BitStorm™ 4800

User's Guide

Document No. 4800-A2-GB20-10

July 2002

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

About This Guide

Document Purpose and Intended Audience

This guide contains information necessary for the use of the three user interfaces of the BitStorm 4800 IP DSLAM:

- Command Line Interface (CLI)
- Web Interface
- SNMP Interface

It is designed for technicians who administer DSL multiplexers, especially those used in Multi-Tenant Unit (MTU)/Multi-Dwelling Unit (MDU) applications.

Document Summary

Section	Description
Chapter 1, BitStorm 4800 Overview	Provides an introduction to the capabilities of the BitStorm 4800.
Chapter 2, Terminology and Conventions	Defines terms used in this manual and in the product's user interfaces.
Chapter 3, Using the Command Line Interface	Explains how to use the Command Line Interface (CLI).
Chapter 4, *Using the Web Interface*	Exlains how to use the web interface.
Chapter 5, *Monitoring and Troubleshooting*	Describes tools for monitoring the system and diagnosing problems.
Appendix A, CLI Command Descriptions	Provides detailed descriptions of all CLI commands.
Appendix B, SNMP Traps	Describes the SNMP traps supported.
Appendix C, MIB Support	Describes the MIBs and objects supported.
Appendix D, OID Cross Reference	Lists supported MIB Object IDs by number.

Section	Description
Appendix E, CLI to MIB Object Cross Reference	Contains a table showing what MIB objects are used to implement CLI commands.
Appendix F, Reference Tables	Contains tables used in CLI commands and web interface screens.
Index	Lists key terms, concepts, and sections in alphabetical order.

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

Product-Related Documents

Complete documentation for this product is available online at **www.paradyne.com**. Select *Library* → *Technical Manuals* → *BitStorm DSL Systems*.

Document Number	Document Title
4800-A2-GN10	*BitStorm 4800 Management Module Installation Instructions* Describes how to install the 4800 and 4804 Management Modules in the BitStorm 4800.
4821-A2-GN20	*BitStorm 4800 Installation Guide* Describes the installation and cabling of the BitStorm 4800 IP DSLAM.
6051-A2-GZ40	*BitStorm 6051 POTS Splitter Installation Instructions* Describes how to install the POTS splitter card and chassis used with the BitStorm 4800 in North America.

To order a paper copy of a Paradyne document:

- Within the U.S.A., call 1-800-PARADYNE (1-800-727-2396)
- Outside the U.S.A., call 1-727-530-8623

Reference Documents

AF-NM-0095.001, *ATM Forum SNMP M4 Network Element View MIB*

ANSI T1.413-1998, *Network to Customer Installation Interfaces – Asymmetric Digital Subscriber Line (ADSL) Metallic Interface*

IEEE 802.1D, *Media Access Control (MAC) Bridges*

IEEE 802.1Q, *Virtual Bridged Local Area Networks*

IEEE 802.3z, *Gigabit Ethernet*

IETF draft-ietf-adslmib-adslext-07.txt, *Definitions of Extention Managed Objects for ADSL Lines*

ITU-T 992.1, *Single-Pair High-Speed Digital Subscriber Line (SHDSL) transceivers*

ITU-T 992.2, *Asymmetrical digital subscriber line (ADSL) transceivers*

RFC 1213, *MIB-II*

RFC 1471, *PPP/LCP MIB*

RFC 1483, *Bridge MIB*

RFC 1659, *RS-232-Like MIB*

RFC 1700, *Assigned Numbers*

RFC 1907, *MIB for SNMPv2*

RFC 2011, *SNMPv2 MIB for IP*

RFC 2096, *IP Forwarding Table MIB*

RFC 2515, *ATM MIB*

RFC 2662, *ADSL Line MIB*

RFC 2665, *Ethernet-Link MIB*

RFC 2668, *802.3 MAU MIB*

RFC 2737, *Entity MIB*

RFC 2863, *Interfaces Group MIB*

BitStorm 4800 Overview

1

Overview

The BitStorm™ 4800 IP DSLAM is an access gateway that combines in one device:

- Layer 2 switching
- Aggregation
- Element management
- Provisioning
- Digital Subscriber Line (DSL) support

The BitStorm 4800 is a replacement for and an alternative to multi-device solutions with switches, routers, and servers that require rewiring buildings, and expensive, downsized ATM DSLAMs not designed for Multi-Tenant Unit (MTU)/Multi-Dwelling Unit (MDU) applications.

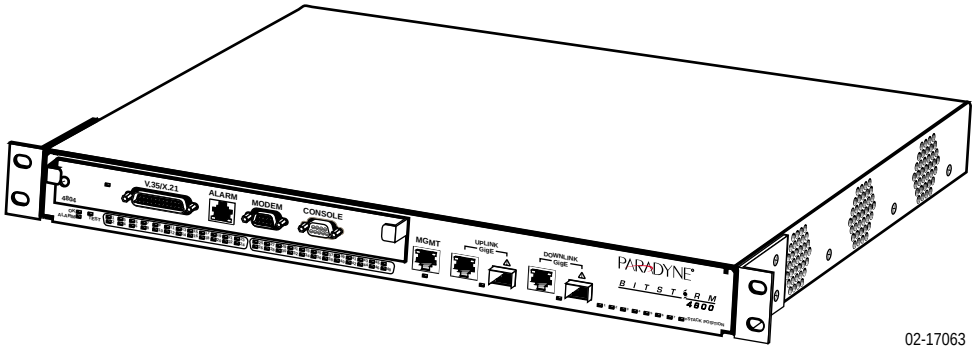


Figure 1-1. BitStorm 4800 with 48 Ports and Model 4804 Management Module

Figure 1-2 shows a typical application for the BitStorm 4800.

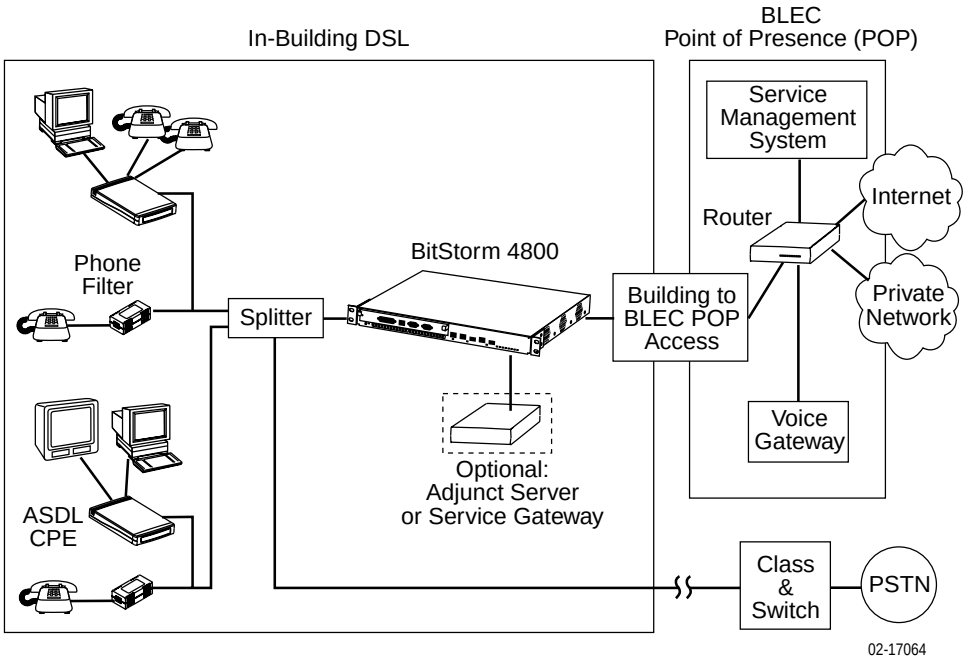


Figure 1-2. BitStorm 4800 Sample Application

Features

The BitStorm 4800 IP DSLAM has the following features:

- Compact size (height = 1U)
- Shelf-mountable (up to eight units high) and rack-mountable
- Low price per port
- Up to 48 ports per unit
- Up to 384 ports per stack, with a single high-speed uplink
- Multiple uplink options:
  - — Gigabit Ethernet uplink using wire or fiber
  - — V.35, EIA-530-A, or X.21 uplink using Model 4804 Management Module with suitable adapter
- Little or no connection management and configuration (uses learning bridge capabilities of Ethernet)
- IEEE 802.3x standards-based flow control for maximum performance and minimum packet loss
- Auto-rating DSL technology to adjust to line conditions
- Auto-sensing on all Ethernet ports to adjust automatically to the speed of attached devices
- Automatic detection of full duplex or half duplex operation on all Ethernet ports
- Automatic switchover detection for Medium-Dependent Interface (MDI) and MDI crossover (MDIX) connections, ensuring plug-and-play compatibility with hubs and endstations
- Web-based server for management
- Virtual Private Networking (VPN) for management, using the IPSec security protocol
- Command Line Interface (CLI) like that of popular routers
- Support for Simple Network Management Protocol (SNMP) Version 1 and Version 2
- Support for off-the-shelf Asynchronous DSL (ADSL) endpoints
- Uplink VLAN tagging for billing and access control

Terminology and Conventions

2

System Terminology

The following terms are used in this manual and the product's user interfaces:

- Port
- Unit
- Stack

Port

A port is one of the physical interfaces of a BitStorm 4800 or Management Module. These are:

- ALARM
- CONSOLE
- DOWNLINK GigE (RJ45)
- DOWNLINK GigE (SFP)
- DSL Ports 1–24 (24-port model) or 1–48 (48-port model)
- MGMT
- MODEM
- UPLINK GigE (RJ45)
- UPLINK GigE (SFP)
- V.35/X.21

Unit

A single BitStorm 4800 is referred to as a unit or chassis. The first or only unit is referred to as Unit 1.

Stack

Up to eight units may be interconnected, sharing a single uplink; this arrangement is called a stack.

DSL Port ID

There are several ways a DSL port can be identified in the BitStorm 4800. The term Port ID in this manual, in reference to a DSL port, refers to any of the possible identifiers for a DSL port.

- **Interface Number.** Ports 1–48 of the BitStorm 4800 can be referred to by the numbers 1–48 respectively. Port numbers 25–48 are invalid for the 24-port model.

  Example:

  ```
  IAC#configure interface dsl 24 line-code dmt
  ```

- **Interface Name.** You can use the **configure interface dsl name** command to assign a name to the port, which you can then use instead of the number. See *Reserved Names* on page 2-3.

  Example:

  ```
  IAC#configure interface dsl room_401 line-code dmt
  ```

- **Unit Number/Port Number.** The port ID can be expressed as a combination of the BitStorm 4800 unit number and a port number. In the initial release, 1 is the only valid unit number.

  Example:

  ```
  IAC#configure interface dsl 1/47 line-code dmt
  ```

- **Unit Number/Port Name.** The unit number can be used with the DSL port name to identify a port.

  Example:

  ```
  IAC#configure interface dsl 1/room_401 line-code dmt
  ```

- **All.** The keyword **all** may be used to specify all DSL ports in a command that refers only to DSL ports.

  Example:

  ```
  IAC#configure interface dsl all line-code dmt
  ```

- **Range.** Any of the port ID types may be used as an operator in a range specification. The only requirement is that the port used as the first operator in a range must have a lower interface number than the second operator.

  Examples:

  ```
  IAC#configure interface dsl room_401-room_424 line-code
  dmt
  IAC#configure interface dsl room_401-24 line-code dmt
  IAC#configure interface dsl 1-24 line-code dmt
  ```

Ethernet Port ID

The Ethernet ports on the BitStorm 4800 are identified by the following names:

- **mgmt** – for the MGMT port
- **downlink** – for the Ethernet DOWNLINK GigE port
- **uplink** – for the Ethernet UPLINK GigE port

These can be used alone or in combination with the unit number to identify the three ports. Unit number is described in *System Terminology* on page 2-1. The term Port ID in this manual, in reference to an Ethernet port, refers to any of the possible identifiers for an Ethernet port.

Example:

```
IAC#configure interface ethernet downlink mode auto

IAC#configure interface ethernet 1/uplink mode auto
```

Reserved Names

The following are reserved names and may not be assigned as DSL port names:

- / (slash)
- all
- dhcp
- downlink
- mgmt
- uplink
- v35

Using the Command Line Interface

3

Overview

The Command Line Interface (CLI) is accessible via either a directly connected terminal session or a Telnet connection. You can use the CLI to:

- Change the operational characteristics of the device by setting configuration values
- Display system status
- Perform diagnostics

The system supports multiple simultaneous CLI sessions.

Access Levels

CLI users have one of two access levels:

- **User** – The user may display certain configuration and status information.
- **Administrator** – The user has access to all commands.

The Administrator level requires a second password.

At least one login ID and one password are internally stored for each user, and can be modified by the administrator. If the user has administrator privileges, one login ID and two passwords are stored (one for User privilege and one for Administrator privilege). The passwords must be different for User level and Administrator level access for the same login ID.

Logging In

When the CLI connection is first established, a login prompt is displayed:

```
Login>
```

Enter a user name. The first time you log in on a new unit, type the name **admin** and press Enter. The password prompt is displayed:

```
Password>
```

Enter the password associated with the user name. The default password for admin is null, so press Enter without typing anything. The following prompt is displayed:

```
IAC>
```

Type **privilege** and press Enter. The password prompt is displayed again to show that you must enter the administrator privilege password. The first time you log in, just press Enter.

The following prompt is displayed:

```
IAC#
```

For security purposes, immediately establish new passwords for the user name admin. See *Configure User-Accounts* in Appendix A, *CLI Command Descriptions*.

Command Line Prompts

The command line prompt shows the user access level, whether there are any unsaved configuration changes, and at what level you are in the command tree.

For the User access level, the following prompt is displayed:

```
IAC>
```

For the Administrator access level, the following prompt is displayed:

```
IAC#
```

If changes have been made to the configuration in this or a previous session that have not been changed, an exclamation point is added to the prompt. For example:

```
IAC#!
```

The next section, *Modes of Operation*, shows how your position in the command tree further affects the prompt.

Modes of Operation

You may enter CLI commands in their entirety on one line. For example:

```
IAC#!configure interface dsl 1/1 line-code dmt

IAC#!configure interface dsl 1/1 latency fast
```

Alternatively, you may logically position the command interface at any point in the command tree structure by entering partial commands. The prompt shows where you are in the command structure. For example:

```
IAC#configure

IAC(configure)#interface

IAC(configure-interface)#dsl

IAC(configure-interface-dsl)#1/1

IAC(configure-interface-dsl-1/1)#line-code dmt

IAC(configure-interface-dsl-1/1)#!latency fast
```

You can move back up the command tree using the **back** command.

Back Command

The **back** command positions the CLI up one level in the command tree. For example, if DSL interface 1/1 is being configured, the following prompt is displayed:

```
IAC(configure-interface-dsl-1/1)#
```

Each **back** command positions the interface one level higher:

```
IAC(configure-interface-dsl-1/1)#back

IAC(configure-interface-dsl)#back

IAC(configure-interface)#back

IAC(configure)#_
```

Automatic Command Completion

Commands and keywords can be abbreviated to as few characters as are required to make them uniquely identifiable. For example, **con** is a valid abbreviation for **configure** and **cop** is a valid abbreviation for **copy**, but the abbreviation **co** is ambiguous.

You can request automatic completion of a command or keyword you have partially typed by pressing the Tab key. If the command or keyword you have typed is ambiguous, the Tab key displays the options for completion.

Command History Buffer

The last 15 commands are maintained in a command history buffer. You can use the Up Arrow and Down Arrow keys to scroll through and redisplay commands, then alter and resubmit a command maintained in the buffer.

More Prompt

The CLI lets you control the flow of text to the screen with a **paging** command (see *Paging* in Appendix A, *CLI Command Descriptions*).

If paging is disabled, text is sent to the screen without interruption. If paging is enabled, only 23 lines of text are displayed at a time. A **More** prompt is displayed on line 24 of your screen, and you can do the following:

- To view the next screen of output, press the spacebar.
- To view the next line of output, press the Enter key.
- To return to the command line, press **q** or any other key besides the spacebar and Enter key.

The paging command affects only the user who enters the command.

Command Help

You can obtain help when you enter commands by using the following methods:

- To list all commands for a specific level, enter a question mark (?) at the system prompt:

  ```
  IAC#?
  ```

- To obtain a list of commands that start with a particular character set, enter an abbreviated command immediately followed by a question mark:

  ```
  IAC#configure sys?
  ```

- To list a command's keywords or arguments, enter a question mark in place of a keyword or argument on the command line:

  ```
  IAC#configure management ?
  ```

Keyboard Definitions

The following table summarizes the special uses of keys in the CLI:

Press . . .	To . . .
Ctrl-c	Clear the current command line entry, exit a command line prompt without answering, or abort the command in progress.
Ctrl-z	Terminate a privileged mode session and continue the session in standard mode. If Ctrl-z is entered by a user not in privileged mode, it places the user at the top of the command tree.
Down Arrow	Recall commands from the command line history buffer starting with the first command in the buffer.
Enter	Submit the current command line, or, if a **More** prompt is displayed, display the next line of text.
q	Abort a **More** prompt and return to the command line prompt. (Pressing any key other than Enter or the spacebar has this effect.)
? (Question Mark)	Display the Help text for the current command.
Spacebar	Display the next page of output when a **More** prompt is displayed on line 24 of your screen.
Up Arrow	Scroll to the previous valid command line entry leaving the cursor at the end of the entry.

Command Syntax Error Handling

The CLI checks the syntax of commands you enter. If an error is detected, the following prompt is displayed:

```
Syntax error - use '?' to see valid completions
```

The prompt returns to normal when you press the Enter key.

Automatic Logout

The unit automatically terminates the CLI session if the Inactivity Timeout duration is exceeded. The Inactivity Timeout is configurable. See *Configure System Options* in Appendix A, *CLI Command Descriptions*.

Configuring the System

In order to configure the unit you must be at the Administrator access level.

Configuration changes take effect immediately. However, the changes are made to the running configuration, which is in RAM (Random Access Memory). You must enter the **save** command to save your changes to the startup configuration in NVRAM (Non-Volatile RAM).

If there are unsaved changes, an exclamation point (!) is added to the prompt to remind you, or other administrators, of the outstanding changes. The changes remain in RAM and can be saved until the unit is powered off or reset.

For information about what elements of the system you can configure, see the **configure** commands in Appendix A, *CLI Command Descriptions*, beginning with *Configure Bridge* on page A-5.

Using the Web Interface

4

Overview

The BitStorm 4800 supports a Web interface that can be used with a Web browser to perform the same functions as the command line interface:

- Change the operational characteristics of the device by setting configuration values
- Display system status
- Perform diagnostics

Web interface users have one of two access levels:

- **User** – The user may display certain configuration and status information.
- **Administrator** – The user has access to all screens and functions.

The unit configuration can be changed only by a user with Administrator level access.

