setting/Contents
sysDescr *(system 1)*	Provides a full name and version identification for the Hotwire system's hardware and software.	The object is set to display a string in the following format: PARADYNE Hotwire DSL; Model: *xxxx-xx-xxx*; S/W Release: *yy.yy.yy;* H/W Revision: *zzz;* Serial Number: *sssssssssss*; Boot: *bb.bb.bb*; 2nd Boot: *xx.xx.xx*; DSP: *xxx* Model starts with the 4-digit model number: ■ 6301 – IDSL router ■ 6302 – IDSL 4-port router ■ 6341 – SDSL router ■ 6342 – SDSL 4-port router ■ 6371 – RADSL router
sysObjectID *(system 2)*	Identifies the network management subsystem for the DSL router.	OIDs (Object Identifiers): ■ 1.3.6.1.4.1.1795.1.14.9.9.35 – 6301 IDSL router ■ 1.3.6.1.4.1.1795.1.14.9.9.36 – 6302 IDSL 4-port router ■ 1.3.6.1.4.1.1795.1.14.9.9.25 – 6341 SDSL router ■ 1.3.6.1.4.1.1795.1.14.9.9.26 – 6342 SDSL 4-port router ■ 1.3.6.1.4.1.1795.1.14.9.9.29 – 6371 RADSL router
sysContact *(system 4)*	Provides the contact information for the person managing the DSL router.	ASCII character string (32 characters), as set by the user: ■ **badValue(3)** – Field length exceeded.
sysName *(system 5)*	Provides a contact name for the DSL router.	ASCII character string (32 characters), as set by the user: ■ **badValue(3)** – Field length exceeded.
sysLocation *(system 6)*	Provides the physical location for the DSL router.	ASCII character string (32 characters), as set by the user: ■ **badValue(3)** – Field length exceeded.
sysServices *(system 7)*	The DSL router provides routing and host application services; i.e., Ping and TraceRoute.	■ **physical(1)** – Layer 1 functionality for DSL and Ethernet interfaces. ■ **datalink/subnetwork(2)** – Layer 2 functionality for: – DSL interface and – Ethernet interface (LLC) ■ **internet(4)** – Layer 3 functionality (IP) for all management links. ■ **end-to-end(8)** – Layer 4 functionality (TCP) for all management links. ■ **application(64)** – Layer 7 functionality (TCP) for all management links. Object is set to 4+8+64 (**76**).

Interfaces Group (RFC 1573)

The evolution of the Interfaces Group of MIB II (RFC 1573 converted to SNMP v1) consists of an object indicating the number of interfaces supported by the DSL router and an interface table containing an entry for each interface. Refer to Table C-3 for the objects supported for the DSL and Ethernet interfaces.

The Interface Stack Group table does not apply, but is required for MIB compliance. One row will be displayed with ifStackHigherLayer=0 and ifStackLowerLayer=0. The ifStackStatus=2 (enumerated value for notInService) and is read-only. The Interface Test Table and the Generic Receive Address Table are not supported.

Table C-3. Interfaces Group Objects (1 of 2)

Object	Description	Setting/Contents
ifNumber *(interfaces 1)*	Supported as specified in the Evolution MIB.	Specifies the number of interfaces for this unit in the ifTable.
ifIndex *(ifEntry 1)*	Provides the index into the interface table (ifTable) and to other MIB tables. ifIndex calculation: (Slot # * 1000 + local port) * 1000 + remote ifIndex	Remote ifIndex (DSL router ifIndex) and Interface: ■ **0** – DSL router. ■ **1** – Ethernet interface. ■ **2** – DSL network interface. ■ **noSuchName** – Unsupported index entered.
ifDescr *(ifEntry 2)*	Supplies text for each interface: ■ DSL interface ■ Ethernet interface	Text Strings for each interface: ■ "DSL Interface; Card Type (IDSL, RADSL, SDSL); S/W Release: *yy.yy.yy*; H/W Release:*zzz*; *[CCA part number]"* ■ "Ethernet Interface; Card Type (frame format of Type II or SNAP); S/W Release: *yy.yy.yy*; H/W Release:*zzz*; *[CCA part number]"*
ifType *(ifEntry 3)*	Identifies the interface type based on the physical/link protocol(s).	Supported values: ■ **radsl(95)** – Used for RADSL. ■ **sdsl(96)** – Used for SDSL. ■ **iso88023Csmacd(6)** – Used for Ethernet. ■ **idsl(154)** – Used for IDSL.
ifMtu *(ifEntry 4)*	Identifies the largest datagram that can be sent or received on an interface.	Integer.
ifSpeed *(ifEntry 5)*	Provides the interface's current bandwidth in bits per second (bps).	■ DSL interface – The downstream rate of the DSL interface once trained, or zero if not trained. ■ Ethernet interface – 10240000 bps (for 10 MB operation) or 102400000 (for 100 MB operation).
ifPhysAddress *(ifEntry 6)*	Identifies the physical address for the interface.	■ DSL interface – The MAC address when operating in 1483 Bridged mode. ■ Ethernet interface – The MAC address.
ifAdminStatus *(ifEntry 7)*	Supported as read-only.	■ **up(1)** – Always displays as up.

Table C-3. Interfaces Group Objects (2 of 2)

Object	Description	Setting/Contents
ifOperStatus *(ifEntry 8)*	Specifies the current operational state of the interface.	■ DSL interface: – **up(1)** – DSL link is established. – **down(2)** – DSL link is not established. ■ Ethernet interface: – **up(1)** – There is a physical connection. – **down(2)** – There is no physical connection.
ifLastChange *(ifEntry 9)*	Indicates the amount of time the interface has been up and running.	Contains the value of sysUpTime object at the time the interface entered its current operational state of Up or Down. If the current state was entered prior to the last reinitialization of the local management subsytem, then this object contains a value of 0 (zero).
ifInOctets *(ifEntry 10)*	Input Counter objects that collect input statistics on data received by the interface.	Integer.
ifInUcastPkts *(ifEntry 11)*		
ifInDiscards *(ifEntry 13)*		
ifInErrors *(ifEntry 14)*		
ifInUnknown Protos *(ifEntry 15)*		
ifOutOctets *(ifEntry 16)*	Output Counter objects that collect output statistics on data received by the interface.	Integer.
ifOutUcastPkts *(ifEntry 17)*		
ifOutDiscards *(ifEntry 19)*		
ifOutErrors *(ifEntry 20)*		

Extension to Interfaces Table (RFC 1573)

This extension contains additional objects for the Interface table. Table C-4 shows the objects supported.

Table C-4. Extension to Interfaces Table

Object	Description	Setting/Contents
ifName *(ifXEntry 1)*	Provides the name of the interface.	Specifies the interface name: ■ **dsl1** – DSL interface. ■ **eth1** – Ethernet interface.
ifHighSpeed *(ifXEntry 15)*	Displays the downstream speed for the DSL or Ethernet interface in Mbps.	Depending on the current mode of operation, displays the speed in 1 million bits per second (Mbps) of the Ethernet interface as: ■ **10 Mbps** ■ **100 Mbps** Due to the speed displaying as Mbps, the DSL interface downstream speed displays as 0 (zero).
ifConnector Present *(ifXEntry 17)*	Indicates whether there is a physical connector for the interface.	The value for all interfaces is always: ■ **true(1)**

IP Group (RFC 1213)

The Internet Protocol Group objects are supported by the unit for all data paths that are currently configured to carry IP data to/from the unit. All of the objects in the IP Group, except for the IP Address Translation table, are fully supported. Table C-5 provides clarification for objects contained in the IP Group.

Table C-5. IP Group Objects (1 of 2)

Object	Description	Setting/Contents
ipForwarding *(ip 1)*	Specifies whether the unit is acting as an IP gateway for forwarding of datagram received by, but not addressed to, the DSL router.	The value is read-only and always displays: **(1)**
ipDefaultTTL *(ip 2)*	TTL = Time To Live.	Minimum value – **15**. Maximum value – **255**. ■ **64** – Default.
ipAddrTable *(ip 20)*	The address table.	The device sets the object ipAdEntReasmMaxSixe to **16384**. Supported as read-only.