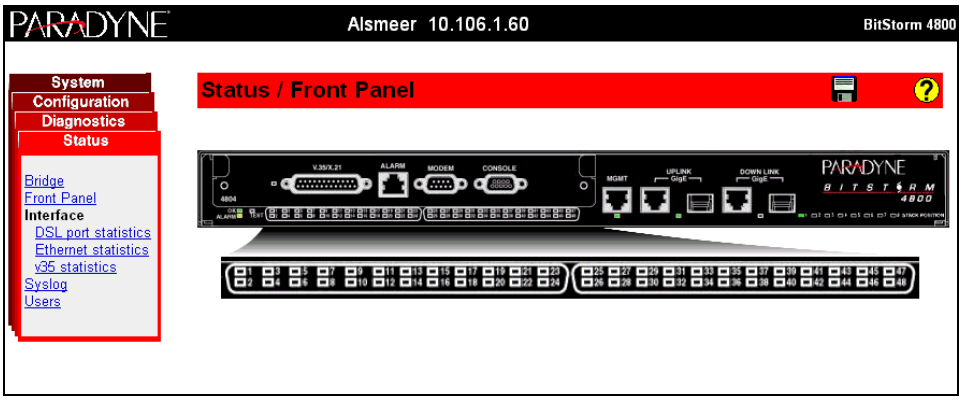
Browsers Supported

The Web interface can be used with Internet Explorer version 4 or above, and Netscape 4.7 and above, under Windows or Unix. Under Windows, version 6 or above of either browser is recommended.

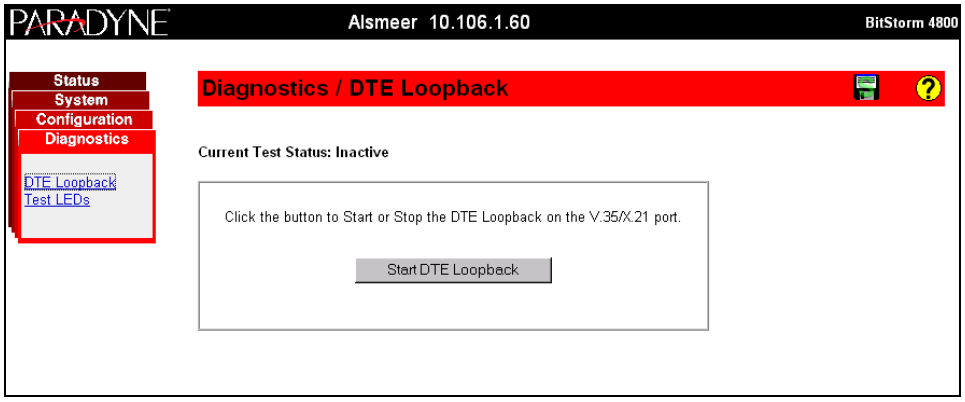
Navigation

All main screens of the Web interface can be reached by clicking on hyperlinks in the four menu boxes on the left side of the screen:

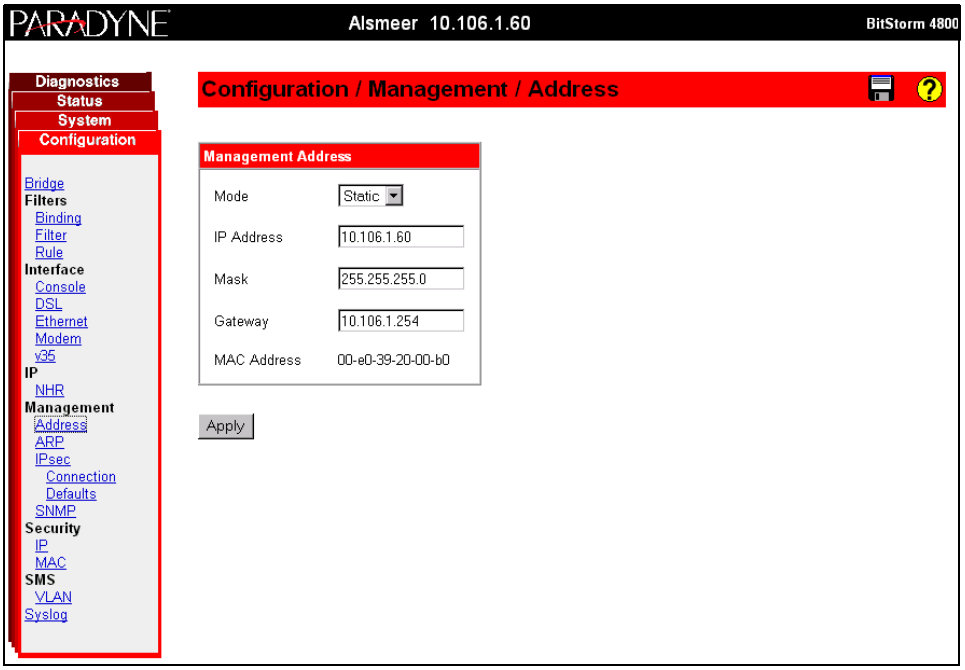
- **Status** – Use the Status screens to display statistics, status, and contents of memory. The Status screen of a 48-port model is shown.



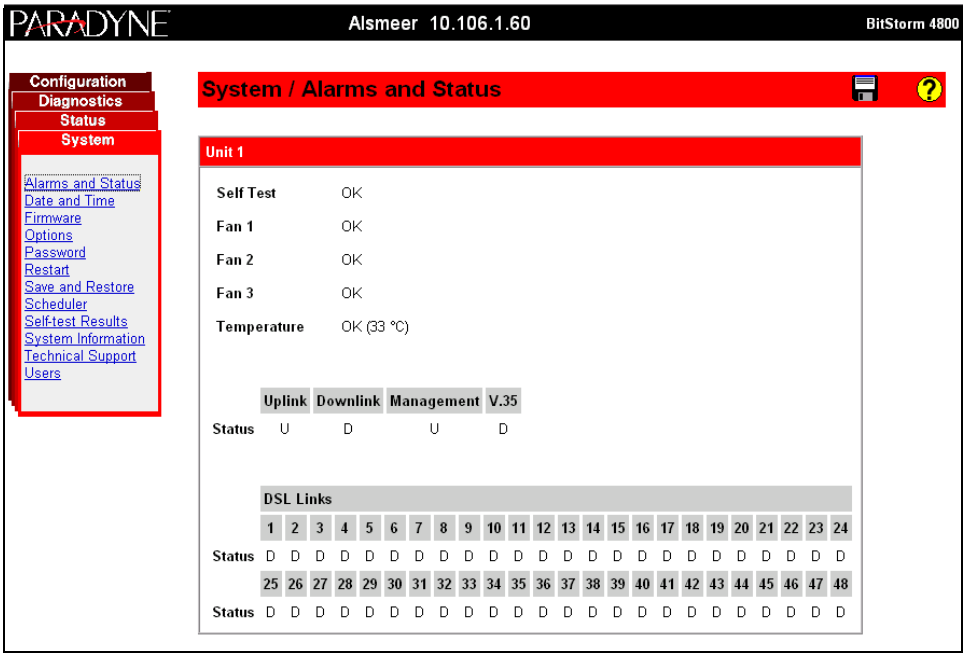
- **Diagnostics** – Use the DIagnostics screens to start and stop tests.



- **Configuration** – Use the Configuration screens to configure the system, interfaces, and filters.



- **System** – Use the System screens to display system information, download firmware, back up configurations, and modify users.



For more information, click on the Help button on any screen.

Logging In

When you first connect to the BitStorm 4800 (by opening its IP address in your Web browser), a password dialog box appears. Enter **admin** for the User Name, and enter nothing in the Password field. Click on OK.

For best security, use the System/Users screen to immediately change the default password for the admin user.

Configuring the System

Use the **Configuration** screens to configure the following:

- Bridge table
- Filters
- Interfaces
- Management
- Security
- Subscriber Management System Virtual Local Area Network
- System log

Use the **System** screens to configure the following:

- Date and time
- System options and identification

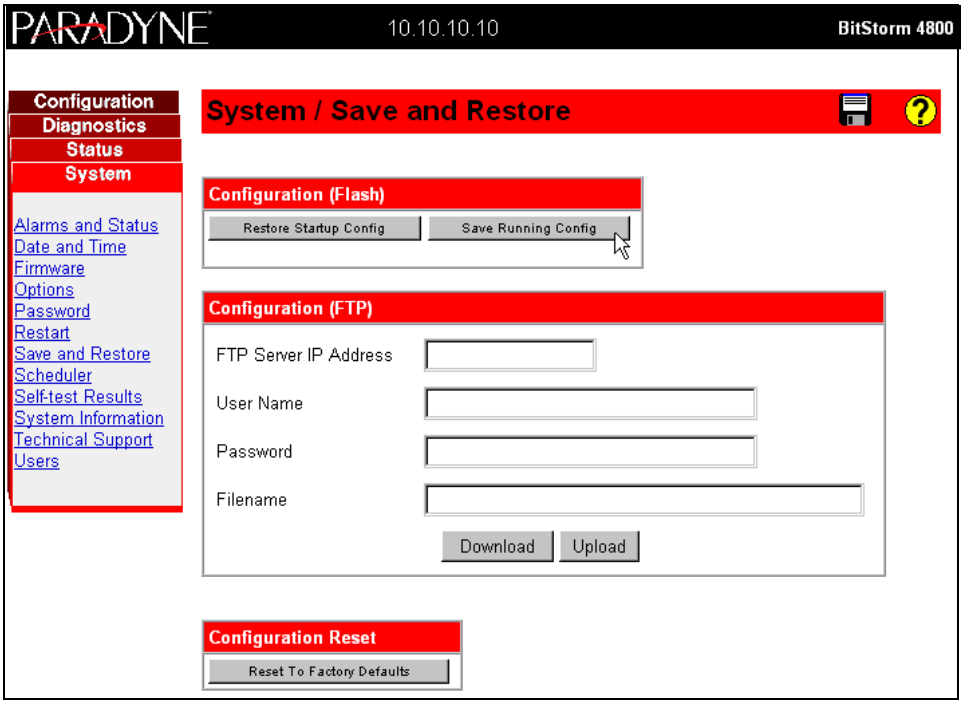
Click on Apply in each screen to save your selections to the running configuration.

Saving the Configuration

▶ Procedure

To save your configuration to non-volatile RAM:

1. Go to the System/Save and Restore screen.
2. Click on Save Running Config.



Logging Out

To end a session, close your Web browser. This prevents an unauthorized user from accessing the system using your user name and password.

Monitoring and Troubleshooting

5

Overview

The chapter describes ways to monitor the status of the BitStorm 4800, and to diagnose problems. These include:

System Log

The system log (syslog) contains messages of up to eight different levels of importance. From high to low, they are:

- **Emergency** – The system is unusable.
- **Alert** – Action must be taken immediately to prevent serious problems.
- **Critical** – Critical condition.
- **Error** – Error condition.
- **Warning** – Warning condition.
- **Notice** – Normal but noteworthy condition.
- **Informational** – Messages pertaining to command processing.
- **Debug** – Debug-level messages for developers.

The level of messages written to the log can be set using **configure syslog** command of the Command Line Interface, or the **Configuration/Syslog** screen of the Web interface. The levels are:

- **emergency** – Only emergency messages are logged.
- **alert** – Alert and emergency messages are logged.
- **informational** – Informational, notice, warning, error, critical, alert, and emergency messages are logged.
- **debug** – All messages are logged.

Viewing the System Log

You can view the system log using the **show syslog** command of the Command Line Interface, or the **Status/Syslog** screen of the Web interface.

Message Format

System log messages have the format:

Priority: *Month/Day*: *HH*:*MM*:*SS* : *Message*

For example:

ALERT Jun 5 00:14:59 Link Down on Port 2

Messages

The following are the system log messages of greatest importance.

Messages may be associated with SNMP traps. See Appendix B, *SNMP Traps*.

Table 5-1. System Log Messages (1 of 3)

Message	Priority	Meaning
Bootp Obtained Mgmt IP Address Address : Address=*address*, Mask=*mask*, Gateway=*address*	Alert	BOOTP obtained the displayed management IP address and gateway address.
Bootp Obtained Mgmt IP Address Address : Address=*address*, Mask=*mask*, Gateway=*address* replaced by Bootp Obtained Mgmt IP Address Address : Address=*address*, Mask=*mask*, Gateway=*address* ;	Alert	BOOTP replaced the management IP address and gateway address.
Bootp Obtained Mgmt IP Address Address : Address=*address*, Mask=*mask*, Gateway=*address* replaced by Statically Configured Mgmt IP Address Address : Address=*address*, Mask=*mask*, Gateway=*address*	Alert	An administrator has replaced the management IP address and gateway address obtained by BOOTP.
Cold Start Completed - System Operational.	Alert	The system has successfully started after a hardware reset.
DSL Port *p* Unit *u* Link Down.	Alert	The specified DSL interface is down.
DSL Port *p* Unit *u* Link Up.	Alert	The specified DSL interface has come up.
Fan *f* has Failed, unit at risk of overheating.	Alert	The specified fan (1–3) has failed. Notify your service representative.
Fan *f* is Restored.	Alert	The specified fan (1–3) has restarted.
Ftp Session Log : UserName : *user* UserAcct : *acct* Cmd Exec : *exec* Cmd Status : *status* Log On Time : *time* Log Off Time : *time* Ftp Server IP : *address*	Alert	An FTP session has occurred with the displayed characteristics.
GigE Down Link: Unit *u*: Link Down.	Alert	The specified GigE Downlink port has gone down.
GigE Down Link: Unit *u*: Link Up.	Alert	The specified GigE Downlink port has come up.

Table 5-1. System Log Messages (2 of 3)

Message	Priority	Meaning
GigE Up Link: Unit *u*: Link Down.	Alert	The specified GigE Uplink port has gone down.
GigE Up Link: Unit *u*: Link Up.	Alert	The specified GigE Uplink port has come up.
MAC Address and Physical Port Mismatch: Unauthorized User (*user*) on DSL port *u* by *access*.	Alert	The hardware address of the user on the specified port has changed, possibly signaling a security breach.
Management Port: Unit *u*: Link Down.	Alert	The MGMT port has gone down.
Management Port: Unit *u*: Link Up.	Alert	The MGMT port has come up.
Power On Self Test FAILED.	Alert	One or more of the hardware self-tests failed. If possible, use the **show system self-test** CLI command or the **System/Self-Test Results** Web interface screen to determine the area of failure. Notify your service representative.
Statically Configured Mgmt IP Address Address : Address=*address*, Mask=*mask*, Gateway=*address* replaced by Bootp Obtained Mgmt IP Address Address : Address=*address*, Mask=*mask*, Gateway=*address*	Alert	The manually set management IP address and gateway address have been replaced by those obtained from a BOOTP request.
Statically Configured Mgmt IP Address Address : Address=*address*, Mask=*mask*, Gateway=*address* replaced by Statically Configured Mgmt IP Address Address : Address=*address*, Mask=*mask*, Gateway=*address* ;	Alert	An administrator has replaced the displayed management IP address and gateway address.
Statically Configured Mgmt IP Address Address : Address=*address*, Mask=*mask*, Gateway=*address* ;	Alert	An administrator has set the displayed management IP address and gateway address.
System Fault communication with Subsystem *subsystem*.	Alert	A system fault occurred. Notify your service representative.
System Restored communication with Subsystem *subsystem*.	Alert	The system recovered from a system fault.
Temperature has fallen below 70 degrees Celsius.	Alert	The unit temperature, which had risen above 70° C, has fallen below that threshold.

Table 5-1. System Log Messages (3 of 3)

Message	Priority	Meaning
Temperature has risen above 70 degrees Celsius, unit at risk of Overheating.	Alert	The unit temperature has risen above 70° C. Shut down the unit as soon as possible, and notify your service representative.
Temperature has risen above 75 degrees Celsius, unit at risk of SHUTTING DOWN.	Emergency	The unit temperature has risen above 75° C. Shut down the unit as soon as possible, and notify your service representative.
Test Agent POST results from *subsystem* Failed.	Alert	The Power-On Self-Test of the specified subsystem failed. Notify your service representative.
Time Client unable to locate NTP Server.	Alert	The SNTP server is not responding, so the system date and time are not set and updated automatically.
V.35 Link: Unit *u*: Link Down.	Alert	The V.35/X.21 interface has gone down.
V.35 Link: Unit *u*: Link Up.	Alert	The V.35/X.21 interface has come up.
V.35 Loopback Test Activated. Duration is *n* seconds.	Alert	A test has been initiated on the V.35/X.21 port.
V.35 Loopback Test Terminated.	Alert	The test on the V.35/X.21 port was terminated.

Front Panel LEDs

If you have access to the unit, check the front panel LEDs. These are described in the *BitStorm 4800 Installation Guide*.

If an LED that should be lit during normal operation is not lit, verify that it is functional by using the **test leds** command of the Command Line Interface or the **Diagnostics/Test LEDs** screen of the Web interface.

Show Commands and Web Interface Status Screens

The **show** command of the Command Line Interface and various screens of the Web interface show the condition of the unit and its interfaces, including error statistics for the ports. The following table shows how to access the information.

Table 5-2. How to Locate Status Information

For Information About . . .	Use the CLI Command . . .	Use the Web Interface Screen . . .
Bridge	show bridge	Status/Bridge
Filters	show filter	Configuration/Filter
Filter Bindings	show filter-binding	Configuration/Binding
Filter Rules	show filter-rule	Configuration/Rule
Console Port	show interface console	Configuration/Console
DSL Ports	show interface dsl *port_id*	Status/DSL Port Statistics
Ethernet Ports	show interface ethernet *port_id*	Status/Ethernet Statistics
Modem Port	show interface modem	Configuration/Modem
V.35/X.21 Port	show interface v35	Status/V.35 Statistics
Management (IP)	show management ip	Configuration/Management/ Address
Management (IPsec)	show management ipsec	Configuration/IPsec
Management (SNMP)	show management snmp	Configuration/SNMP
Self-Test Results	show system selftest	System/Self-Test Results
Syslog	show syslog	Status/Syslog
System	show system status	Status/System Information
Users	show user-accounts	Status/Users

CLI Command Descriptions

A

CLI Commands

The BitStorm 4800 can be managed with text commands from the Command Line Interface (CLI). The CLI can be accessed:

- Locally via a PC or asynchronous terminal connected to the CONSOLE port.
- Remotely via a Telnet session.

The following conventions are used in descriptions of the commands:

Convention	Meaning
[ ]	A choice of optional parameters. Command parameters enclosed in neither brackets nor braces are required.
{ }	A choice of required parameters. Command parameters enclosed in neither brackets nor braces are required.
x | y	Mutually exclusive elements. Enter one element only (either x or y in this example).
[{ }]	A required choice within an optional element.
Helvetica Italic	A variable.
Courier Bold	A command and its keywords. It is necessary to type only as much of a command or keyword as is required to distinguish it from others. The CLI software automatically fills in the rest.
Underscore	If a keyword is underscored, it is the default value for the command.
x.x.x.x	IP address or subnet mask. Each *x* denotes a decimal value 0–255.
xx-xx-xx-xx-xx-xx	MAC address. Each *x* denotes a hexadecimal digit 0–f.

Commands are shown in this appendix in alphabetical order, regardless of function or access level required.

For general information about using the CLI, see Chapter 3, *Using the Command Line Interface*.

Back

The **back** command logically positions the CLI in the command structure.

Table A-1. Back Command

back
Minimum Access Level: **User**
The **back** command positions access up one level in the command tree. For example, if DSL interface 1/1 is being configured, the following prompt is displayed: **IAC(configure-interface-dsl-1/1)#** The back command returns the display to the **iac-configure-interface-dsl#** prompt. Example: IAC(configure-interface-dsl-1/1)#**back** IAC(configure-interface-dsl)#**back** IAC(configure-interface)#_

Clear

The **clear** command empties the specified object.

Table A-2. Clear Command

clear management snmp nms-address {*ip_address_1***}... [***ip_address_8***]**
Minimum Access Level: **Administrator**
The **clear management snmp nms-address** command clears the IP addresses of up to eight NMS management stations. ***ip_address_1... ip_address_8*** – Specifies one or more NMS addresses. Example: IAC#**clear management snmp nms-address 137.70.92.192**
clear management snmp nms-traps {*ip_address_1***}... [***ip_address_8***]**
Minimum Access Level: **Administrator**
The **clear management snmp nms-traps** command clears the IP addresses of up to eight NMS trap managers. ***ip_address_1... ip_address_8*** – Specifies one or more trap manager addresses. Example: IAC#**clear management snmp nms-traps 137.70.92.2**
clear syslog
Minimum Access Level: **Administrator**
The **clear syslog** command clears all entries in the system log. Example: IAC#**clear syslog**

Configure

The **configure** command causes the CLI to enter configuration mode, from which you can specify what element of the system you would like to configure.

Table A-3. Configure Command

configure
Minimum Access Level: **Administrator**
The **configure** command causes the CLI to enter configuration mode. Once the **IAC(configure)#** prompt is displayed, you can enter one of the configuration subcommands. Example: IAC#**configure** IAC(configure)#**interface** IAC(configure-interface)#**bridge** IAC(configure-interface-bridge)#**mode switch** IAC(configure-interface-bridge)#!**save** IAC(configure-interface-bridge)#

Configure Bridge

The **configure bridge** command configures the handling of the bridge table.

Table A-4. Configure Bridge Command

configure bridge clear
Minimum Access Level: **Administrator**
The **configure bridge clear** command deletes learned entries from the bridge table. Static entries are not affected. Example: IAC#**configure bridge clear**
configure bridge mode {mux | sms | switch | uplink-tag}
Minimum Access Level: **Administrator**
The **configure bridge mode** command specifies the mode the bridge will operate in. **mux** – Multiplexing forwarding mode. The system treats each DSL port as if it were a private network connected to the uplink, and never forwards data on another DSL port. **sms** – Subscriber Management System (SMS) mode. The system treats each DSL port as if it were a private network connected to the uplink, and never forwards data on another DSL port. In addition, a management Virtual Local Area Network (VLAN) is created on the uplink for use by the SMS. **switch** – Switched mode. The system acts as a transparent learning bridge. This is the default. **uplink-tag** – UpLink Tagging mode. All traffic from the DSL subscriber ports is given a unique VLAN tag. The system therefore treats each DSL port as if it were a private network connected to the uplink, and never forwards data on another DSL port. Example: IAC#**configure bridge mode mux**
configure bridge timeout {*time***}**
Minimum Access Level: **Administrator**
The **configure bridge timeout** command specifies the maximum amount of time a learned entry may exist in the bridge table without apearing as the source address of a received frame. ***time*** – The amount of time, in seconds, that an entry may exist. The valid range is 10–1000000 seconds, or 0 (zero, which specifies that no timeouts will occur). The default is 300. Example: IAC#**configure bridge timeout 0**

Configure Date

The **configure date** command sets the date, time, and time zone in the BitStorm 4800.

When it is first powered on, the unit attempts to obtain the date and time from an NTP server on the Internet. If it fails, the unit's date is set to January 1, 2001, and the time is set to 00:00:00.

Table A-5. Configure Date Command

configure date [*mm/dd/yy* **|** *dd/mm/yy***] [***hh:mm***]**
Minimum Access Level: **Administrator**
The **configure date** command sets the date and time. ***mm/dd/yy*** or ***dd/mm/yy*** – specifies the month, day, and year, each as two digits. The date format is set by the **configure system options** command (see Table A-18, Configure System Options Command); the default order is month, day, and year. ***hh:mm*** – Specifies the time in hours (0–23) and minutes (0–59). Example: `IAC#configure date 03/21/02 13:05`
configure date-timezone {*time_zone***}**
Minimum Access Level: **Administrator**

The **configure date-timezone** command specifies the time zone the date and time are relative to.
 	
time_zone – Specifies the offset in hours from Greenwich Mean Time (GMT) that the date and time represent. Hours before GMT are expressed as negative numbers and hours after GMT are expressed as positive numbers (with or without a plus sign). Half hours are supported as decimals. Valid values are –12 through 12.
 	
Offsets are listed in Table F-1, Time Zone Names, in Appendix F, *Reference Tables*. You can also obtain a list of time zone offsets using the command:
 	
`configure date-timezone ?`
 	
The unit does not adjust for Daylight Savings Time.
 	
Examples:
 	
`IAC#configure date-timezone +2`
`IAC#configure date-timezone 9`
`IAC#configure date-timezone -3.5`

Configure Factory

The **configure factory** command loads the factory default parameters into the running configuration. The default parameters take immediate effect, but are not saved. Execute the Save command to save the parameters to Non-Volatile Random-Access Memory (NVRAM).

Factory defaults include a management address of 10.10.10.10, so if you are managing the BitStorm 4800 using Telnet over a different address, your connection is terminated upon execution of the **configure factory** command. It is therefore recommended that this command be executed from the Console or Modem port.

Table A-6. Configure Factory Command

configure factory
Minimum Access Level: **Administrator**
The **configure factory** command loads factory default parameters. Example: IAC#**configure factory**

Configure Filter

Filters restrict select types of user data on a particular interface. There are three steps to implementing a filter in the BitStorm 4800:

- Define filter rules (see *Configure Filter-Rule* on page A-10)
- Define a named filter comprising one or more rules (see Table A-7, Configure Filter Command)
- Bind the filter to an interface (see *Configure Filter-Binding* on page A-9)

The **configure filter** command creates and deletes filters.

Table A-7. Configure Filter Command

`configure filter create` *filter_name* **`{forward | discard}`** **`[`***rule_name_1***`]... [`***rule_name_16***`]`**
Minimum Access Level: **Administrator**
The **configure filter create** command creates a filter based on existing filter rules. ***filter_name*** – Specifies the filter to be created. The name may contain up to 32 printable characters. **forward** – Specifies that a packet is to be forwarded to the user when none of the conditions specified in the rule or rules are matched. **discard** – Specifies that a packet is to be discarded when none of the conditions specified in the rule or rules are matched. ***rule_name_1*** through ***rule_name_16*** – Specifies up to 16 different rule names. These must be already defined using the **configure filter-rule** command (see Table A-9, Configure Filter-Rule Command). Example: `IAC#configure filter create no_at_or_ipx forward no_at no_ipx`
`configure filter delete` *filter_name*
Minimum Access Level: **Administrator**
The **configure filter delete** command deletes a filter. ***filter_name*** – Specifies the filter to be deleted. It must not be bound to an interface. To delete a binding, use the **configure filter-binding** command (see Table A-8, Configure Filter-Binding Command). Example: `IAC#configure filter delete no_decnet`

Configure Filter-Binding

The configure **filter-binding** command associates a filter with a particular port, or removes such an association.

Table A-8. Configure Filter-Binding Command

configure filter-binding create *filter_name* **{outbound | inbound | both}** *port_id*
Minimum Access Level: **Administrator**
The **configure filter-binding create** command associates a filter to a port. ***filter_name*** – Specifies the filter to be associated with a port. It must exist. (See *Configure Filter* on page A-8.) **outbound** – Specifies that traffic from the port is affected by the filter. **inbound** – Specifies that traffic to the port is affected by the filter. **both** – Specifies that traffic both to and from the port is affected by the filter. ***port_id*** – Specifies the DSL port whose traffic is to be filtered. Example: `IAC#configure filter-binding create no_at_or_ipx 1/1`
configure filter-binding delete *filter_name* **{outbound | inbound | both}** *port_id*
Minimum Access Level: **Administrator**
The **configure filter-binding delete** command removes the association of a filter to a port. ***filter_name*** – Specifies the filter whose association is to be deleted. The filter itself remains intact. **outbound** – Specifies that traffic from the port is affected by the filter whose binding is to be deleted. **inbound** – Specifies that traffic to the port is affected by the filter whose binding is to be deleted. **both** – Specifies that traffic both to and from the port is affected by the filter whose binding is to be deleted. ***port_id*** – Specifies the DSL port whose filter is to be deleted. Example: `IAC#configure filter-binding delete no_at_or_ipx 1/1`

Configure Filter-Rule

The configure **filter-rule** command creates and deletes rules for filtering traffic on the DSL ports.

Table A-9. Configure Filter-Rule Command

configure filter-rule create {*rule_name***}{forward|discard} {ether | ether-snap}[***ethertypes***]**
Minimum Access Level: **Administrator**

The **configure filter-rule create** command creates a rule for filtering traffic.
rule_name – The name of the rule to be created. The name may contain up to 32 printable characters.
forward – If a packet matches the rule it is forwarded.
discard – If a packet matches the rule it is discarded.
ether – Specifies that the rule applies to Layer 2 Ethernet traffic.
ether-snap – Specifies that the rule applies to Layer 2 SubNetwork Access Protocol (SNAP) traffic.
ethertypes – Specifies the Ethertype the rule is in effect for. Hexadecimal values and value ranges for Ethertypes as listed in RFC 1700 are valid. These Ethertypes are shown in Table F-2, Ethertypes, in Appendix F, *Reference Tables*.
Values in value ranges must be separated by a hyphen.
Examples:
`IAC#configure filter-rule create DecNetdrop discard ether 6003`
`IAC#configure filter-rule create IPXdrop discard ether 8137-8138`

configure filter-rule delete {*rule_name***}**
Minimum Access Level: **Administrator**
The **configure filter-rule delete** command deletes a rule for filtering traffic. ***rule_name*** – The name of the rule to be deleted. Example: `IAC#configure filter-rule delete IPXdrop`

Configure Interface

The **configure interface** command sets parameters for the Console, DSL, Ethernet, Modem, and V.35/X.21 interfaces.

Table A-10. Configure Interface Command (1 of 11)

configure interface console data-bits {7 | 8}
Minimum Access Level: **Administrator**
The **configure interface console data-bits** command sets the number of data bits in a byte on the Console port. **data-bits** – Valid choices are 7 and 8. The default is 8. Example: IAC#**configure interface console data-bits 7**
configure interface console parity {even | none | odd}
Minimum Access Level: **Administrator**
The **configure interface console parity** command sets the parity bit type for the Console port. **parity** – Valid choices are none, odd, and even. The default is none. Example: IAC#**configure interface console parity even**
configure interface console rate {1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200}
Minimum Access Level: **Administrator**
The **configure interface console rate** command sets the rate of the Console port in bps. **rate** – Valid rates are 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200. The default is 9600 bps. Example: IAC#**configure interface console rate 57600**
configure interface console show
Minimum Access Level: **Administrator**
The **configure interface console show** command displays parameters for the Console port without leaving configuration mode. Example: IAC#**configure interface console show**

Table A-10. Configure Interface Command (2 of 11)

configure interface console stop-bits {1 | 2}
Minimum Access Level: **Administrator**
The **configure interface console stop-bits** command sets the number of stop bits delimiting a byte on the Console port. **stop-bits** – Valid choices are 1 and 2. The default is 1. Example: IAC#**configure interface console stop-bits 1**
configure interface dsl {*port_id***} atm data-connection {***vpi/vci***}**
Minimum Access Level: **Administrator**
The **configure interface dsl atm data-connection** command specifies, by VPI/VCI, the virtual circuit used for data. ***port_id*** – Identifies the port to be configured. The possible forms of the identifier are described in *System Terminology* in Chapter 2, *Terminology and Conventions*. **atm data-connection** – Valid input is the VPI/VCI for the data connection. The default is 0/35. The valid range for VPI is 0–15. The valid range for VCI is 32–255. Examples: IAC#**configure interface dsl 1/1 atm data-connection 1/35**
configure interface dsl {*port_id***}** **atm encapsulation {llc-bridged | vcm-bridged}**
Minimum Access Level: **Administrator**
The **configure interface dsl atm encapsulation** command specifies whether the port uses Logical Link Control (LLC) or Virtual Channel Multiplexing (VCM) bridged encapsulation. ***port_id*** – Identifies the port to be configured. The possible forms of the identifier are described in *System Terminology* in Chapter 2, *Terminology and Conventions*. **atm encapsulation** – Valid choices are: – llc-bridged – The interface uses LLC bridged encapsulation. This is the default. – vcm-bridged – The interface uses VCM bridged encapsulation. Example: IAC#**configure interface dsl 1/1 atm encapsulation vcm-bridged**

Table A-10. Configure Interface Command (3 of 11)

configure interface dsl {*port_id***} behavior {adaptive | fixed}**
Minimum Access Level: **Administrator**
The **configure interface dsl behavior** command specifies whether the port will adapt its rate to line conditions. ***port_id*** – Identifies the port to be configured. The possible forms of the identifier are described in *System Terminology* in Chapter 2, *Terminology and Conventions*. **behavior** – Valid choices are: – adaptive – The rate automatically adapts to line conditions at startup. This is the default. – fixed – Only one rate is allowed downstream or upstream, defined by max-downstream-speed and max-upstream-speed. Example: IAC#**configure interface dsl 1/48 behavior fixed**
configure interface dsl {*port_id***} latency {fast | interleaved}**
Minimum Access Level: **Administrator**
The **configure interface dsl latency** command specifies whether an interleave buffer is used. ***port_id*** – Identifies the port to be configured. The possible forms of the identifier are described in *System Terminology* in Chapter 2, *Terminology and Conventions*. **latency** – Valid choices are: – fast – No interleave buffer is used. This is the default. – interleaved – This port uses an interleave buffer. Example: IAC#**configure interface dsl 1/24 latency interleaved**
configure interface dsl {*port_id***} line-code {ansi | dmt | g.lite | multimode}**
Minimum Access Level: **Administrator**
The **configure interface dsl line-code** command specifies the line code for a DSL port. ***port_id*** – Identifies the port to be configured. The possible forms of the identifier are described in *System Terminology* in Chapter 2, *Terminology and Conventions*. **line-code** – Valid choices are: – ansi – The port uses ANSI T1.413-1998. – dmt – The port uses G.dmt (G.992.1). – g.lite – The port uses G.lite (G.992.2). – multimode – The port automatically senses the line code in accordance with G.994.1. This is the default. Example: IAC#**configure interface dsl 1/24 line-code ansi**

Table A-10. Configure Interface Command (4 of 11)

configure interface dsl {*port_id***} linkupdown-trap {disabled | enabled}**
Minimum Access Level: **Administrator**
The **configure interface dsl linkupdown-trap** command specifies whether an SNMP trap should be sent upon link up and link down events. ***port_id*** – Identifies the port to be configured. The possible forms of the identifier are described in *System Terminology* in Chapter 2, *Terminology and Conventions*. **linkupdown-trap** – Valid choices are: – disabled – No traps are sent upon link up and link down events. – enabled – A trap is sent upon a link up or link down event. This is the default. Example: `IAC#configure interface dsl 1/1 linkupdown-trap disabled`
configure interface dsl {*port_id***} max-downstream-speed {***rate***}**
Minimum Access Level: **Administrator**
The **configure interface dsl max-downstream-speed** command specifies the maximum rate, in Kbps, available for traffic from the port toward the CPE. If behavior is set to fixed, this is the only downstream rate. ***port_id*** – Identifies the port to be configured. The possible forms of the identifier are described in *System Terminology* in Chapter 2, *Terminology and Conventions*. ***rate*** – Valid rates are: – For dmt and ansi: 64 to 8128 Kbps in 32 Kbps increments. The default is 8128. – For g.lite: 64 to 4000 Kbps in 32 Kbps increments. The default is 4000. Example: `IAC#configure interface dsl 1/2 max-downstream-speed 512`
configure interface dsl {*port_id***} max-upstream-speed {***rate***}**
Minimum Access Level: **Administrator**
The **configure interface dsl max-upstream-speed** command specifies the maximum rate, in Kbps, available for traffic toward the port from the CPE. If behavior is set to fixed, this is the only upstream rate. ***port_id*** – Identifies the port to be configured. The possible forms of the identifier are described in *System Terminology* in Chapter 2, *Terminology and Conventions*. ***rate*** – Valid rates are 32 to 1024 Kbps in 32 Kbps increments. The default is 1024. Example: `IAC#configure interface dsl 1/1 max-upstream-speed 128`

Table A-10. Configure Interface Command (5 of 11)

configure interface dsl {*port_id***} min-downstream-speed {***rate***}**
Minimum Access Level: **Administrator**
The **configure interface dsl min-downstream-speed** command specifies the minimum rate, in Kbps, to adapt to for traffic from the port toward the CPE. ***port_id*** – Identifies the port to be configured. The possible forms of the identifier are described in *System Terminology* in Chapter 2, *Terminology and Conventions*. **min-downstream-speed** – Valid rates are: – For dmt and ansi: 64 to 8128 Kbps in 32 Kbps increments. The default is 128. – For g.lite: 64 to 4000 Kbps in 32 Kbps increments. The default is 128. Example: IAC#**configure interface dsl 1/2 min-downstream-speed 96**
configure interface dsl {*port_id***} min-snr-margin {***margin***}**
Minimum Access Level: **Administrator**
The **configure interface dsl min-snr-margin** command specifies the minimum SNR margin, in dB, required for the port. See *SNR Margin (DSL Interfaces)* on page A-22 for more information. ***port_id*** – Identifies the port to be configured. The possible forms of the identifier are described in *System Terminology* in Chapter 2, *Terminology and Conventions*. ***margin*** – Valid choices are 0–15 dB in 1 dB increments. The default is 0. Examples: IAC#**configure interface dsl 1/1 min-snr-margin 9**
configure interface dsl {*port_id***} min-upstream-speed {***rate***}**
Minimum Access Level: **Administrator**
The **configure interface dsl min-upstream-speed** command specifies the minimum rate, in Kbps, to adapt to for traffic toward the port from the CPE. ***port_id*** – Identifies the port to be configured. The possible forms of the identifier are described in *System Terminology* in Chapter 2, *Terminology and Conventions*. ***rate*** – Valid rates are 32 to 1024 Kbps in 32 Kbps increments. The default is 64. Example: IAC#**configure interface dsl 1/2 min-upstream-speed 64**
configure interface dsl {*port_id***} name {***port_name***}**
Minimum Access Level: **Administrator**
The **configure interface dsl name** command specifies a unique name for this port. ***port_id*** – Identifies the port to be configured. The possible forms of the identifier are described in *System Terminology* in Chapter 2, *Terminology and Conventions*. **name** – May be up to 16 printable characters. The name may not include a forward slash (/) or the following keywords: all, dhcp, downlink, mgmt, uplink, or v35. Example: **IAC#configure interface dsl 1/1 name Room_100**