Table C-5. IP Group Objects (2 of 2)

Object	Description	Setting/Contents
ipNetToMediaTable *(ip 22)*	This table allows access to contents of the ARP cache.	This table is implemented with read/write access.
ipNetToMediaType *(ipNetToMediaEntry 4)*	Supported for ARP table entries.	■ **other(1)** – Entry is incomplete. ■ **invalid(2)** – Invalidates corresponding entry in the ipNetToMediaTable. ■ **dynamic(3)** – Results in a response with a badValue error status. Dynamic ARP table entries will still display with the correct dynamic (3) value, but a Set is not allowed. ■ **static(4)**

IP CIDR Route Group (RFC 2096)

This MIB obsoletes and replaces IP Group from MIB II. The IP CIDR Route Group objects are supported for all data paths currently configured to carry IP data to or from the device (i.e., the DSL and Ethernet interfaces). All of the objects in this group are fully supported except as noted in Table C-6. The IP Forwarding Group is not supported.

Table C-6. IP CIDR Route Group Objects (1 of 2)

Object	Description	Setting/Contents
ipCidrRouteTable *(ipForward 4)*	Replaces the ipRouteTable in MIB II. It adds knowledge of autonomous system of the next hop, multiple next hops, policy routing, and classless inter-domain routing.	This is a read/write table. If an interface route is deleted but not the corresponding upstream route (such as with DHCP relay), an SNMP Get for this object will still show a table entry for the address and mask assigned to the interface. ■ **reject(2)** – Value for route type and the ipCidrRouteDownstreamValid will be false.
ipCidrRouteDest *(ipCidrRouteEntry 1)*	Serves as an index to the routing table.	This object cannot take a Multicast (Class D) address value.
ipCidrRouteMask *(ipCidrRouteEntry 2)*	This is the mask that is logical-ANDed with the destination address.	This is the mask before being compared to the value in the ipCidrRouteDest field.
ipCidrRouteTos *(ipCidrRouteEntry 3)*	The policy specifier is the IP Table of the Service field.	This object will always be **0** (zero).
ipCidrRouteNextHop *(ipCidrRouteEntry 4)*	The next hop route IP address for remote routes.	If there is no router, the value is **0.0.0.0**.
ipCidrRouteIfIndex *(ipCidrRouteEntry 5)*	Corresponds to the IfIndex value.	Identifies the local interface through which the next hop of the route should be reached.

Table C-6. IP CIDR Route Group Objects (2 of 2)

Object	Description	Setting/Contents
ipCidrRouteType *(ipCidrRouteEntry 6)*	This is a read-only object.	■ **other(1)** – Not specified by this MIB (used as interface route). ■ **reject(2)** – Entry not valid for downstream routing. ■ **local(3)** – Route to a directly connected local host or service network. ■ **remote(4)** – Route to a nonlocal host or service network.
ipCidrRouteProto *(ipCidrRouteEntry 7)*	Corresponds to routing mechanisms via which this route was learned. Inclusion of values for gateway routing protocols does not imply that the host supports these protocols.	This is a read-only object. ■ **other(1)** – The entry is a host route set up by DHCP or loopback route. ■ **local(2)** – Local interface. ■ **netmgmt(3)** – Static route.
ipCidrRouteAge *(ipCidrRouteEntry 8)*	Reflects the number of seconds since this route was last updated or otherwise determined to be correct.	This is a read-only object. When displayed, a value of **0** (zero) represents a route that will be retained permanently.
ipCidrRouteInfo *(ipCidrRouteEntry 9)*	This object refers to the particular routing protocol responsible for this route.	If this information is not present (determined by ipCidrRouteProto value), the value is set to the OBJECT IDENTIFIER (**00**).
ipCidrRouteNextHopAS *(ipCidrRouteEntry 10)*	Next hop route.	Always set to a value of **0** (zero).
ipCidrRouteMetric1 – ipCidrRouteMetric5 *(ipCidrRouteEntry 11 – ipCidrRouteEntry 15)*	For future use.	Only value accepted is **-1**.
ipCidrRouteStatus *(ipCidrRouteEntry 16)*	Used to create or delete rows in a table.	—

Transmission Group

The objects in the Transmission Group are supported for the Ethernet Interface. These objects are not defined within MIB II but rather through other Internet-standard MIB definitions. The objects in the transmission group are extended by RFC 2665 MIB definitions. The object dot3 *(Transmission group 7)* is supported on the Ethernet Interface.