Table A-10. Configure Interface Command (6 of 11)

configure interface dsl [*port_id***] show**
Minimum Access Level: **Administrator**
The **configure interface dsl show** command displays parameters for a DSL port without leaving configuration mode. ***port_id*** – Identifies the port whose configuration is to be displayed. If no port is specified, the port currently in configuration mode, if any, is displayed. Examples: IAC#**configure interface dsl 1/7 show** IAC(configure-interface-dsl-1/7)#**show**
configure interface dsl {*port_id***} state {disabled | enabled}**
Minimum Access Level: **Administrator**
The **configure interface dsl state** command specifies the availability of a DSL port. ***port_id*** – Identifies the port to be configured. The possible forms of the identifier are described in *System Terminology* in Chapter 2, *Terminology and Conventions*. **state** – Specifies the availability of the port. Valid choices are disabled and enabled. The default is enabled. Example: IAC#**configure interface dsl 1/24 state enabled**
configure interface dsl {*port_id***} target-downstream-margin {***margin***}**
Minimum Access Level: **Administrator**
The **configure interface dsl target-downstream-margin** command specifies the Signal to Noise Ratio (SNR) margin, in dB, required at startup for traffic from the port toward the CPE. See *SNR Margin (DSL Interfaces)* on page A-22 for more information. ***port_id*** – Identifies the port to be configured. The possible forms of the identifier are described in *System Terminology* in Chapter 2, *Terminology and Conventions*. ***margin*** – Valid choices are 2–15 dB in 1 dB increments. The default is 6. Example: IAC#**configure interface dsl 1/1 target-downstream-margin 3**
configure interface dsl {*port_id***} target-upstream-margin {***margin***}**
Minimum Access Level: **Administrator**
The **configure interface dsl target-upstream-margin** command specifies the SNR margin, in dB, required at startup for traffic toward the port from the CPE. See *SNR Margin (DSL Interfaces)* on page A-22 for more information. ***port_id*** – Identifies the port to be configured. The possible forms of the identifier are described in *System Terminology* in Chapter 2, *Terminology and Conventions*. ***margin*** – Valid choices are 2–15 dB in 1 dB increments. The default is 6. Example: IAC#**configure interface dsl 1/1 target-upstream-margin 3**

Table A-10. Configure Interface Command (7 of 11)

configure interface ethernet {*port_id***}** **connector {rj45 | fiber}**
Minimum Access Level: **Administrator**
The **configure interface ethernet connector** command specifies the physical interface to be used when both interfaces are active at the same time. Ordinarily the BitStorm 4800 uses the fiber optic port if an SFP transceiver is detected, so this command provides a way to force the use of the 8-position modular jack even if a transceiver is installed. ***port_id*** – Identifies the Ethernet port to be configured. The possible forms of the identifier are described in *Ethernet Port ID* in Chapter 2, *Terminology and Conventions*. **connector** – Valid choices are: – rj45 – The BitStorm 4800 uses the 8-position modular jack for the *port_id* interface. – fiber – The BitStorm 4800 uses the fiber optic port for the *port_id* interface. Example: IAC#**configure interface ethernet 1/uplink connector rj45**
configure interface ethernet {*port_id***}** **flow-control {enabled | disabled}**
Minimum Access Level: **Administrator**
The **configure interface ethernet flow-control** command specifies whether flow control should be used on the port. ***port_id*** – Identifies the Ethernet port to be configured. The possible forms of the identifier are described in *Ethernet Port ID* in Chapter 2, *Terminology and Conventions*. **flow-control** – Valid choices are disabled and enabled. The default is enabled. Example: IAC#**configure interface ethernet 1/mgmt flow-control enabled**
configure interface ethernet {*port_id***}** **mode {auto | manual}**
Minimum Access Level: **Administrator**
The **configure interface ethernet mode** command specifies whether the duplex mode and rate are automatically set, and the crossover type automatically sensed. ***port_id*** – Identifies the Ethernet port to be configured. The possible forms of the identifier are described in *Ethernet Port ID* in Chapter 2, *Terminology and Conventions*. **mode** – Valid choices are: – auto – The BitStorm 4800 automatically senses the rate and duplex mode. This is the default. – manual – The administrator must set the rate and duplex mode. Example: IAC#**configure interface ethernet 1/mgmt mode manual**

Table A-10. Configure Interface Command (8 of 11)

configure interface ethernet {*port_id*} rate {10full | 10half | 100full | 100half | 1000full | 1000half}
Minimum Access Level: **Administrator**
The **configure interface ethernet rate** command specifies the duplex mode and rate if mode is set to manual. ***port_id*** – Identifies the Ethernet port to be configured. The possible forms of the identifier are described in *Ethernet Port ID* in Chapter 2, *Terminology and Conventions*. **rate** – Valid choices are: – 10full – 10 Mbps and full duplex – 10half – 10 Mbps and half duplex – 100full – 100 Mbps and full duplex – 100half – 100 Mbps and half duplex – 1000full – 1000 Mbps and full duplex – 1000half – 1000 Mbps and half duplex Example: **IAC#configure interface ethernet 1/mgmt rate 100full**
configure interface ethernet [*port_id*] show
Minimum Access Level: **Administrator**
The **configure interface ethernet show** command displays parameters for an Ethernet port without leaving configuration mode. ***port_id*** – Identifies the port whose configuration is to be displayed. If no port is specified, the port currently in configuration mode, if any, is displayed. Examples: IAC(configure-interface-ethernet-1/uplink)#**show** IAC#**configure interface ethernet 1/uplink show**
configure interface ethernet {*port_id*} xover {mdi | mdix}
Minimum Access Level: **Administrator**
The **configure interface ethernet xover** command specifies the crossover type when mode is set to manual. ***port_id*** – Identifies the Ethernet port to be configured. The possible forms of the identifier are described in *Ethernet Port ID* in Chapter 2, *Terminology and Conventions*. **xover** – Valid choices are: – mdi – The port is connected to a Network Interface Card (NIC). – mdix – The port is connected to a hub. Example: IAC#**configure interface ethernet 1/mgmt xover mdi**

Table A-10. Configure Interface Command (9 of 11)

configure interface modem data-bits {7 | 8}
Minimum Access Level: **Administrator**
The **configure interface modem data-bits** command sets the number of data bits in a byte on the Modem port. **data-bits** – Valid choices are 7 and 8. The default is 8. Example: IAC#**configure interface modem data-bits 7**
configure interface modem parity {even | none | odd}
Minimum Access Level: **Administrator**
The **configure interface modem parity** command sets the parity bit type for the Modem port. **parity** – Valid choices are none, odd, and even. The default is none. Example: IAC#**configure interface modem parity even**
configure interface modem rate {1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200}
Minimum Access Level: **Administrator**
The **configure interface modem rate** command sets the rate of the Modem port in bps. **rate** – Valid rates are 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200. The default is 9600 bps. Example: IAC#**configure interface modem rate 57600**
configure interface modem show
Minimum Access Level: **Administrator**
The **configure interface modem show** command displays parameters for the Modem port without leaving configuration mode. Example: IAC#**configure interface modem show**
configure interface modem stop-bits {1 | 2}
Minimum Access Level: **Administrator**
The **configure interface modem** command sets the number of stop bits delimiting a byte on the Modem port. **stop-bits** – Valid choices are 1 and 2. The default is 1. Example: IAC#**configure interface modem stop-bits 1**

Table A-10. Configure Interface Command (10 of 11)

configure interface v35 clock-source {external | internal}
Minimum Access Level: **Administrator**
The **configure interface v35 clock-source** command specifies the source of clocking for the V.35/X.21 interface on a 4804 Management Module. **clock-source** – Valid choices are external and internal. The default is external. If interface-type is set to x21 (X.21), the only valid option is internal. Example: IAC#**configure interface v35 clock-source internal**
configure interface v35 flow-control {cts | dsr | none}
Minimum Access Level: **Administrator**
The **configure interface v35 flow-control** command determines what lead, if any, is used for flow control. **flow-control** – Valid choices are: – cts – The CTS lead is monitored for flow control. – dsr - The DSR lead is monitored for flow control. – none - No hardware flow control is used. This is the default. Example: IAC#**configure interface v35 flow-control dsr**
configure interface v35 idle-char {flag | mark}
Minimum Access Level: **Administrator**
The **configure interface v35 idle-char** command specifies whether the port should transmit the flag character (hexadecimal 7E) or all ones (hexadecimal FF) between frames on the V.35/X.21 interface on a 4804 Management Module. **flag** – Valid choices are flag and mark. The default is flag. Example: IAC#**configure interface v35 idle-char mark**
configure interface v35 invert-tx-clock {disabled | enabled}
Minimum Access Level: **Administrator**
The **configure interface v35 invert-tx-clock** command specifies whether the clock supplied by the 4804 Management Module V.35/X.21 port on the TXC interchange circuit DB (ITU/T 114) is phase inverted with respect to the Transmitted Data interchange circuit BA (ITU/T 103). **invert-tx-clock** – Invert Transmit Clock. Valid choices are disabled and enabled. The default is disabled. Example: IAC#**configure interface v35 invert-tx-clock enabled**

Table A-10. Configure Interface Command (11 of 11)

configure interface v35 rate {*rate*}
Minimum Access Level: **Administrator**
The **configure interface v35 rate** command specifies the port rate in Kbps for the V.35/X.21 interface on a 4804 Management Module. This value is ignored if clock-source is external. **rate** – Valid rates are 64 to 8192 Kbps in 64 Kbps increments. The default is 2048. Example: IAC#**configure interface v35 rate 1536**
configure interface v35 show
Minimum Access Level: **Administrator**
The **configure interface v35 show** command displays parameters for the V.35/X.21 port without leaving configuration mode. Example: IAC#**configure interface v35 show**
configure interface v35 state {disabled | enabled}
Minimum Access Level: **Administrator**
The **configure interface v35 state** command specifies the availability of the V.35/X.21 interface on a 4804 Management Module. **state** – Valid choices are disabled and enabled. The default is enabled. Example: IAC#**configure interface v35 state disabled**
configure interface v35 type {eia530a | v35 | x21}
Minimum Access Level: **Administrator**
The **configure interface v35 type** command specifies the electrical interface used for the V.35/X.21 port on a 4804 Management Module. **type** – Valid choices are: – eia530a – The interface is EIA-530-A. – v35 – The interface is V.35. This is the default. – x21 – The interface is X.21. Example: IAC#**configure interface v35 type v35**

SNR Margin (DSL Interfaces)

SNR (Signal-to-Noise Ratio) is the amplitude of the desired signal compared to the amplitude of noise on the line. Margin is the amount of noise that can be tolerated before a communication error or link establishment failure occurs. There are three settings in the BitStorm 4800 related to SNR margin:

- min-snr-margin
- target-downstream-margin
- target-upstream-margin

If behavior is set to adaptive, the target-downstream-margin and target-upstream-margin settings determine the highest rates the modems can train to. These rates may be less than the maximum configured rates.

For example, if target-downstream-margin is set to 6, the modems will train (establish communication) at the highest rate downstream at which there is at least 6 dB of margin, or, if it is lower, the maximum configured rate (max-downstream-speed, in this case).

If behavior is set to fixed, the target margins determine the acceptability of the signal at the selected fixed rate. If the margin is lower than the target margin at that rate, the modems train again.

The min-snr-margin setting is for the upstream direction only. It causes the modem to retrain if the margin falls and remains below the setting for 60 seconds.

Configure IP

The **configure IP** command is used to specify IP parameters.

Table A-11. Configure IP Command

configure ip nhr {*ip_address***}**
Minimum Access Level: **Administrator**
The **configure ip nhr** command determines the Next-Hop Router (NHR) address for all ports in the system. ***ip_address*** – Specifies the IP address of the next-hop router. Example: IAC#**configure ip nhr 135.75.90.112**

Configure Management

The **configure management** command sets parameters for remote management of the BitStorm 4800.

Table A-12. Configure Management Command (1 of 9)

configure management address {bootp | {{*ip_address***} {***subnet_mask***} {***default_gateway***}}}**
Minimum Access Level: **Administrator**
The **configure management address** command specifies the IP address of the BitStorm 4800, or specifies that it will be assigned using BOOTP (Bootstrap Protocol). **bootp** – Specifies that a BOOTP server will determine the management IP address. Management addresses are cleared in anticipation of a BOOTP response. ***ip_address*** – Specifies the management IP address. The default address is 10.10.10.10. ***subnet_mask*** – Specifies the subnet mask to be applied to the IP address. The default mask is 255.255.255.0. ***default_gateway*** – Specifies the management next hop or gateway IP address. The default gateway is 10.10.10.254. Examples: IAC#**configure management address bootp** IAC#**configure management address 137.90.127.3 255.255.255.0 137.90.127.1**
configure management ipsec {disable | enable}
Minimum Access Level: **Administrator**
The **configure management ipsec** command determines whether management traffic is subject to IPsec. **disable** – Specifies that IPsec is not used. IPsec parameters may be set while in this state, but they have no effect until IPsec is enabled. This is the default. **enable** – Specifies that IPsec is used to implement a Virtual Private Network (VPN). Example: IAC#**configure management ipsec enable**

Table A-12. Configure Management Command (2 of 9)

configure management ipsec connection create {*connection_name***} {***remote_tunnel_address***} {***remote_host_address***}**
Minimum Access Level: **Administrator**
The **configure management ipsec connection create** command creates a new IPsec profile. ***connection_name*** – Specifies the name of the connection policy to be created. It may be from 1–16 printable characters. ***remote_tunnel_address*** – Specifies the IP address of the remote end of the IPsec tunnel. ***remote_host_address*** – Specifies the IP address of the remote host using the tunnel. Example: IAC#**configure management ipsec connection create sec2 135.90.200.200 10.10.2.2**
configure management ipsec connection default ah-alg {sha1 | md5}
Minimum Access Level: **Administrator**
The **configure management ipsec connection default ah-alg** command sets the default Authentication Header protocol algorithm. **sha1** – Specifies that the default is the Secure Hash Algorithm. **md5** – Specifies that the default is the Message Digest 5 algorithm. Example: IAC#**configure management ipsec connection default ah-alg md5**
configure management ipsec connection default ah-md5-key {*ahmd5key_string***}**
Minimum Access Level: **Administrator**
The **configure management ipsec connection default ah-md5-key** command sets the default initial key for the Authentication Header Message Digest 5 algorithm. ***ahmd5key_string*** – Defines the default key. This is a string of up to 32 hexadecimal digits (0–f). The default is 21aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa. Example: IAC#**configure management ipsec connection default ah-md5-key d2e4d3c1**

Table A-12. Configure Management Command (3 of 9)

configure management ipsec connection default ah-sha1-key {*ahsha1_string***}**
Minimum Access Level: **Administrator**
The **configure management ipsec connection default ah-sha1-key** command sets the default initial key for the Authentication Header Secure Hash Algorithm. ***ahsha1_string*** – Defines the default key. This is a string of up to 40 hexadecimal digits (0–f). The default is 21aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa. Example: IAC#**configure management ipsec connection default ah-sha1-key d2e4d3c1**
configure management ipsec connection default des-key {*deskey_string***}**
Minimum Access Level: **Administrator**
The **configure management ipsec connection default des-key** command sets the default initial key for the Data Encryption Standard algorithm. ***deskey_string*** – Defines the default key. This is a string of up to 16 hexadecimal digits (0–f). The default is 21aaaaaaaaaaaaaa. Example: IAC#**configure management ipsec connection default des-key d2e4d3c1**
configure management ipsec connection default encryption {des | null}
Minimum Access Level: **Administrator**
The **configure management ipsec connection default encryption** command sets the default encryption algorithm. **des** – Specifies that the default is the Data Encryption Standard (DES) algorithm. **null** – Specifies that the default is no encryption. Example: IAC#**configure management ipsec connection default encryption des**
configure management ipsec connection default esp-alg {sha1 | md5}
Minimum Access Level: **Administrator**
The **configure management ipsec connection default esp-alg** command sets the default Encapsulating Security Payload protocol algorithm. **sha1** – Specifies that the default is the Secure Hash Algorithm. **md5** – Specifies that the default is the Message Digest 5 algorithm. Example: IAC#**configure management ipsec connection default esp-alg md5**

Table A-12. Configure Management Command (4 of 9)

configure management ipsec connection default esp-md5-key {*espmd5key_string***}**
Minimum Access Level: **Administrator**
The **configure management ipsec connection default esp-md5-key** command sets the default initial key for the Encapsulating Security Payload protocol Message Digest 5 algorithm. ***espmd5key_string*** – Defines the default key. This is a string of up to 32 hexadecimal digits (0–f). The default is 21aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa. Example: IAC#**configure management ipsec connection default both esp-md5-key d2e4d3c1**
configure management ipsec connection default esp-sha1-key {*espsha1_string***}**
Minimum Access Level: **Administrator**
The **configure management ipsec connection default esp-sha1-key** command sets the default initial key for the Encapsulating Security Payload protocol Secure Hash Algorithm. ***espsha1_string*** – Defines the default key. This is a string of up to 40 hexadecimal digits (0–f). The default is 21aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa. Example: IAC#**configure management ipsec connection default esp-sha1-key d2e4d3c1**
configure management ipsec connection delete {*connection_name***}**
Minimum Access Level: **Administrator**
The **configure management ipsec connection delete** command deletes an IPsec profile. ***connection_name*** – Specifies the name of the connection policy to be deleted. Example: IAC#**configure management ipsec connection delete sec2**
configure management ipsec connection modify {*connection_name***} algorithm {sha1 | md5}**
Minimum Access Level: **Administrator**
The **configure management ipsec connection modify algorithm** command sets the algorithm for a specified connection. ***connection_name*** – Specifies the name of the connection policy to modify. **sha1** – Specifies that the default is the Secure Hash Algorithm. **md5** – Specifies that the default is the Message Digest 5 algorithm. Example: IAC#**configure management ipsec connection modify sec1 algorithm md5**