SNMP Group

The SNMP Group objects that apply to a management agent are fully supported. The following objects apply only to an NMS and return a value of **0** (zero) if accessed:

- snmpInTooBigs *(snmp 8)*
- snmpInNoSuchNames *(snmp 9)*
- snmpInBadValues *(snmp 10)*
- snmpInReadOnlys *(snmp 11)*
- snmpInGenErrs *(snmp 12)*
- snmpInGetResponses *(snmp 18)*
- snmpInTraps *(snmp 19)*
- snmpOutGetRequests *(snmp 25)*
- snmpOutGetNexts *(snmp 26)*
- snmpOutSetRequests *(snmp 27)*

Ethernet-Like MIB (RFC 2665)

Only the Ethernet-like statistics group is supported, with the following objects:

- dot3StatsIndex *(dot3StatsEntry 1)*
- dot3StatsAlignmentErrors *(dot3StatsEntry 2)*
- dot3StatsFCSErrors *(dot3StatsEntry 3)*
- dot3StatsSingleCollisionFrames *(dot3StatsEntry 4)*
- dot3StatsMultipleCollisionFrames *(dot3StatsEntry 5)*
- dot3StatsSQETestErrors *(dot3StatsEntry 6)*
- dot3StatsDeferredTransmissions *(dot3StatsEntry 7*)
- dot3StatsLateCollisions *(dot3StatsEntry 8)*
- dot3StatsExcessiveCollisions *(dot3StatsEntry 9)*
- dot3StatsInternalMacTransmitErrors *(dot3StatsEntry 10)* – always **0** (zero)
- dot3StatsCarrierSenseErrors (*dot3StatsEntry 11)*
- dot3StatsFrameTooLongs *(dot3StatsEntry 13)*
- dot3StatsInternalMacReceiverErrors *(dot3StatsEntry 16)* – always **0** (zero)
- dot3StatsSymbolErrors *(dot3StatsEntry 18)* – always **0** (zero)
- dot3StatsDuplexStatus *(dot3StatsEntry 19)*

Paradyne Enterprise MIBs

The following Paradyne Enterprise MIB Objects are supported by the unit:

- *Device Control MIB* (pdn_Control.mib)
- *Device Diagnostics MIB* (pdn_diag.mib)
- *Health and Status MIB* (pdn_HealthAndStatus.mib)
- *Configuration MIB* (pdn_Config.mib)
- *Interface Configuration MIB* (pdn_inet.mib)
- *ARP MIB* (pdn_Arp.mib)
- *NAT MIB* (pdn_NAT.mib)
- *DHCP MIB* (pdn_dhcp.mib)
- *DSL Endpoint MIB* (DslEndpoint.mib)
- *SYSLOG MIB* (pdn_syslog.mib)
- *Interface Configuration MIB* (pdn_IfExtConfig.mib)

Device Control MIB

Objects supported by the Device Control MIB, pdn-Control.mib, include the Device Control Group (fully supported) and the Device Control Download group.

Table C-7. Device Control Table Objects

Object	Description	Setting/Contents
devHWControl Reset (*control 1)*	Initiates a hardware power-on reset.	Value from this object: ■ **noOp(1)** ■ **Reset(2)** – Resets the DSL router with no warning.
devControlDownLoadIndex *(devControlDownloadEntry 1)*	Represents the firmware bank.	■ bank **(1)** ■ bank **(2)**
devControlDownLoadRelease *(devControlDownLoadEntry 2)*	Indicates the software release for the bank.	Numeric.
devControlDownLoadOperStatus *(devControlDownLoadEntry 3)*	Indicates whether the downloaded entry contains a valid or invalid software release.	■ **(1)** – Valid software release. ■ **(2)** – Invalid software release. Displays if devControlDownLoadRelease is blank.
devControlDownLoadAdminStatus *(devControlDownLoadEntry 4)*	Indicates whether the downloaded entry is active or inactive.	■ **Active(1)** ■ **Inactive(2)** Supported as read-only.

Device Diagnostics MIB

Objects supported by the Device Diagnostics MIB, pdn_diag.mib, include the Application Test Input Group (Ping and TraceRoute) and Test Traps, providing an NMS a trigger for a diagnostic test.

To start a test from NMS, you must obtain the Test ID by performing a Get. This Test ID is then used as the index when setting the parameters via objects in the Application Test Table. Refer to the applNewTestId object in Table C-8.

Table C-8. Application Test Group Objects (1 of 3)

Object	Description	Setting/Contents
applMaxNumberOfTests *(applTest 1)*	The number of application-based tests that can be started on the device.	The DSL router only supports one test.
applCurrentNumberOfTests *(applTest 2)*	The number of application-based tests that are currently running on the device.	The DSL router only supports one test at a time.
applStopAllTests (*applTest 3)*	Initiates the clearing of all application-based tests.	■ **noOp** – No operation. ■ **Stop** – All tests are stopped and current test results remain available. ■ **StopAndClear** – All tests are stopped and all test results are cleared.
applNewTestId *(applTest 4)*	To start a test from NMS, complete a Get on this object to obtain the test ID. Note that this invalidates any existing test information for Ping, TraceRoute, and Test Status tables.	■ *nnn* – Existing unused test ID. ■ **0** (zero) – A test ID cannot be assigned at this time.
applTestId *(testStatusEntry 1)*	Contains identifiers that allow NMS to find the most recent test.	Contains applNewTestID after Get.
applTestType *(testStatusEntry 2)*	Indicates the test type assigned to this object.	■ **1.3.6.4.1795.1.14.5.1.3** – Ping Test Type. ■ **1.3.6.4.1795.1.14.5.1.4** – TraceRoute Test Type.
applTestStatus *(testStatusEntry 3)*	Indicates the test status.	■ **none(1)** – No active test. ■ **inProgress(2)** – Active test. ■ **success(3)** – Test completed. ■ **failed(4)** – Test failed. ■ **abort(5)** – Test aborted.
applTestErrorCode *(testStatusEntry 4)*	Contains additional test details, such as error codes.	Test Error codes: ■ **none** – No errors. ■ **timeout** ■ **icmpError** ■ **systemError**

Table C-8. Application Test Group Objects (2 of 3)

Object	Description	Setting/Contents
applTestOwner *(testStatusEntry 5)*	Identifies who started the test.	1 – 40 characters.
applTestRowStatus *(testStatusEntry 6)*	Use to create a new row or delete an existing row.	Set to **active(1)** to create a new row.
applPingTestId *(applpingTestEntry 1)*	Contains identifier that allows the Network Manager to view the results of Ping and TraceRoute tests.	Device supports only one at a time.
applPingTestIpAddress *(applpingTestEntry 2)*	Identifies IP address to be pinged.	Set destination IP address.
applPingTestSourceIpAddress *(applpingTestEntry 3)*	Identifies the source IP address.	Set source IP address.
applPingTestPacketSize *(applpingTestEntry 4)*	Specifies Ping packet size. Range includes 28 bytes of header information.	■ **28** – **15028** – Range. ■ **64** – Default.
applPingTestTimeout *(applpingTestEntry 5)*	Number of seconds between echo request attempts.	■ **10** – Default**.**
applPingTestMaxPings *(applpingTestEntry 6)*	Maximum number of Pings.	■ **1** – Only supported value.
applPingTestPktsSent *(applpingTestEntry 7)*	Number of packets sent.	■ **1** – Only supported value.
applPingTestPktsRecv *(applpingTestEntry 8)*	Number of packets received without error.	■ **0** ■ **1**
applPingTestMinTime *(applpingTestEntry 9)*	Minimum round trip time.	■ **0** – Not supported.
applPingTestMaxTime *(applpingTestEntry 10)*	Maximum round trip time.	■ **0** – Not supported.
applPingTestAvgTime *(applpingTestEntry 11)*	Average round trip time.	■ **0** – Not supported.
applPingTestDomain *(applpingTestEntry 12)*	Specifies the destination IP address's domain as management or service. If the source IP address is entered, mgmt(2) is not valid.	■ **mgmt(2)** – Management domain. ■ **service(3)** – Service domain.
applPingTestIfIndex *(applpingTestEntry 13)*	Specifies the interface over which the Ping will take place.	Defaults to the interface based upon current routing.
applTracerouteTestId *(traceroute 1)*	Unique TraceRoute test ID.	Contains applNewTestID after Get.
applTracerouteIpAddress *(traceroute 2)*	Destination IP address for TraceRoute test.	Set destination IP address.
applTracerouteSourceIpAddress *(traceroute 3)*	Identifies the source IP address.	Set source IP address.