Table A-12. Configure Management Command (5 of 9)

configure management ipsec connection modify {*connection_name***} authorization-key {***key_string***}**
Minimum Access Level: **Administrator**
The **configure management ipsec connection modify authorization-key** command sets the key for a specified connection. ***connection_name*** – Specifies the name of the connection policy to modify. ***key_string*** – Defines the key. This is a string of up to 40 hexadecimal digits (0–f). Example: IAC#**configure management ipsec connection modify sec1 authorization-key d2e4d3c1**
configure management ipsec connection modify {*connection_name***} antireplay {disable | enable}**
Minimum Access Level: **Administrator**
The **configure management ipsec connection modify antireplay** command determines whether the anti-replay feature is used. ***connection_name*** – Specifies the name of the connection policy to modify. **disable** – Specifies that anti-replay is not in effect. **enable** – Specifies that anti-replay is in effect. Example: IAC#**configure management ipsec connection modify sec1 antireplay enable**
configure management ipsec connection modify {*connection_name***} encryption {des | null}**
Minimum Access Level: **Administrator**
The **configure management ipsec connection modify encryption** command sets the encryption standard for a specified connection. ***connection_name*** – Specifies the name of the connection policy to modify. **des** – Specifies that the encryption standard is the Data Encryption Standard. **null** – Specifies that no encryption is used. Example: IAC#**configure management ipsec connection modify sec1 encryption des**

Table A-12. Configure Management Command (6 of 9)

configure management ipsec connection modify {*connection_name***} encryption-key {***key_string***}**
Minimum Access Level: **Administrator**
The **configure management ipsec connection modify encryption-key** command sets the encryption key for a specified connection. ***connection_name*** – Specifies the name of the connection policy to modify. ***key_string*** – Defines the key. This is a string of up to 16 hexadecimal digits (0–f). Example: IAC#**configure management ipsec connection modify sec2 encryption-key d2e4d3c1**
configure management ipsec connection modify {*connection_name***} protocol {ah | esp}**
Minimum Access Level: **Administrator**
The **configure management ipsec connection modify protocol** command sets the IPsec encryption protcol for a specified connection. ***connection_name*** – Specifies the name of the connection policy to modify. **ah** – Specifies that the protocol is Authentication Header. **esp** – Specifies that the protocol is Encapsulating Security Payload. Example: IAC#**configure management ipsec connection modify sec2 protocol ah**
configure management ipsec connection modify {*connection_name***} remote-host-address {***remote_host***}**
Minimum Access Level: **Administrator**
The **configure management ipsec connection modify remote-host-address** command changes the IP address of the remote host using the IPsec tunnel for a specified connection. ***connection_name*** – Specifies the name of the connection policy to modify. ***remote_host*** – Specifies the IP address of the remote host. It does not need to be routable. It may be a single IP address or two IP addresses separated by a hyphen denoting a range of IP addresses. Examples: IAC#**configure management ipsec connection modify sec1 remote-host-address 135.90.27.2** IAC#**configure management ipsec connection modify sec2 remote-host-address 135.90.27.2-135.90.27.23**

Table A-12. Configure Management Command (7 of 9)

configure management ipsec connection modify {*connection_name***} remote-tunnel-address {***remote_host***}**
Minimum Access Level: **Administrator**
The **configure management ipsec connection modify remote-tunnel-address** command changes the routable IP address of the IPsec tunnel at the remote end for a specified connection. ***connection_name*** – Specifies the name of the connection policy to modify. ***remote_host*** – Specifies the routable IP address of the IPsec tunnel at the remote end. Example: IAC#**configure management ipsec connection modify sec1 remote-tunnel-address 135.90.27.3**
configure management ipsec connection modify {*connection_name***} spi {***spi***} [in | out | both]**
Minimum Access Level: **Administrator**
The **configure management ipsec connection modify spi** command sets the Security Profile Index for the Encapsulating Security Payload protocol for a specified connection. ***connection_name*** – Specifies the name of the connection policy to modify. ***spi*** – The SPI number (1–65535). **in** – The SPI is assigned to the inbound connection. **out** – The SPI is assigned to the outbound connection. **both** – The SPI is assigned to both the inbound and outbound connections. This is the default. Example: IAC#**configure management ipsec connection modify sec2 spi 27**
configure management ipsec local-tunnel-address {*local_tunnel_address***}**
Minimum Access Level: **Administrator**
The **configure management ipsec local-tunnel-address** command defines the IP address of the near end of the IPsec tunnel. ***local_tunnel_address*** – Specifies the IP address of the near end of the IPsec tunnel. Example: IAC#**configure management ipsec local-tunnel-address 10.10.10.12**

Table A-12. Configure Management Command (8 of 9)

configure management snmp access-validation {disabled | enabled}
Minimum Access Level: **Administrator**
The **configure management snmp access-validation** command specifies whether the BitStorm 4800 validates the IP address of incoming SNMP (Simple Network Management Protocol) messages. **disabled** – No access validation occurs. This is the default. **enabled** – If the IP address of an SNMP packet is not one of those specified using the **configure management snmp nms-address** command, the packet is discarded. Example: IAC#**configure management snmp access-validation enabled**
configure management snmp nms-address {*nms_address1***}... [***nms_address8***]**
Minimum Access Level: **Administrator**
The **configure management snmp nms-address** command specifies the IP addresses of up to eight NMS (Network Management System) workstations allowed to access the BitStorm 4800. If SNMP Access Validation is disabled, these addresses have no effect. ***nms_address1*... *nms_address8*** – Specifies one to eight IP addresses of NMS workstations. Example: IAC#**configure management snmp nms-address 135.76.90.90 135.76.91.1**
configure management snmp nms-traps {*traps_address1***}... [***traps_address8***]**
Minimum Access Level: **Administrator**
The **configure management snmp nms-traps** command specifies the IP addresses of up to eight trap managers to which traps are sent. ***traps_address1*... *traps_address8*** – Specifies one to eight IP addresses of traps managers. Example: IAC#**configure management snmp nms-traps 135.76.90.90 135.76.91.1**
configure management snmp private-string {*private_community_string***}**
Minimum Access Level: **Administrator**
The **configure management snmp private-string** command specifies the community string for read-write access. ***private_community_string*** – Specifies the string used for read-write access. It may be up to 64 printable characters. The default is public. Example: IAC#**configure management snmp private-string topsecret**

Table A-12. Configure Management Command (9 of 9)

configure management snmp public-string {*public_community_string***}**
Minimum Access Level: **Administrator**
The **configure management snmp public-string** command specifies the community string for read-only access. ***public_community_string*** – Specifies the string used for read-only access. It may be up to 64 printable characters. The default is public. Example: IAC#**configure management snmp public-string mediumsecret**
configure management snmp state {disabled | enabled}
Minimum Access Level: **Administrator**
The **configure management snmp state** command specifies the availability of the SNMP agent. **state** – Valid choices are disabled and enabled. The default is disabled. Example: IAC#**configure management snmp state disabled**
configure management vlan {*vlan_tag***}**
Minimum Access Level: **Administrator**
The **configure management vlan** command specifies a VLAN tag to be added to management traffic. VLAN tagging is enabled only if the Bridge Mode is sms or uplink-tag. See *Configure Bridge* on page A-5. ***vlan_tag*** – Specifies the value of the VLAN tag. Valid values are 1–15. Example: IAC#**configure management vlan 12**

Configure Scheduler

The **configure scheduler** command sets parameters for automatic backup.

Table A-13. Configure Scheduler Command (1 of 2)

configure scheduler {disabled | enabled}
Minimum Access Level: **Administrator**
The **configure scheduler** command determines whether automatic configuration backup occurs. **disabled** – Specifies automatic configuration backup will not occur. This is the default. **enabled** – Specifies that automatic configuration backup will occur. Example: IAC#**configure scheduler enabled**
configure scheduler dynamic [*hh:mm***]**
Minimum Access Level: **Administrator**
The **configure scheduler dynamic** command specifies that automatic configuration backup will occur after each configuration change. ***hh:mm*** – Specifies the amount of time after a configuration change that a configuration backup will automatically occur. Time is specified in hours (1–24) and minutes (0-59) separated by a colon. The default and minimum is 00:30 (30 minutes). Example: IAC#**configure scheduler dynamic 24:00**
configure scheduler fixed {daily | monday | tuesday | wednesday | thursday | friday | saturday | sunday} {*hh:mm***}**
Minimum Access Level: **Administrator**
The **configure scheduler fixed** command specifies the fixed times at which configuration backups will occur. ***day_of_week*** – Specifies the day of the week backups will occur. If daily is selected, a backup occurs every day. ***hh:mm*** – Specifies the time of day the backup will occur. Time is specified in hours (1–23) and minutes (0–59) separated by a colon. Example: IAC#**configure scheduler sunday 00:00**

Table A-13. Configure Scheduler Command (2 of 2)

configure scheduler ftp {*ip_address***} {***user_name***} {***password***} {***filename***}**
Minimum Access Level: **Administrator**
The **configure scheduler ftp** command defines the FTP (File Transfer Protocol) server used for automatic configuration backup. ***ip_address*** – Specifies the network address of the FTP server. ***user_name*** – Specifies a user name accepted by the FTP server. ***password*** – Specifies the password associated with the user name. ***filename*** – Specifies the file containing the configuration backup. Example: IAC#**configure scheduler ftp 135.27.90.98 admin admnpass iac2_bkup**
configure scheduler ftp timestamp {append | none}
Minimum Access Level: **Administrator**
The **configure scheduler ftp timestamp** command determines whether a timestamp is added to filenames to distinguish them from each other and prevent overwriting existing files. **append** – Date and time are added to the filename. **none** – The filename is used as entered. This is the default. Example: IAC#**configure scheduler ftp timestamp append**

Configure Security

The **configure security** command limits access to the system.

See *IP Security* on page A-38 for a detailed description of the IP security table.

Table A-14. Configure Security Command (1 of 3)

configure security ip {*port_id***} {disabled | enabled}**
Minimum Access Level: **Administrator**
The **configure security ip** command determines whether there is a limit on the number of IP addresses associated with a DSL port. For more information see *IP Security* on page A-38. ***port_id*** – Identifies the DSL port to be affected. The possible forms of the identifier are described in Chapter 2, *Terminology and Conventions*. **disabled** – Specifies that there are no restrictions on the number of IP addresses on the specified port. This is the default. **enabled** – Specifies that there are restrictions on the number of IP addresses allowed on the specified port. The system must be in multiplex forwarding (mux) mode, else the following message is displayed: **Command not allowed: System must be in mux forwarding mode** See Table A-4, Configure Bridge Command for information about mux forwarding mode. Example: IAC#**configure security ip 1/1 enabled**
configure security ip {*port_id***} add {***ip_address***} {***nhr_address***}**
Minimum Access Level: **Administrator**
The **configure security ip add** command specifes an IP address allowed to be active on a particular DSL port. For more information see *IP Security* on page A-38. ***port_id*** – Identifies the DSL port to be affected. The possible forms of the identifier are described in Chapter 2, *Terminology and Conventions*. ***ip_address*** – Specifies an IP address allowed to be active on the port. If the table of allowed IP addresses already has the number of addresses specified by the **configure security IP max-ip** command, the following error message is displayed: **Command not allowed: Too many static entries** ***nhr_address*** – Specifies the address of the Next Hop Router for this port. It overrides the default address. Example: IAC#**configure security ip 1/1 add 135.27.90.2 135.27.90.21**

Table A-14. Configure Security Command (2 of 3)

configure security ip {*port_id***} delete {***ip_address***}**
Minimum Access Level: **Administrator**
The **configure security ip delete** command deletes an IP address in the table of addresses allowed to be active on a particular DSL port. ***port_id*** – Identifies the port to be affected. The possible forms of the identifier are described in Chapter 2, *Terminology and Conventions*. ***ip_address*** – Specifies an IP address to be deleted. The address must exist in the table of addresses for this port. You can display the table using the **configure security ip show** command. Example: IAC#**configure security ip 1/1 delete 135.27.90.2**
configure security ip {*port_id***} max-ip {***max_ip***}**
Minimum Access Level: **Administrator**
The **configure security ip max-ip** command specifes the number of IP addresses allowed to be active on a particular DSL port. For more information see *IP Security* on page A-38. ***port_id*** – Identifies the port to be affected. The possible forms of the identifier are described in Chapter 2, *Terminology and Conventions*. ***max_ip*** – Specifies the maximum number of IP addresses allowed on the port. The valid range is 1–20. The default is 1. Example: IAC#**configure security ip 1/48 max-ip 2**
configure security ip {*port_id***} show**
Minimum Access Level: **Administrator**
The **configure security ip show** command displays the table of addresses allowed for a particular DSL port. ***port_id*** – Identifies the port whose table is to be displayed. The possible forms of the identifier are described in Chapter 2, *Terminology and Conventions*. Example: IAC#**configure security ip 1/48 show**

Table A-14. Configure Security Command (3 of 3)

configure security mac {*port_id***} add {***mac_address***}**
Minimum Access Level: **Administrator**
The **configure security mac add** command specifes a MAC address allowed to send data to a particular DSL port. The address is added to a table of up to 20 entries. ***port_id*** – Identifies the port to be affected. The possible forms of the identifier are described in Chapter 2, *Terminology and Conventions*. ***mac_address*** – Specifies a MAC address allowed to send data to the port. Traffic from any other MAC address is dropped. Adding an address automatically enables the MAC address filtering feature for the port. The address must be in the form *xx-xx-xx-xx-xx-xx*, where each *x* is a hexadecimal digit 0–f. Example: IAC#**configure security mac 1/1 add 00-01-d2-e4-d3-c1**
configure security mac {*port_id***} delete {***mac_address* **| all}**
Minimum Access Level: **Administrator**
The **configure security mac delete** command deletes a MAC address in the table of addresses allowed to send data to a particular DSL port. ***port_id*** – Identifies the port to be affected. The possible forms of the identifier are described in Chapter 2, *Terminology and Conventions*. ***mac_address*** – Specifies a MAC address to be deleted. The address must exist in the table of addresses for this port. You can display the table using the configure security mac show command. The address must be in the form *xx-xx-xx-xx-xx-xx*, where each *x* is a hexadecimal digit 0–f. **all** – Specifies that all MAC addresses defined for the port are to be deleted. The MAC address filtering feature is disabled for the port. Example: IAC#**configure security mac 1/1 delete 00-01-d2-e4-d3-c1**
configure security mac {*port_id***} show**
Minimum Access Level: **Administrator**
The **configure security mac show** command displays the table of MAC addresses allowed for a particular DSL port. ***port_id*** – Identifies the port whose table is to be displayed. The possible forms of the identifier are described in Chapter 2, *Terminology and Conventions*. Example: IAC#**configure security ip 1/48 show**

IP Security

Entries in the table of allowed IP addresses are made in one of two ways:

- **Dynamic** entries are automatically learned by the unit by monitoring DHCP messages that pass through the unit between a subscriber's host and a DHCP server. Learning of dynamic entries in this manner is always active. Dynamic entries are not retained in non-volatile storage so they are lost when the unit is reset or loses power. Dynamic entries are removed if and when the lease on the DHCP-provided address expires or when the host relinquishes its lease on the address.
- **Static** entries are entered by an administrator using the **configure security ip add** command. Static entries are saved in non-volatile storage and can only be removed by administrator action.

Entries in this table are used for two functions:

- If the bridge mode is configured for multiplexing, entries in the table control the flow of hardware (MAC) address information via ARP requests and responses passing through the unit.

  If the unit is configured for multiplexing and there is not an entry in this table for a subscriber's host, that host will not be able to obtain MAC address information for other hosts on the subnet via the BitStorm 4800. In addition, hosts that are connected on the upstream side of the unit will not be able to obtain MAC information for this subscriber's host. (A host that is connected on the DSL side of the unit cannot obtain MAC address information about any host other than the port's Next Hop Router when the unit is configured for multiplexing.)

  For typical TCP/IP communications, the inability to obtain MAC address information effectively blocks communications. However, it may have no effect at all on other protocols (such as PPPoE) that do not require the MAC address information that is obtained via ARP messages.
- If IP Security is enabled for a DSL port, the unit drops all messages that are received at that port whose Ethertype is not either ARP or IP and whose source IP address is not found in the IP address table.

When IP Security is enabled for a DSL port, the restrictions on upstream data flow described above are enforced. In addition to restricting communication to only those addresses that are in the table, a maximum can be set on the number of addresses that can be in use on a port. This number is the sum of the static and dynamic entries for that port. If the limit is reached, the unit will block all requests for allocation of additional addresses via DHCP. This condition remains until one of the following happens:

- The lease on an existing dynamic entry for this port expires
- A subscriber's host connected to this port releases its DHCP-assigned address
- One or more entries are deleted from the table by an administrator
- The limit on the number of entries is increased
- IP Security is disabled on the port

Configure SNTP

The **configure sntp** commands define the use of a Simple Network Time Protocol (SNTP) server to set and update the date in time in the unit. If SNTP is enabled, the unit makes an SNTP request at initialization and then periodically at the interval specified by the **configure sntp interval** command.

Table A-15. Configure SNTP Command

configure sntp {disable | enable}
Minimum Access Level: **Administrator**
The **configure sntp** command determines whether the unit makes SNTP requests. **disable** – The unit does not make SNTP requests. Date and time must be set manually. **enable** – The unit updates the date and time periodically by sending requests to an SNTP server. Example: IAC#**configure sntp disable**
configure sntp address {*ip_address***}**
Minimum Access Level: **Administrator**
The **configure sntp address** command specifies the IP address of an SNTP server. ***ip_address*** – The address of an SNTP server. The default is 192.5.41.40. Example: IAC#**configure sntp address 137.90.127.40**
configure sntp interval {*interval***}**
Minimum Access Level: **Administrator**
The **configure sntp interval** command specifies the frequency that the unit should make SNTP requests to update the date and time. ***interval*** – The period, in hours, between SNTP requests. Valid values are 1–24. The default is 24. Example: IAC#**configure sntp interval 12**

Configure Syslog

The **configure syslog** command limits the messages written to the system log file.

Table A-16. Configure Syslog Command

configure syslog rate-limiting {disabled | enabled}
Minimum Access Level: **Administrator**
The **configure syslog rate-limiting** command determines whether duplicate messages are written to the system log. **disabled** – All messages (satisfying the syslog threshold setting) are written to the system log. This is the default. **enabled** – Duplicate messages are written to the system log only if they are received more than five minutes apart. Example: `IAC#configure syslog rate-limiting disabled`
configure syslog threshold {emergency | alert | information | debug}
Minimum Access Level: **Administrator**
The **configure syslog threshold** command specifies the levels of messages that are written to the system log. **emergency** – Only emergency messages are written to the system log. **alert** – Emergency and alert messages are written to the system log. This is the default. **information** – Emergency, alert, and informational messages are written to the system log. **debug** – Emergency, alert, informational, and debugging messages are written to the system log. Example: `IAC#configure syslog threshold information`

Configure System Information

The **configure system information** commands store a system name, location, and description.

Table A-17. Configure System Information Command

configure system information system-location {*location***}**
Minimum Access Level: **Administrator**
The **configure system information system-location** command stores the location of the system. ***location*** – Up to 36 printable characters. No spaces are allowed. Example: IAC#**configure system information system-location Building_C_First_Floor**
configure system information system-name {*name***}**
Minimum Access Level: **Administrator**
The **configure system information system-name** command stores a name identifying the system. ***name*** – Up to 36 printable characters. No spaces are allowed. Example: IAC#**configure system information system-name Paradyne_IAC_8**

Configure System Options

The **configure system options** commands configure system-wide parameters for the BitStorm 4800.

Table A-18. Configure System Options Command (1 of 2)

configure system options date-display-format {dd/mm/yy | mm/dd/yy}
Minimum Access Level: **Administrator**
The **configure system options date-display-format** command determines the date format displayed and accepted by the system. **dd/mm/yy** – The date display format is in the order day, month, year. **mm/dd/yy** – The date display format is in the order month, day, year. This is the default. Example: IAC#**configure system options date-display-format dd/mm/yy**
configure system options inactivity-timeout {*time*}
Minimum Access Level: **Administrator**
The **configure system options inactivity-timeout** command specifies how long a telnet session can exist with no activity before it is terminated by the system. ***time*** – Specifies the amount of time in minutes an inactive telnet session can exist before it is terminated. The valid range is 1–20. The default is 5 minutes. A value of 0 (zero) disables the inactivity timeout. Example: IAC#**configure system options inactivity-timeout 10**
configure system options port-display-format {name | sle | unit/port}
Minimum Access Level: **Administrator**
The **configure system options port-display-format** command determines the way DSL ports are identified by the system. The various ways of distinguishing ports are described in *System Terminology* in Chapter 2, *Terminology and Conventions*. **name** – Ports are referred to by name. **sle** – Ports are referred to by Single Logical Entity (SLE) number. **unit/port** – Ports are referred to by unit number and port number. This is the default. Example: IAC#**configure system options port-display-format sle**

Table A-18. Configure System Options Command (2 of 2)

configure system options test-timeout {*time***}**
Minimum Access Level: **Administrator**
The **configure system options test-timeout** command specifies the maximum amount of time a disruptive test is allowed to run. ***time*** – Specifies the amount of time in minutes a disruptive test can run before it is terminated. The valid range is 1–30. The default is 5 minutes. Example: IAC#**configure system options test-timeout 2**

Configure Uplink

The **configure uplink** command determines whether the GigE Uplink port or the V.35/X.21 port on the Management Module is used for the uplink. If the Management Module has a V.35/X.21 port, the V.35/X.21 port is the default uplink. This command therefore allows you to override the default by specifying the GigE Uplink port as the uplink.

Table A-19. Configure Uplink Command

configure uplink {gige-uplink | module}
Minimum Access Level: **Administrator**
The **configure uplink** command determines the port used for the uplink. **gige-uplink** – The uplink is the GigE Uplink Ethernet port. **module** – The uplink is the V.35/X.21 port on the Management Module. Example: IAC#**configure uplink gige-uplink**

Configure Uplink-Tag

The **configure uplink-tag** commands assign a VLAN tag to every DSL port. The range of numbers is determined by a base number and an index number:

Table A-20. VLAN Tag Ranges

Base	Index 1	Index 2	Index 3	Index 4	Index 5
16	16 – 63	64 – 111	112 – 159	160 – 207	208 – 255
512	512 – 559	560 – 607	608 – 655	656 – 703	704 – 751
1024	1024 –1071	1072 – 1119	1120 – 1167	1168 – 1215	1216 – 1263
1536	1536 –1583	1584 – 1631	1632 – 1679	1680 – 1727	1728 – 1775
2048	2048 – 2095	2096 – 2143	2144 – 2191	2192 – 2239	2240 – 2287
2560	2560 – 2607	2608 – 2655	2656 – 2703	2704 – 2751	2752 – 2799
3072	3072 – 3119	3120 – 3167	3168 – 3215	3216 – 3263	3264 – 3311
3584	3584 – 3631	3632 – 3679	3680 – 3727	3728 – 3775	3776 – 3823

The default base value is 16 and the default index value is 1, so the default VLAN tags for DSL ports 1–48 of a unit are 16–63, respectively.

Table A-21. Configure Uplink-Tag Command

`configure uplink-tag base {`*`base`***`}`**
Minimum Access Level: **Administrator**
The **configure uplink-tag base** command determines the base value to be used for setting VLAN tags for the DSL ports. ***base*** – Specifies the base value used in setting the range of VLAN tags. Valid values are 16, 512, 1024, 1536, 2048, 2560, 3072, and 3584. The default is 16. See Table A-20, VLAN Tag Ranges, to see the effect of the base on VLAN tag ranges. Example: `IAC#configure uplink-tag base 1024`
`configure uplink-tag index {`*`index`***`}`**
Minimum Access Level: **Administrator**
The **configure uplink-tag index** command determines the index value to be used for setting VLAN tags for the DSL ports. ***index*** – Specifies the index value used in setting the range of VLAN tags. Valid values are 1–5. The default is 1. See Table A-20, VLAN Tag Ranges, to see the effect of the index on VLAN tag ranges. Example: `IAC#configure uplink-tag index 2`

Configure User-Accounts

The **configure user-accounts** commands create and delete user accounts for managing the BitStorm 4800.

Table A-22. Configure User-Accounts Command

configure user-accounts **create {***user***} {***login_password***} [***privilege_password***]**
Minimum Access Level: **Administrator**
The **configure user-accounts create** command creates a user account and defines passwords for it. It also can be used to change passwords. ***user*** – Specifies a user name of 1–15 printable characters. Spaces are not allowed. If the user already exists, the command modifies the password or passwords for the user. ***login_password*** – Specifies a password of 1–15 printable characters. Spaces are not allowed. A login password is required of all users. ***privilege_password*** – Specifies a password of 1–15 printable characters. Spaces are not allowed. The optional second password allows users to enter privileged mode to configure the system. The privilege password must be different than the login password. Example: IAC#**configure user-accounts create admin2 sesame vip** IAC#**configure user-accounts create admin2 sesame newpass**
configure user-accounts delete {*user***}**
Minimum Access Level: **Administrator**
The **configure user-accounts delete** command deletes a user account. ***user*** – Specifies the user account to be deleted. Example: IAC#**configure user-accounts delete tempacct**

Copy

The **copy** command saves and restores configurations.

Table A-23. Copy Command

copy ftp {*ip_address***} {***user_name***} {***password***} {***filename***} startup-config**
copy running-config startup-config
copy startup-config ftp {*ip_address***} {***user_name***} {***password***} {***filename***}**
copy startup-config running-config
Minimum Access Level: **Administrator**
The **copy** command copies the configuration of the BitStorm 4800. It can be used to save and recover configurations. **ftp** – Specifies that the source or destination file is on an FTP server. The ftp keyword must be followed in order by: – ***ip_address*** – The IP address of the FTP server – ***user_name*** – A user name allowed on the FTP server – ***password*** – The password associated with the user name – ***filename*** – The name of the source or destination file **running-config** – Specifies that the source or destination file is the configuration in active volatile memory. The running configuration is not permitted as the source or destination of an FTP operation. **startup-config** – Specifies that the source or destination file is the configuration in non-volatile memory. Example: IAC#**copy ftp 135.90.28.28 ftpuser ftppw save.config startup-config**

End

The **end** command terminates privileged mode.

Table A-24. End Command

end
Minimum Access Level: **Administrator**
The **end** command terminates a privileged mode session and continues the session in standard mode. If the end command is executed by a user not in privileged mode, it places the user at the top of the command tree like one or more **back** commands. Example: IAC#**end** You are ending your privilege mode session IAC>_

Exit

The **exit** command terminates the user session.

Table A-25. Exit Command

exit
Minimum Access Level: **User**
The **exit** command terminates the user session. If the user session is by telnet, the connection is dropped. Example: IAC#**exit**

Firmware

The **firmware** command downloads and applies new firmware to the BitStorm 4800, and displays the version numbers of the active and alternate firmware.

Table A-26. Firmware Command (1 of 2)

firmware download {*ip_address***} {***user_name***} {***password***} {***filename***} {no | yes}**
Minimum Access Level: **Administrator**
The **firmware download** command downloads new firmware to the BitStorm 4800, and optionally applies it immediately. ***ip_address*** – Specifies the network address of the FTP server. ***user_name*** – Specifies a user name accepted by the FTP server. ***password*** – Specifies the password associated with the user name. ***filename*** – Specifies the file containing the configuration backup. **no** – The file is downloaded to the alternate firmware area, but not applied or executed. **yes** – The file is downloaded and applied immediately. The BitStorm 4800 is reset. Example: IAC#**firmware download 135.27.90.98 admin admnpass firm0302.bin no**
firmware download-status
Minimum Access Level: **Administrator**
The **firmware download-status** command displays the status of the active or last firmware download. Example: IAC#**firmware download-status**

Table A-26. Firmware Command (2 of 2)

firmware revision
Minimum Access Level: **Administrator**
The **firmware revision** command displays the revision numbers of the firmware currently running and alternate firmware maintained in memory. Example: `IAC#`**`firmware revision`**
firmware switch
Minimum Access Level: **Administrator**
The **firmware switch** command loads and executes the alternative firmware file. This resets the BitStorm 4800. Example: `IAC#`**`firmware switch`** `IAC#Switch from firmware revision S01.02.03 to firmware revision S01.02.04? (yes/no)` **`yes`** `IAC#Firmware switched, system rebooting`

Paging

The **paging** command enables and disables the More prompt.

Table A-27. Paging Command

paging {disabled | enabled}
Minimum Access Level: **User**
The **paging** command determines how a full screen of output is displayed. The selection affects only the user who enters the command. **disabled** – Specifies that output is sent to the screen without interruption. **enabled** – Specifies that when 23 lines of output have been sent to the screen, a **More** prompt is displayed on line 24. When **More** is displayed, you can: – Press the space bar to view the next screen of output – Press the Enter key to view the next line of output Example: `IAC>`**`paging enabled`**

Password

The **password** command changes the password at the current level:

- If the **password** command is executed while in privilege mode, the privilege password is changed
- If the **password** command is executed while in user mode, the user password is changed

Table A-28. Password Command

password
Minimum Access Level: **User**

The **password** command changes the user or administrator (privilege) password, depending on which level is active.
Example:
`IAC#password`
`enter old admin level password: ****`
`enter new admin level password: ******`
`enter new admin level password again: ******`
`password changed`
`IAC#`

Privilege

The **privilege** command switches the user to Administrator mode.

Table A-29. Privilege Command

privilege
Minimum Access Level: **User**

The **privilege** command causes the user to be prompted for an administrator password. When the password is entered correctly, the user is placed in Administrator (privileged) mode.
Example:
`IAC>privilege`
`Password: ******`
`IAC#`

Restart

The **restart** command restarts the unit.

Table A-30. Restart Command

restart unit {*unit_number* **|** *unit_name***}**
Minimum Access Level: **Administrator**
The **restart unit** command restarts the unit, causing it to reload the startup configuration and retrain the DSL ports. Example: IAC#**restart unit 1**

Save

The **save** command saves the running configuration to Non-Volatile Random Access Memory (NVRAM).

Table A-31. Save Command

save
Minimum Access Level: **Administrator**
The **save** command copies the running configuration, which is in volatile memory, to the startup configuration file, which is in nonvolatile memory. The **IAC#** prompt changes to **IAC#!** when the configuration has been changed and has not yet been saved. It returns to **IAC#** after the **save** command is executed. Example: IAC#!**save** IAC#_

Show

The **show** command displays configuration options and statistics.

Table A-32. Show Command (1 of 20)

show bridge [*port_id***]**
Minimum Access Level: **User**
The **show bridge** command displays the MAC table. ***port_id*** – Specifies that the display should be limited to entries for a single port. Example: `IAC#show bridge`
Display results: ■ **Mode** – The functional mode of the bridge: – switched – Switched mode. The system acts as a transparent learning bridge. – multiplexing – The system treats each DSL port as if it were a private network connected to the uplink, and never forwards data on another DSL port. – sms – The system treats each DSL port as if it were a private network connected to the uplink, and never forwards data on another DSL port. In addition, a management VLAN is created on the uplink for use by the SMS. ■ **Total Entries** – The number of entries currently in the table. ■ **hardware address** – The MAC address of the table entry. ■ **port-id** – The port ID of the entry. ■ **status** – The status of the entry: – invalid – This learned entry has timed out but has not yet been deleted. – learned – This entry was learned. – management – This entry has a matching static address. – other – None of the other statuses apply to this entry. – self – This entry is the BitStorm 4800.
show bridge timeout
Minimum Access Level: **User**
The **show bridge timeout** command displays the bridge table entry timeout value in seconds. Example: `IAC#show bridge timeout`
Display results: ■ ***timeout*** – The bridge table entry timeout value.

Table A-32. Show Command (2 of 20)

show date
Minimum Access Level: **User**
The **show date** command displays the system date, time, and time zone Example: `IAC#show date`
Display results: ■ ***mm/dd/yy*** or ***dd/mm/yy*** – The date in the chosen system format. ■ ***hh/mm/ss*** – The time in hours, minutes, and seconds. ■ **timezone** – The offset from Greenwich Mean Time.
show filter [*filter_name***]**
Minimum Access Level: **User**
The **show filter** command displays configured data filters. ***filter_name*** – Specifies that the display should be limited to a single filter. Example: `IAC#show filter`
Display results: ■ ***filter-name*** – The name of the filter. ■ ***action*** – The action to be performed: – forward – Specifies that a packet is to be forwarded to the user when none of the conditions specified in the rule or rules are matched. – discard – Specifies that a packet is to be discarded when none of the conditions specified in the rule or rules are matched. ■ **rule-name** – The name assigned to the rule or rules associated with this filter. ■ **type** – The rule type: – ether – The rule is based on Ethertypes. ■ **action** – The action to perform if the rule is satisfied: – forward – The packet is forwarded. – discard – The packet is discarded. ■ **rule** – The rule criteria: – The Ethertypes the rule affects.

Table A-32. Show Command (3 of 20)

show filter-binding [filter [*filter_name***]] | [port [***port_id***]]**
Minimum Access Level: **User**
The **show filter-binding** command displays the bindings of filters to interfaces. **filter** – Specifies that output is sorted by filter name. ***filter_name*** – Specifies that the display should be limited to a single filter. **port** – Specifies that output is sorted by port number. ***port_id*** – Specifies that the display should be limited to a single port. Example: `IAC#show filter-binding`
Display results: ■ **port-id** – The port the rule is bound to. ■ **filter-name** – The name of the filter. ■ **direction** – The direction of the data stream affected by this binding: – inbound – Traffic toward the port is affected. – outbound – Traffic from the port is affected.
show filter-rule [*rule_name***]**
Minimum Access Level: **User**
The **show filter-rule** command displays configured filter rules. ***filter_name*** – Specifies that the display should be limited to a single filter. Example: `IAC#show filter-rule`
Display results: **rule-name** – The name assigned to the rule. ■ **type** – The rule type: – ether – The rule is based on Ethertypes. – ether-snap – The rule applies to Layer 2 SubNetwork Access Protocol (SNAP) traffic. ■ **action** – The action to perform if the rule is satisfied: – forward – The packet is forwarded. – discard – The packet is discarded. ■ **rule** – The rule criteria: – The Ethertypes the rule affects.

Table A-32. Show Command (4 of 20)

show interface console
Minimum Access Level: **User**
The **show interface console** command displays the configuration of the Console port on the 4800 or 4804 Management Module. Example: `IAC#show interface console`
Display results: Configuration parameters for the port. See the **configure interface console** commands in Table A-10, Configure Interface Command, for information about the parameters.
show interface dsl {*port_id*} clear-statistics
Minimum Access Level: **User**
The **show interface dsl clear-statistics** command resets statistics for all DSL ports or a specified DSL port. ***port_id*** – Specifies that the display should be limited to this specified port. If **all** is specified, all statistics are cleared. **clear-statistics** – Resets to zero the statistics for this session. This affects only the statistics displayed using the **show** command during this session. All statistics continue to be maintained. Example: `IAC#show interface dsl all clear-statistics`
show interface dsl {*port_id*} configuration
Minimum Access Level: **User**
The **show interface dsl configuration** command displays information about all DSL ports or a specified DSL port. ***port_id*** – Specifies that the display should be limited to this specified port. If **all** is specified, information is displayed for all ports. **configuration** – Specifies that the port's configuration should be displayed. Example: `IAC#show interface dsl 1/1 configuration`
Display results: Configuration parameters for the port. See the **configure interface dsl** commands in Table A-10, Configure Interface Command, for information about the parameters.

Table A-32. Show Command (5 of 20)

show interface dsl {*port_id*} performance
Minimum Access Level: **User**
The **show interface dsl performance** command displays performance information for all DSL ports or a specified DSL port. ***port_id*** – Specifies that the display should be limited to this specified port. If **all** is specified, information is displayed for all ports. **performance** – Specifies that performance statistics for the specified port should be displayed. Example: `IAC#show interface dsl all performance`
Display results: ■ **Status** – The status of the link: – dormant – The link has not yet trained up. – down – The link is down. – notConnected – The link is training. – unknown – The link's status cannot be determined. – up – The link is enabled and ready to send packets. ■ **Line Rate Up** – The upstream data rate. ■ **Line Rate Down** – The downstream data rate. ■ **Margin Up** – The amount of distortion that can be tolerated, in dBm, upstream. ■ **Margin Down** – The amount of distortion that can be tolerated, in dBm, downstream. ■ **Attainable Rate** – The maximum rate negotiated. ■ **Attenuation** – The decrease of intensity of the signal across the link, in dB.
show interface dsl {*port_id*} rate
Minimum Access Level: **User**
The **show interface dsl rate** command displays the data rate for all DSL ports or a specified DSL port. ***port_id*** – Specifies that the display should be limited to this specified port. If **all** is specified, information is displayed for all ports. **rate** – Specifies that the current rate of the specified port should be displayed. Example: `IAC#show interface dsl all rate`

Table A-32. Show Command (6 of 20)

show interface dsl rate, *continued*
Display results: ■ **Status** – The status of the link: – dormant – The link has not yet trained up. – down – The link is down. – notConnected – The link is training. – unknown – The link's status cannot be determined. – up – The link is enabled and ready to send packets. ■ **Line Rate Up** – The upstream data rate. ■ **Line Rate Down** – The downstream data rate.
`show interface dsl {`*`port_id`***`} statistics`**
Minimum Access Level: **User**
The **show interface dsl statistics** command displays statistics for all DSL ports or a specified DSL port. ***port_id*** – Specifies that the display should be limited to this specified port. If **all** is specified, information is displayed for all ports. **statistics** – Specifes that the error statistics for the specified port should be displayed. Example: `IAC#`**`show interface dsl 1/1 statistics`**
Display results: ■ **dsl link** – The status of the link: – dormant – The link has not yet trained up. – down – The link is down. – notConnected – The link is training. – unknown – The link's status cannot be determined. – up – The link is enabled and ready to send packets. ■ **current link up time** – The number of days, hours, minutes, and seconds the interface has been active. ■ **line code** – The line code used on the port: DMT, ANSI, or G.lite. ■ **latency** – The buffer setting for the port: fast or interleaved.