Table C-8. Application Test Group Objects (3 of 3)

Object	Description	Setting/Contents
applTraceroutePacketSize *(traceroute 4)*	Specifies TraceRoute packet size. Range + 28 bytes of header information.	■ **28** — **15028** – Range. ■ **64** – Default.
applTracerouteTimeOut *(traceroute 5)*	Timeout value in seconds between echo request attempts.	■ **10** – Default.
applTracerouteMaxHops *(traceroute 6)*	Maximum number of hops to be tested.	■ **8** – Default.
applTracerouteDomain *(traceroute 7)*	Specifies the destination IP address's service domain.	■ **mgmt(2)** – Management Domain. ■ **service(3)** – Service Domain. Default.
applTracerouteIfIndex *(traceroute 8)*	Specifies the route for the TraceRoute test.	If the target interface is not specified, the default will display the calculated ifIndex.
applTracerouteTestOwner *(traceroute 9)*	Identifies who started the test.	1 – 40 characters.
applTracerouteTestId *(applTracerouteResultsEntry 1)*	Contains the results of a TraceRoute test.	Supports only one test per device.
applTracerouteHopCount *(applTracerouteResultsEntry 2)*	Number of hops to reach the gateway.	—
applTracerouteResultsIpAddr *(applTracerouteResultsEntry 3)*	IP address of the gateway.	—
applTracerouteResultsHopCount *(applTracerouteResultsEntry 4)*	Number of hops to reach the gateway.	—
applTracerouteResultsPacketSize *(applTracerouteResultsEntry 5)*	Specifies the data size of the packets (in bytes) sent during the TraceRoute test.	—
applTracerouteResultsProbe1 *(appTracerouteResultsEntry 6)*	Displays roundtrip time in 100 ms intervals of the first probe sent to the gateway.	■ **0** – Probe has timed out.
applTracerouteResultsProbe2 *(applTracerouteResultsEntry 7)*	Displays roundtrip time in 100 ms intervals of the second probe sent to the gateway.	■ **0** – Probe has timed out.
applTracerouteResultsProbe3 *(applTracerouteResultsEntry 8)*	Displays roundtrip time in 100 ms intervals of the third probe sent to the gateway.	■ **0** – Probe has timed out.
diagTestTrapEnable *(configure 1)*	Use to enable or disable diagApplTestStart and diagApplTestStop traps.	Bit Sum. ■ **1** – Test Start. ■ **2** – Test Over.

Health and Status MIB

Objects supported by the Health and Status MIB, pdn_HealthAndStatus.mib, include the following groups:

- Device Health and Status
- Device Selftest Status
- Device Abort Status
- Device Failure Status
- Traps

Table C-9. Device Status Group Objects Table

Object	Description	Setting/Contents
devHealthandStatus *(devStatus1)*	This object displays alarm messages if any alarms are generated by the device.	Possible alarms are: ■ Alarm: Management Address Conflict. ■ Alarm: Failed Selftest. ■ Alarm: System Error. ■ No alarm is set.
devSelfTestResults *(devStatus 2)*	This object corresponds to self-test results. This value is used as a binding for devSelfTestFailure Trap.	■ **P** – Passed selftest. ■ **F** – Failed selftest.
devAbortStatus *(devStatus 3)*	This object is used to retrieve the latest abort status that is stored in the agent.	Possible abort codes are: ■ INVALID_INTR ■ INT_TIMEOUT ■ O_YAMOS_FAILURE ■ INIT_NOBUFS ■ SYSCALL_FAILED ■ G_NO_BUF ■ G_BAD_CONFIG ■ G_NO_ABORT
devFailureStatus *(devStatus 4)*	This object is used to retrieve the latest failure status.	This value is used as a binding for the deviceFailure trap.
devStatusTrapEnable *(devStatus 8)*	Allows user to enable or disable the selftest failure indication trap and the device failure indication trap individually.	Bit Sum. ■ **1** – devSelfTest failure. ■ **2** – device failure.
devStatusTestFailure	Signifies that the sending protocol's device failed selftest.	The variable binding for this trap is the devSelfTestResults object of the Health and Status MIB.
deviceFailure	Signifies that the sending protocol's device failed.	The reason for the failure was not selftest.