Table A-32. Show Command (7 of 20)

show interface dsl statistics, *continued*
DSL Statistics (Up and Down denote values for the upstream and downstream directions): ■ **margin** – The amount of noise margin that can be tolerated, in dB. ■ **rate** – The data rate. ■ **attainable rate** – An estimate of the maximum attainable rate. ■ **attenuation** – The decrease of intensity of the signal across the link, in dB. ■ **errored seconds** – Seconds during which an error occurred. ■ **severely errored seconds** – Seconds during which there was a major error such as an out of frame condition, or a bit error density greater than 10^{-2}. ■ **unavailable seconds** – Seconds accrued after ten consecutive severely errored seconds. ■ **loss of power** – Number of times the remote unit has been powered off. ATM Statistics (Up and Down denote values for the upstream and downstream directions): ■ **total cells rx –** Total number of ATM cells received. ■ **total cells tx –** Total number of ATM cells sent. ■ **total HEC** – Number of cells from the CPE whose headers were corrected. ■ **total OCD** – Number of Out of Cell Delineation events on the link from the CPE. Ethernet Statistics: ■ **total frames discarded** – Number of frames discarded due to errors. ■ **total bytes rx** – Number of bytes received on the port. ■ **total bytes tx** – Number of bytes transmitted by the port. ■ **total frames rx** – Number of bytes received on the port. ■ **total frames tx** – Number of bytes transmitted by the port. ■ **total rx errors** – Number of frames received with errors. ■ **total tx errors** – Number of frames transmitted with errors.
show interface ethernet {*port_id***} clear-statistics**
Minimum Access Level: **User**
The **show interface ethernet clear-statistics** command resets statistics for all Ethernet ports or a specified port. ***port_id*** – Specifies that the display should be limited to this specified port. If **all** is specified, information is displayed for all Ethernet ports. **clear-statistics** – Resets to zero the statistics for this session. This affects only the statistics displayed using the **show** command during this session. All statistics continue to be maintained. Example: `IAC#show interface ethernet 1/mgmt clear-statistics`

Table A-32. Show Command (8 of 20)

show interface ethernet {*port_id*} configuration
Minimum Access Level: **User**
The **show interface ethernet configuration** command displays configuration information for all Ethernet ports or a specified port. ***port_id*** – Specifies that the display should be limited to this specified port. If **all** is specified, information is displayed for all Ethernet ports. **configuration** – Specifies that the port's configuration should be displayed. Example: `IAC#show interface ethernet 1/mgmt configuration`
Display results: ■ **current link up time** – The number of days, hours, minutes, and seconds the interface has been active. The remainder of the display shows configuration parameters for the port. See the **configure interface ethernet** commands in Table A-10, Configure Interface Command, for more information about the parameters.
show interface ethernet {*port_id*} statistics
Minimum Access Level: **User**
The **show interface ethernet statistics** command displays statistics for all Ethernet ports or a specified port. ***port_id*** – Specifies that the display should be limited to this specified port. If **all** is specified, information is displayed for all Ethernet ports. **statistics** – Specifes that the error statistics for the specified port should be displayed. Example: `IAC#show interface ethernet 1/mgmt statistics`
Display results: ■ **ethernet link** – The status of the link: – dormant – The link has no device attached. – down – The link is down. – unknown – The link's status cannot be determined. – up – The link is enabled and ready to send packets. ■ **current link up time** – The number of days, hours, minutes, and seconds the interface has been active. ■ **rate** – The data rate of the port. ■ **mode** – The duplex mode: full duplex or half duplex. ■ **connector type** – The connector used for the link: rj45 or fiber. ■ **total bytes rx** – Number of bytes received on the port. ■ **total bytes tx** – Number of bytes transmitted by the port. ■ **total frames rx** – Number of bytes received on the port. ■ **total frames tx** – Number of bytes transmitted by the port. ■ **total frames discarded** – Number of frames discarded by the port.

Table A-32. Show Command (9 of 20)

show interface modem
Minimum Access Level: **User**
The **show interface modem** command displays the configuration of the Modem port on the 4800 or 4804 Management Module. Example: `IAC#show interface modem`
Display results: ■ **current link up time** – The number of days, hours, minutes, and seconds the interface has been active. The remainder of the display shows configuration parameters for the port. See the **configure interface modem** commands in Table A-10, Configure Interface Command, for more information about the parameters.
show interface v35 clear-statistics
Minimum Access Level: **User**
The **show interface v35 clear-statistics** command resets statistics for the V.35/X.21 port of the 4804 Management Module. **clear-statistics** – Resets to zero the statistics for this session. This affects only the statistics displayed using the **show** command during this session. All statistics continue to be maintained. Example: `IAC#show interface v35 clear-statistics`
show interface v35 configuration
Minimum Access Level: **User**
The **show interface v35 configuration** command displays configuration information for the V.35/X.21 port of the 4804 Management Module. **configuration** – Specifies that the V.35/X.21 port's configuration should be displayed. Example: `IAC#show interface v35 configuration`
Display results: ■ **current link up time** – The number of days, hours, minutes, and seconds the interface has been active. The remainder of the display shows configuration parameters for the port. See the **configure interface v35** commands in Table A-10, Configure Interface Command, for more information about the parameters.

Table A-32. Show Command (10 of 20)

show interface v35 statistics
Minimum Access Level: **User**
The **show interface v35 statistics** command displays statistics for the V.35/X.21 port of the 4804 Management Module. **statistics** – Specifes that the error statistics for the V.35/X.21 port should be displayed. Example: `IAC#show interface v35 statistics`
Display results: ■ **serial link** – The status of the link: – dormant – The link has no device attached. – down – The link is down. – testing – A test is in progress on the link. – unknown – The link's status cannot be determined. – up – The link is enabled and ready to send packets. ■ **current link up time** – The number of days, hours, minutes, and seconds the interface has been active. ■ **link type** – The electrical interface: – eia530a – The interface is EIA-530-A. – v35 – The interface is V.35. – x21 – The interface is X.21. ■ **RTS** – The status of the Request To Send lead (on or off). ■ **CTS** – The status of the Clear To Send lead (on or off). ■ **DSR** – The status of the Data Set Ready lead (on or off). ■ **DTR** – The status of the Data Terminal Ready lead (on or off). ■ **LSD** – The status of the Line Signal Detect lead (on or off). HDLC Uplink Statistics: ■ **total frames received –** Total number of frames received. ■ **total frames transmitted –** Total number of frames sent. ■ **total receive errors** – Number of errors detected in incoming data. ■ **total transmit errors** – Number of errors detected in outgoing data PPP Uplink Statistics: ■ **total receive bytes –** Total number of bytes received. ■ **total transmit bytes –** Total number of bytes sent. ■ **total receive errors** – Number of errors detected in incoming data. ■ **total transmit errors** – Number of errors detected in outgoing data

Table A-32. Show Command (11 of 20)

show ip nhr
Minimum Access Level: **User**
The **show ip nhr** command displays the address of the Next Hop Router. Example: `IAC#show ip nhr`
Display results: ■ **nhr address** – The management Next Hop Router IP address.
show management arp
Minimum Access Level: **User**
The **show management arp** command displays the ARP table for the management interface. Example: `IAC#show management arp`
Display results: ■ **ip address** – The IP address of the entry. ■ **mac address** – The hardware address of the entry. ■ **type** – The source of the address: – dynamic – The address was learned. – static – The address was added to the table by an administrator.
show management ip
Minimum Access Level: **User**
The **show management ip** command displays the Management Module settings. Example: `IAC#show management ip`
Display results: ■ **ip address** – The management IP address. ■ **subnet mask** – The subnet mask to be applied to the IP address. ■ **gateway** – The management next hop or gateway IP address.

Table A-32. Show Command (12 of 20)

show management snmp
Minimum Access Level: **User**
The **show management snmp** command displays the settings for SNMP access. Example: `IAC#show management snmp`
Display results: ■ **state** – The availability of SNMP access (disabled or enabled). ■ **access-validation** – Whether access validation is in force (disabled or enabled). ■ **public-string** – The community string for read-only access. ■ **private-string** – The community string for read-write access. ■ **nms-address** – The addresses of NMS workstations permitted access if access validation is enabled. ■ **nms-traps** – The addresses to which traps are sent.
show management vlan
Minimum Access Level: **User**
The **show management vlan** command displays the settings for Bridge Mode and management VLAN tagging. Example: `IAC#show management vlan`
Display results: ■ **Bridge Mode** – The Bridge Mode: – sms – Subscriber Management System mode. – uplink-tag – UpLink Tagging mode. ■ **Management VLAN** – The VLAN tag in use (1–15).
show scheduler
Minimum Access Level: **User**
The **show scheduler** command displays the scheduler settings. Example: `IAC#show scheduler`
Display results: ■ **state** – The availability of the scheduler (disabled or enabled). ■ **server** – The address of the FTP server used for automatic configuration backup. ■ **filename** – The file containing the backup. ■ **mode** – The type of backup: – dynamic – Backup occurs upon any configuration change. – fixed – Backup occurs at a specified day and time. ■ **time** – For fixed mode, the day and time backups occur.

Table A-32. Show Command (13 of 20)

show security ip [*port_id*]
Minimum Access Level: **User**
The **show security ip** command displays the settings for IP address security. ***port_id*** – Specifies the port to be displayed. The possible forms of the identifier are described in *System Terminology* in Chapter 2, *Terminology and Conventions*. If **all** is specified or the parameter is omitted, information for all ports is displayed. Example: `IAC#show security ip 1/48`
Display results: ■ **State** – Whether IP security is in effect (disabled or enabled). ■ **Maximum IP addresses** – Maximum number of IP addresses allowed on the port. ■ **Port** – DSL port ID. ■ **IP Address** – IP address allowed on the port. ■ **NHR** – Next Hop Router for the port. ■ **Type** – The source of the address: – dynamic – The address was learned. – static – The address was added to the table of allowed addresses by the administrator.
show security mac [*port_id*]
Minimum Access Level: **User**
The **show security mac** command shows the settings for MAC address security. ***port_id*** – Specifies the port to be displayed. The possible forms of the identifier are described in *System Terminology* in Chapter 2, *Terminology and Conventions*. If **all** is specified or the parameter is omitted, information for all ports is displayed. Example: `IAC#show security mac 1/48`
Display results: ■ **State** – Whether MAC security is in effect (disabled or enabled). ■ **Port** – DSL port ID. ■ **MAC Address** – MAC address allowed to send data to the port.

Table A-32. Show Command (14 of 20)

show sntp
Minimum Access Level: **User**
The **show sntp** command displays the configuration parameters for SNTP. Example: `IAC#show sntp`
Display results: ■ **state** – Whether the unit makes SNTP requests: – disable – The unit does not make SNTP requests. – enable – The unit updates the date and time periodically by sending requests to an SNTP server. ■ **ip address** – The address defined for the SNTP server. ■ **interval** – The number of hours between SNTP requests.
show syslog
Minimum Access Level: **User**
The **show syslog** command displays the configuration and contents of the system log. Example: `IAC#show syslog`
Display results: ■ **threshold** – The level of messages written to the log: – emergency – Only emergency messages are written to the system log. – alert – Emergency and alert messages are written to the system log. This is the default. – information – Emergency, alert, and informational messages are written to the system log. – debug – Emergency, alert, informational, and debugging messages are written to the system log. ■ **rate-limiting** – Whether rate limiting (suppression of duplicate messages) is in effect (disabled or enabled). ■ **Priority** – The level of the message. ■ **Date and Time** – The date and time the message was written. ■ **Message** – The message text.

Table A-32. Show Command (15 of 20)

show system information
Minimum Access Level: **User**
The **show system information** command shows the system administrative information. Example: `IAC#show system information`
Display results: System-level information: ■ **System Name** – The name assigned to the system defined by the administrator. ■ **System Location** – The location of the system defined by the administrator. ■ **FW Revision** – The revision level of the firmware running in the system. Unit-level information. The first or only unit is designated Unit 1: ■ **Up Time** – The number of days, hours, minutes, and seconds the unit has been running. ■ **Model** – The Paradyne model number of Unit *n*. ■ **Serial Number** – The unit serial number. ■ **Main Card HW Rev** – The hardware revision level of the main circuit card. ■ **PLD (Main) Rev** – The firmware revision level of the PLD (Programmable Logic Device) on the main circuit card. ■ **Child Card HW Rev** – The hardware revision level of the child card. Management Module information: **Model** – The Paradyne model number of the module. **Serial Number** – The module's serial number. **HW revision** – The hardware revision level of the module's circuit card. **PLD (Mgmt)** – The firmware revision level of the management PLD. **PLD (V.35)** – The firmware revision level of the V.35 PLD. **MAC Address** – The hardware address of the Management Module.

Table A-32. Show Command (16 of 20)

show system options
Minimum Access Level: **User**
The **show system options** command shows the system configuration. Example: `IAC#show system options`
Display results: ■ **test-time-out** – The amount of time a test is allowed to run. ■ **port-number-display-format** – The format of port IDs used in system messages: – name – Port name. – SLE – Single Logical Entity number. – unit/port – Unit number and port number. ■ **date-display-format** – The format of dates displayed and accepted by the system: – dd/mm/yy – Day, month, year. – mm/dd/yy – Month, day, year. ■ **inactivity-time-out** – The amount of time before an inactive Telnet session is terminated.

Table A-32. Show Command (17 of 20)

show system self-test [*unit_id***]**
Minimum Access Level: **User**
The **show system self-test** command shows the self-test results for the unit, or for all hardware components. ***unit_id*** – Specifies the unit to display detailed self-test results for. If no unit is specified, a summary is displayed showing **pass** or **fail** for the system. The *unit_id* may be the unit number or the unit name. Example: IAC#**show system self-test 1**
Display results: Unit *n*: ■ Overall test results (pass or fail). Port processor (results displayed for processors 1–6): ■ **SEEP** – Serial Electrically Erasable PROM (p for pass or f for fail). ■ **CPU Reg** – Central Processing Unit control registers (p for pass or f for fail). ■ **CPU Timer** – Processor clock (p for pass or f for fail). ■ **SDRAM** – Synchronous Dynamic Random Access Memory (p for pass or f for fail). DSL ports (results displayed for ports 1–24 or 1–48; p for pass or f for fail): ■ **Memory** – Port SDRAM. ■ **Data Pump** – Port ADSL pump. ■ **PHY** – Port physical interface. Management Module: ■ **CPU Reg** – Central Processing Unit control registers (Pass or Fail). ■ **CPU Timer** – Processor clock (Pass or Fail). ■ **SDRAM** – Synchronous Dynamic Random Access Memory (Pass or Fail). ■ **File System** – Firmware and configuration data memory (Pass or Fail). V.35 Uplink: ■ **CPU Reg** – Central Processing Unit control registers (Pass or Fail). ■ **CPU Timer** – Processor clock (Pass or Fail). ■ **SDRAM** – Synchronous Dynamic Random Access Memory (Pass or Fail). ■ **Uplink Interface** – Physical interface (Pass or Fail). GigE Uplink Interface, GigE Downlink Interface, Management Port: ■ **MAC** – Media Access Control (Pass or Fail). ■ **PHY** – Physical interface (Pass or Fail). ■ **Device Reg** – Device registers (Pass or Fail).

Table A-32. Show Command (18 of 20)

show system status
Minimum Access Level: **User**
The **show system alarm** command shows the state of alarms throughout the system. Example: `IAC#show system status`
Display results: ■ **Unit** – The unit number. ■ **selftest** – The result of the power-on self-test (fail or pass). ■ **uplink** – The state of the uplink (blank or alarm). ■ **fan *n*** – The state of the fans 1–3 (blank or alarm). ■ **temperature** – The system temperature, in Centigrade. Under DSL port numbers 1–24 or 1–48 is one of the following: – **D**: Port is down. – **U**: Port is up. – **.** (period): Port is disabled.
show technical-support
Minimum Access Level: **User**
The **show technical-support** command shows contact information similar to that in *Warranty, Sales, Service, and Training Information* at the beginning of this manual. Example: `IAC#show technical-support`
show uplink
Minimum Access Level: **User**
The **show uplink** command shows the uplink selected. See *Configure Uplink* on page A-44. Example: `IAC#show uplink`
Display results: ■ **uplink** – The uplink selected for use: – gige-uplink – The GigE Uplink port. – module – The V.35/X.21 port on the Management Module.

Table A-32. Show Command (19 of 20)

show uplink-tag
Minimum Access Level: **User**
The **show uplink-tag** command shows the VLAN tag associated with each DSL port if uplink tagging is used. See *Configure Uplink-Tag* on page A-45. Example: `IAC#show uplink-tag`
Display results: ■ **Base vlan tag number** – The base value used to set VLANs. ■ **Index** – The index value used to set VLANs. ■ **PORT** and **VLAN** – Port numbers 1–24 or 1–48 are listed followed by their unique VLAN tag numbers.
show user-accounts
Minimum Access Level: **Administrator**
The **show user-accounts** command shows user names configured in the system. Example: `IAC#show user-accounts`
Display results: ■ **User Name** – The name used for logging in. Passwords are not displayed. ■ **Privilege Level** – The access level assigned to this user name: – admin – The user name has administrator privileges. – user – The user name has user privileges.
show users
Minimum Access Level: **User**
The **show users** command shows users currently logged on the system. Example: `IAC#show users`
Display results: ■ **User** – User name. ■ **Port** – Mode of access: – console – Console port. – modem – Modem port. – telnet – Telnet session. – web – Web interface. ■ **Location** – For Telnet and Web interface sessions, the IP address of the user. For the Console port and the Modem port, n/a (Not Applicable).

Table A-32. Show Command (20 of 20)

show vlans {*vlan_tag***}**
Minimum Access Level: **User**
The **show vlans** command shows the MAC addresses associated with a specified VLAN tag number. ***vlan_tag*** – Specify a valid VLAN tag number for this unit (16–3823), or the keyword **all** to display all MAC addresses for all ports. Examples: IAC#**show vlans 63** IAC#**show vlans all**
Display results: ■ **vlan-id** – A VLAN tag number. ■ **port-id** – The port the VLAN tag number is associated with. ■ **hardware-address** – The MAC address associated with the port.

Test

The **test** command initiates tests.

Table A-33. Command

test dte-loopback {start | stop}
Minimum Access Level: **Administrator**

The **test dte-loopback** command places the V.35/X.21 port of the Management Module in loopback. All data received on the port is returned without modification.
 	
No test results are displayed. You must attach external test equipment to perform a bit error rate test.
 	
start – Places the V.35/X.21 port in loopback mode.
 	
stop – Returns the V.35/X.21 port to normal mode, terminating the test.
 	
If the command is not issued to stop the test, the test stops automatically after the number of minutes specified in the test-timeout value of the **configure system options** command. See Table A-18, Configure System Options Command.
 	