Configuration MIB

The supported groups used with the DSL Configuration MIB, pdn_Config.mib, are:

- Device Configuration Copy Group
- Trap Configuration Group
- Paradyne Device Configuration Time Group
- Traps

Table C-10. Device Configuration Copy Group Objects Table

Object	Description	Setting/Contents
devConfigAreaCopy *(devConfigArea1)*	Use to configure the current configuration to the factory defaults settings. NOTE: ALL current configuration input is purged when the DSL router is resets as a result of this command. Data purged includes: – Interface IP addresses – IP route table entries – ARP cache entries – NAT entries – DHCP server entries	■ **noOp (1)** – always reads as this value and represents: **factory1-to-active(8)**
devConfigTrapEnable *(devConfigTrap1)*	This object determines which trap types are sent, represented by a bit map as a sum. Allows multiple trap types to be enabled or disabled simultaneously.	Bit positions: ■ **1** – warmStart trap ■ **2** – authenticationFailure trap ■ **4** – enterpriseSpecific traps ■ **8** – LinkUp trap ■ **16** – LinkDown trap
devConfigTimeOfDay *(devConfigTime 1)*	Displays the current time.	—
cCN(7)	Signifies a configuration change or a software upgrade.	■ **7** – Warning trap
cCNTrapEnable *(router 28)*	Use to enable or disable the configuration change trap.	■ **1** – Disable trap ■ **2** – Enable trap

Interface Configuration MIB

The Paradyne proprietary Interface Configuration group, pdn_inet.mib, is supported. Refer to Table C-11 for additional details.

Table C-11. Interface Configuration Group Objects Table

Object	Description	Setting/Contents
pdnInetIpAddress *(pdnInetIpAddressTableEntry 1)*	Identifies the interface IP address.	■ Interface IP address or ■ **0.0.0.0** – Unnumbered interface
pdnInetIpSubnetMask *(pdnInetIpAddressTableEntry 2)*	Identifies the interface subnet mask.	■ **P** – Passed selftest ■ **F** – Failed selftest
pdnInetIpAddressType *(pdnInetIpAddressTableEntry 3)*	Use to view the address type for an interface. Supported as read-only.	■ **primary** ■ **secondary**
pdnInetIpRowStatus *(pdnInetIpAddressTableEntry 4)*	Use to add/delete/modify rows in this table.	When used to add a new interface entry, the objects specifying the table entry must be included in the same Set PDU.

ARP MIB

The objects from the proxy ARP MIB group, pdn_Arp.mib, are:

- pdnNetToMediaClearAllArp *(pdnNetToMediaConfig 2)* – Setting this object to **clear** removes all entries from the ARP table and is equivalent to the command: **`arp purge`**
- pdnNetToMediaProxyArpTable

NAT MIB

The objects in the Network Address Translation MIB group, pdn_NAT.mib, are fully supported. The groups are:

- **Network Address Translation Group** – Facilitates the creation and configuration of NAT entries. The DSL router accepts any valid public IP address (up to 256 addresses) and subnet mask for basic NAT operation.
- **NAPT Mapping Group** – Facilitates the creation and configuration of NAPT mappings. The DSL router accepts any single, public IP address for NAPT operation. The subnet mask 255.255.255.255 is used when the NAPT IP address configuration information is viewed.
- **NAT Basic Mapping Group** – Facilitates the creation and configuration of Basic NAT mappings.

DHCP MIB

The supported objects in the DHCP Server/Relay MIB, pdn_dhcp.mib, facilitates the creation and configuration of DHCP server table entries. The following groups are supported:

- **DHCP Server Configuration Group** – Fully supported. One object is clarified below:
  - dhcpServerRouterIpAddr *(dhcpserv 7)* – Enables you to configure the router IP address used by the DHCP server. This address is provided to clients in the DHCP reply message from the DHCP server. If this value is not set, the accepted value is **0**.**0.0.0**.
- **DHCP Binding Group** – Facilitates the display of DHCP bindings. This group is fully supported.
- **DHCP Relay Group** – Facilitates the display of DHCP Relay. This group is fully supported. The following clarifies some of the DHCP Relay objects:
  - dhcpRelayIpAddr *(xdslDhcpRelayAgent 6)* – This is the IP address of DHCP server.
  - dhcpRelayEnable *(xdslDhcpRelayAgent 7)* – Use to enable or disable the DHCP relay agent.
  - dhcpRelayMaxClients *(xdslDhcpRelayAgent 8)* – Enables user to specify the number of clients allowed to request IP address assignments from the server.

DSL Endpoint MIB

This DSL Endpoint MIB, pdn_DslEndpoint.mib, facilitates configuration of DSL multirate products and is fully supported. Objects are clarified in Table C-12. The groups in this MIB are:

- IP Routing Group – This table is an extension of the ipCidrRoute table (see *IP CIDR Route Group (RFC 2096)* on page C-8.
- IP Multicast Group
- IP Processing Group
- Console Group

Table C-12. DSL Endpoint Configuration Group Objects Table

Object	Description	Setting/Contents
ipCidrRouteUpstreamNextHop *(IpCidrRouteXEntry 1)*	Corresponds to the upstream Next Hop Router address. If the DSL interface is numbered, each upstream Next Hop Router address must be in a subnet defined by a DSL interface IP address and subnet mask.	■ Ethernet Interface IP address. ■ **0.0.0.0** – No upstream next hop is identified.
ipCidrRouteDownstreamValid *(IpCidrRouteXEntry 2)*	If false, the row containing it is not valid for downstream routing.	■ **true** ■ **false**
ipCidrClearAllRoutes *(IpCidrRouteX 2)*	If set to clear, all IP routes are removed from the routing table.	■ **noOp** ■ **clear**
ipCidrRouterID *(IpCidrRouteX 3)*	Specifies the router ID (primary IP address).	Must be equal to a nonzero value for the interface IP address.
pdnIpMulticastEnable *(pdnRouterConfiguration 1)*	Enables or disables forwarding of IP multicast packets.	■ **enable** ■ **disable**
pdnIpProcessingEnable *(pdnRouterConfiguration 2)*	Enables or disables service domain processing of IP packets.	This setting is retained across power cycles.
pdnConsoleEnabled *(pdnRouterConfiguration 7)*	Enables or disables the console port.	■ **true(1)** – Enable. ■ **false(2)** – Disable.

SYSLOG MIB

The System Log MIB (SYSLOG), pdn_syslog.mib, is fully supported.

Interface Configuration MIB

The Interface Configuration MIB, pdn_IfExtConfig.mib, is used to configure interface-related objects and is fully supported. One object is clarified below:

- pdn_IfExtConfigIPRoutedPDUs *(pdnIfExtConfigEntry 1)* – You can configure the IP-routed PDUs in the LLC SNAP encapsulation or VC-based Multiplexing encapsulation (RFC1483) in the upstream direction. If neither is configured, the value none is used.

DSL Router Terminal Emulation

D

DSL Router Terminal Emulation

The Command Line Interface is available at the DSL router when the Console cable is connected to a VT100-compatible terminal or a PC running a terminal emulation program. Verify the terminal settings:

- Data rate set to 19.2 kbps (19200 bps)
- Character length set to 8
- Parity set to None
- Stop bits set to 1
- Flow control set to Off or None

Accessing the List Command Output

Use the **`list confg`** command to output command strings needed to restore the current running configuration. Output from the List Confg command can be captured to a text file using most terminal emulation programs. Examples of two VT100-compatible programs are provided.

Once the text file is captured, the DSL router can be placed in configuration mode. The text file can be fed back to configure the DSL router.

Terminal Emulation Programs

Examples of configuring two different terminal emulation programs:

- **HyperTerminal** – playback feature is accessed through its Transfer menu.
- **Procomm+** – playback feature is accessed through its Online menu.

▶ Procedure

To configure the HyperTerminal:

1. Select menu option *Transfer* → *Send Text File.*
2. Select *File* → *Properties.*
3. In the Properties dialog, select the Settings tab.
4. Set Emulation to VT100.
5. Select the Terminal Setup button and set to 132 column mode.
6. Select OK to exit Terminal Setup.
7. Select the ASCII Setup button.
   - — Set Line delay to 50 ms.
   - — Set Character delay to 2 ms.
8. Select OK to exit ASCII Setup.
9. Select OK to exit Properties.

▶ Procedure

To configure Procomm+:

1. Select menu option *Online* → *Send File.*
2. In the Send File dialog, set the protocol to ASCII.
3. Select the Setup button.
4. Select the Transfer Protocol button (on the left).
5. Select ASCII in the Current Protocol drop-down box.
   - — Set delay between Character to 2 ms.
   - — Set delay between Lines to 2 ms.
6. Check and set Use 13 for Line pace character.
7. Check display text.
8. Save the configuration.

Index

Symbols

Numbers

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V