Example:
 	
`IAC#test dte-loopback start`
`IAC#test dte-loopback stop`

test leds
Minimum Access Level: **Administrator**
The **test leds** command causes all Light-Emitting Diodes (LEDs) on the front panel of the unit to turn on for 30 seconds. See the *BitStorm 4800 Installation Guide* for the locations of all LEDs. Verify that all LEDs are lit. If an LED does not light up during the LED test, notify your service representative. Example: `IAC#test leds`

SNMP Traps

B

The following table shows supported traps. See *System Log* in Chapter 5, *Monitoring and Troubleshooting*, for the related system log file message and the action to take, if any, when one of these traps is received.

For a description of the MIBs supported by the BitStorm 4800, see Appendix C, *MIB Support*.

Table B-1. SNMP Traps (1 of 2)

Trap	Description	Severity	Variable Bindings	MIB
authenticationFailure	Console login failure	Minor	snmpTrapOID snmpTrapEnterprise devAuthenticationFailure-IpAddress	SNMPv2-MIB
coldStart	External power cycle of the device has occurred (hardware reset)	Warning	snmpTrapOID snmpTrapEnterprise	SNMPv2-MIB
devFileXferEvent	A configuration download failed	Warning	devFileXferStatus devFileXferErrorStatus devFileXferOperation devFileXferFileType devFileXferFileName	PDN-CONTROL-MIB
diagIfTestOver	DTE Loopback stopped	Normal	ifIndex applTestId applTestType applTestStatus	PDN-DIAGNOSTICS-MIB
diagIfTestStart	DTE Loopback started	Normal	ifIndex applTestId applTestType	PDN-DIAGNOSTICS-MIB
fanEntityModule-Operational	At least one fan is operational after a failure	Minor	entPhysicalIndex	PDN-DSLAM-SYSTEM-MIB

Table B-1. SNMP Traps (2 of 2)

Trap	Description	Severity	Variable Bindings	MIB
fanEntityModuleFailure	One or more fans failed	Major	entPhysicalIndex	PDN-DSLAM-SYSTEM-MIB
linkDown	The link is down	Major	ifIndex ifAdminStatus ifOperstatus	IF-MIB
linkUp	The link is up	Normal	ifIndex ifAdminStatus ifOperstatus	IF-MIB
mpeCcn	Configuration change (rate limited)	Warning	entPhysicalIndex	PDN-MPE-DSLAM-SYSTEM-MIB
mpeDeviceFailure	Internal system fault (loss of communication)	Major	entPhysicalIndex	PDN-MPE-DSLAM-SYSTEM-MIB
mpeDeviceFailure-Cleared	Internal system fault (loss of communication) cleared	Minor	entPhysicalIndex	PDN-MPE-DSLAM-SYSTEM-MIB
mpeEntSensor-ThresholdNotification	Over-temperature condition, or over-temperature condition cleared	Major	entPhysicalIndex mpeEntSensorThresholdValue mpeEntSensorValue	MPE-ENTITY-SENSOR-MIB
mpeEntSensorSystem ResetNotification	System shut down due to over-temperature condition	Minor	entPhysicalIndex mpeEntSensorThresholdValue mpeEntSensorValue	MPE-ENTITY-SENSOR-MIB
mpeSelfTestFailure	Any portion of a restart or self-start failed	Major	mpeDevSelfTestResults	PDN-MPE-HEALTH_AND_STATUS_MIB
pdnDevFileXferEvent	A firmware download failed	Major	pdnDevFileXferStatus pdnDevFileXferErrorStatus pdnDevFileXferOperation pdnDevFileXferFileType pdnDevFileXferFileName	PDN-CONTROL-MIB
unauthorizedUserEvent	Unauthorized user	Minor	ipNetToMediaIfIndex ipNetToMediaPhysAddress	PDN-ARP-MIB
warmStart	Power-on reset (software reset)	Warning	snmpTrapOID snmpTrapEnterprise	SNMPv2-MIB

MIB Support

C

Overview

Table C-1, Ordered MIB List, shows the order MIBs should be loaded into an NMS application.

The remainder of this appendix shows the extent of support in the BitStorm 4800 for the supported MIBs in the order they appear in the table:

Locating MIBs

Both standard and enterprise MIBs may be downloaded from the World Wide Web:

- Standard MIBs (those published as RFCs) are available from http://www.rfc-editor.org.
- Paradyne enterprise MIBs for the BitStorm 4800 are available in a single file from the Paradyne website at http://www.paradyne.com/tech_support/mibs.html. The MIBs must be loaded into your MIB browser in the order they are provided.

Order for Loading MIBs

The following table shows the recommended order for loading MIBs into an NMS application. The MIB file supplied by Paradyne has them in this order.

The list satisfies all dependencies shown in the IMPORTS clause of the MIBs. Not all MIBs may be required by your application.

Table C-1. Ordered MIB List (1 of 2)

MIB	RFC or Filename	Implemented in BitStorm 4800
SNMPv2-TC	RFC 2579	
SNMPv2- MIB	RFC 1907	Yes
RFC1213-MIB	RFC 1213	Yes
IANAifType-MIB	http://www.iana.org/assignments/ianaiftype.mib	
PDN-HEADER-MIB	pdn_Header.mib	See *PDN-HEADER-MIB* on page C-7
PDN-TC	pdn_tc.mib	
SNMP-FRAMEWORK-MIB	RFC 2571	
IP-MIB	RFC 2011	Yes
ENTITY-MIB	RFC 2737	Yes
IF-MIB	RFC 2863	Yes
ATM-TC-MIB	RFC 2514	
ATM-MIB	RFC 2515	Yes
HOST-RESOURCES-MIB	RFC 2790	
ATM-FORUM-SNMP-M4-MIB	af-nm-0095.001.mib.txt	Yes
RS-232-MIB	RFC 1659	Yes
EtherLike-MIB	RFC 2665	Yes
MAU-MIB	RFC 2668	Yes
PerfHist-TC-MIB	RFC 2493	
ADSL-TC-MIB	RFC 2662	
ADSL-LINE-MIB	RFC 2662	Yes
ADSL-LINE-EXT_MIB	draft-ietf-adslmib-adslext-07.txt	Yes
BRIDGE-MIB	RFC 1493	Yes
RFC1158-MIB	RFC 1158	
RFC1271-MIB	RFC 1271	
TOKEN-RING-RMON-MIB	RFC 1513	

Table C-1. Ordered MIB List (2 of 2)

MIB	RFC or Filename	Implemented in BitStorm 4800
RMON-MIB	RFC 2819	
RMON2-MIB	RFC2021	
Q-BRIDGE-MIB	RFC 2674	Yes
PPP-LCP-MIB	RFC 1471	Yes
PDN-MPE-DEVICE-CONTROL-MIB	mpe_Control.mib	Yes
PDN-MPE-HEALTH-AND-STATUS-MIB	mpe_HealthAndStatus.mib	Yes
PDN-MPE-DSLAM-MIB	mpe_dslam.mib	Yes
PDN-MPE-ENTITY-SENSOR-MIB	mpe_sensor.mib	Yes
PDN-ARP-MIB	pdn_Arp.mib	Yes
PDN-ATMSTATS-MIB	pdn_AtmStats.mib	Yes
PDN-CONFIG-MIB	pdn_Config.mib	Yes
PDN-CONTROL-MIB	pdn_Control.mib	Yes
PDN-IPSEC-MANUAL-MIB	pdn_IPSec.mib	Yes
PDN-IF-EXT-MIB	pdn_IfExt.mib	Yes
PDN-SECURITY-MIB	pdn_Security.mib	Yes
PDN-SYNCPORTSTATS-MIB	pdn_SyncPortStats.mib	Yes
PDN-DIAGNOSTICS-MIB	pdn_diag.mib	Yes
PDN-DSLAM-MIB	pdn_dslam.mib	Yes
PDN-ETHER-MIB	pdn_ether.mib	Yes
PDN-FILTER-MIB	pdn_filter.mib	Yes
PDN-INET-MIB	pdn_inet.mib	Yes
PDN-SYSLOG-MIB	pdn_syslog.mib	Yes
PDN-UPLINK-TAGGING-MIB	PDN-UPLINK-TAGGING-MIB.mib	Yes
PDN-STACKABLE-MIB	PDN-STACKABLE-MIB.mib	Yes
PDN-DEVICE-TIME-MIB	pdn_time.mib	Yes

SNMPv2-MIB

The SNMPv2-MIB is defined in RFC 1907. The following groups are supported:

- system (OID mib-2 1)
- snmp (OID mib-2 11)

System Group

The system group is a collection of objects common to all managed systems.

Table C-2. System Group OIDs

Object	OID	Syntax	Access	Status	Supported
sysDescr	{ system 1 }	DisplayString	read-only	current	Yes
sysObjectID	{ system 2 }	OBJECT IDENTIFIER	read-only	current	Yes
sysUpTime	{ system 3 }	TimerTicks	read-only	current	Yes
sysContact	{ system 4 }	DisplayString (0-32)	read-write	current	Yes
sysName	{ system 5 }	DisplayString (0-32)	read-write	current	Yes
sysLocation	{ system 6 }	DisplayString (0-32)	read-write	current	Yes
sysServices	{ system 7 }	INTEGER	read-only	current	Yes
sysORLast Change	{ system 8 }	TimeStamp	read-only	current	No
sysORTable	{ system 9 }	Sequence of sysOREntry	not-accessible	current	No

sysDescr

The sysDescr object provides the full name and version identification for the systems hardware and software. It displays a string with the following format:

`Paradyne BitStorm 4800; S/W Release:` *yy.yy.yy*;

Where:

— *yy.yy.yy* – Is the software revision number

sysObjectID

The sysObjectID is the vendor's identifier for a system component. The following is the sysObjectID OID tree for the BitStorm family. 1.3.6.1.4.1.1795 is the enterprise OID.

1.3.6.1.4.1.1795.1.14.17 BitStorm

1.3.6.1.4.1.1795.1.14.17.1 Stack

1.3.6.1.4.1.1795.1.14.17.1.1 Unit

SNMP Group

The SNMP group provides instrumentation and control of an SNMP entity.

Table C-3. SNMP Group OIDs (1 of 2)

Object	OID	Syntax	Access	Status	Supported
snmpInPkts	{ snmp 1}	Counter32	read-only	current	Yes
snmpOutPkts	{ snmp 2}	Counter32	read-only	obsolete	No
snmpInBadVersions	{ snmp 3}	Counter32	read-only	current	Yes
snmpInBadCommunity Names	{ snmp 4}	Counter32	read-only	current	Yes
snmpInBadCommunityUses	{ snmp 5 }	Counter32	read-only	current	Yes
snmpInASNParseErrs	{ snmp 6 }	Counter32	read-only	current	Yes
snmpInTooBigs	{ snmp 8 }	Counter	read-only	obsolete	No
snmpInNoSuchNames	{ snmp 9 }	Counter	read-only	obsolete	No
snmpInBadValues	{ snmp 10 }	Counter	read-only	obsolete	No
snmpInReadOnlys	{ snmp 11 }	Counter	read-only	obsolete	No
snmpInGenErrs	{ snmp 12 }	Counter	read-only	obsolete	No
snmpInTotalReqVars	{ snmp 13 }	Counter	read-only	obsolete	No
snmpInTotalSetVars	{ snmp 14 }	Counter	read-only	obsolete	No
snmpInGetRequests	{ snmp 15 }	Counter	read-only	obsolete	No
snmpInGetNexts	{ snmp 16 }	Counter	read-only	obsolete	No
snmpInSetRequests	{ snmp 17 }	Counter	read-only	obsolete	No
snmpInGetResponses	{ snmp 18 }	Counter	read-only	obsolete	No
snmpInTraps	{ snmp 19 }	Counter	read-only	obsolete	No
snmpOutTooBigs	{ snmp 20 }	Counter	read-only	obsolete	No
snmpOutNoSuchNames	{ snmp 21 }	Counter	read-only	obsolete	No
snmpOutBadValues	{ snmp 22 }	Counter	read-only	obsolete	No
snmpOutGenErrs	{ snmp 24 }	Counter	read-only	obsolete	No

Table C-3. SNMP Group OIDs (2 of 2)

Object	OID	Syntax	Access	Status	Supported
snmpOutGetRequests	{ snmp 25 }	Counter	read-only	obsolete	No
snmpOutGetNexts	{ snmp 26 }	Counter	read-only	obsolete	No
snmpOutSetRequests	{ snmp 27 }	Counter	read-only	obsolete	No
snmpOutGetResponses	{ snmp 28 }	Counter	read-only	obsolete	No
snmpOutTraps	{ snmp 29 }	Counter	read-only	obsolete	No
snnpEnableAuthenTraps	{ snmp 30 }	INTEGER	read-write	current	Yes
snmpSilentDrops	{ snmp 31 }	Counter32	read-only	current	Yes
snmpProxyDrops	{ snmp 31 }	Counter32	read-only	current	Yes

RFC1213-MIB

The RFC1213-MIB is defined in RFC 1213. It comprises the following groups:

Table C-4. MIB-II Groups Supported

Group	OID	Supported
system	mib-2 1	Yes, as in RFC 1907. See *System Group* on page C-5.
interfaces	mib-2 2	Yes, as in RFC 2863. See *IF-MIB* on page C-13.
at	mib-2 3	No
ip	mib-2 4	Yes, as in RFC 2011. See *IP-MIB* on page C-8.
icmp	mib-2 5	No
tcp	mib-2 6	No
udp	mib-2 7	No
egp	mib-2 8	No
cmot	mib-2 9	No
transmission	mib-2 10	No
snmp	mib-2 11	Yes, as in RFC 1907. See *SNMP Group* on page C-6.

PDN-HEADER-MIB

The PDN-HEADER-MIB defines the OIDs for all the other enterprise MIBs. The PDN-HEADER-MIB must be loaded before any of the other enterprise MIBS, else your MIB browser will generate an error message and not load the MIBS.

IP-MIB

The IP-MIB is defined in RFC 2011. The IP group is supported. This MIB applies to the management processor as an IP host in the management network, and not to the unit's handling of user data.

IP Group

The IP group include objects for managing implementations of the Internet Protocol.

Table C-5. IP Group

Object	OID	Syntax	Access	Status	Supported
ipForwarding	{ ip 1 }	INTEGER	read-write	current	Yes
ipDefaulTTL	{ ip 2 }	INTEGER	read-write	current	Yes
ipInReceives	{ ip 3 }	Counter32	read-only	current	Yes
ipInHdrErrors	{ ip 4 }	Counter32	read-only	current	No
ipInAddrErrors	{ ip 5 }	Counter32	read-only	current	No
ipForwDatagrams	{ ip 6 }	Counter32	read-only	current	No
ipInUnknownProtos	{ ip 7 }	Counter32	read-only	current	No
ipInDiscards	{ ip 8 }	Counter32	read-only	current	No
ipInDelivers	{ ip 9 }	Counter32	read-only	current	No
ipOutRequests	{ ip 10 }	Counter32	read-only	current	No
ipOutDiscards	{ ip 11 }	Counter32	read-only	current	No
ipOutNoRoutes	{ ip 12 }	Counter32	read-only	current	No
ipReasmTimeout	{ ip 13 }	Integer32	read-only	current	No
ipReasmReqds	{ ip 14 }	Counter32	read-only	current	No
ipReasmOKs	{ ip 15 }	Counter32	read-only	current	No
ipReasmFails	{ ip 16 }	Counter32	read-only	current	No
ipFragOKs	{ ip 17 }	Counter32	read-only	current	No
ipFragFails	{ ip 18 }	Counter32	read-only	current	No
ipFragCreates	{ ip 19 }	Counter32	read-only	current	No
ipAddrTable	{ ip 20 }	Sequence of ipAddrEntry	not-accessible	current	Yes

ENTITY-MIB

The ENTITY-MIB is defined in RFC 2737. It comprises the following objects:

Table C-6. Entity MIB

Object	OID	Syntax	Access	Status	Supported
entPhysicalTable	{ entityPhysical 1 }	Sequence of entPhysical Entry	not-accessible	current	Yes
entLogicalTable	{ entityLogical 1 }	Sequence of entLogical Entry	not-accessible	current	No
entLPMappingTable	{ entityMapping 1 }	Sequence of entLPMapping Entry	not-accessible	current	No
entAliasMappingTable	{ entityMapping 2 }	Sequence of entAlias MappingEntry	not-accessible	current	Yes
entPhysicalContainsTable	{ entityMapping 3 }	Sequence of entPhysical ContainsEntry	not-accessible	current	Yes
entLastChangeTime	{ entityGeneral 1 }	TimeStamp	read-only	current	Yes

entPhysicalIndex

The entPhysicalIndex identifies a physical feature. It is encoded as a 10-digit decimal number in the form of:

R R C C S S L P P P

Where:

- **RR** – Is a reserved area implied to be 0
- **CC** – Is the chassis number in the range of 0–99
- **SS** – Is a slot number (always 00, denoting Not Applicable)
- **L** – Is a layer number in the range of 0–9
- **PPP** – Is a port number in the range of 0–999

Table C-7. entPhysicalIndex Values (1 of 2)

Entity	Physical Index RR CC SS L PPP
Stack	00 00 00 0 001
Chassis	00 *cc* 00 0 000
Main Card	00 *cc* 00 0 001
Child Card	00 *cc* 00 0 002
Management Module	00 *cc* 00 0 003
Console Port	00 *cc* 00 0 050
Modem Port	00 *cc* 00 0 051
Rear Fan	00 *cc* 00 0 101
Center Fan	00 *cc* 00 0 102
Front Fan	00 *cc* 00 0 103
Temperature Sensor	00 *cc* 00 0 201
Management Processor	00 *cc* 00 0 300
Uplink Processor	00 *cc* 00 0 301
Security Processor	00 *cc* 00 0 302
Port Processor 1	00 *cc* 00 0 310
Port Processor 2	00 *cc* 00 0 311
Port Processor 3	00 *cc* 00 0 312
Port Processor 4	00 *cc* 00 0 313
Port Processor 5	00 *cc* 00 0 314

Table C-7. entPhysicalIndex Values (2 of 2)

Entity	Physical Index RR CC SS L PPP
Port Processor 6	00 *cc* 00 0 315
Main Card PLD	00 *cc* 00 0 501
Management Processor PLD	00 *cc* 00 0 502
V.35 Processor PLD	00 *cc* 00 0 503
ADSL Port *y*	00 *cc* 00 1 *yyy* (where *yyy* = 1–48 for DSL ports 1–48)
Ethernet Management Port	00 *cc* 00 1 060
Ethernet Downlink Port	00 *cc* 00 1 061
Ethernet Uplink Port	00 *cc* 00 1 062
Uplink Port	00 *cc* 00 1 070

entPhysicalVendorType

Table C-8. entPhysicalVendorType Values

Entity	OID	Name
ADSL Port *y*	1.3.6.1.4.1.1795.1.14.17.5.4	ips-adsl-port
Center Fan	1.3.6.1.4.1.1795.1.14.17.6.1	ips-fan
Chassis	1.3.6.1.4.1.1795.1.14.17.2.1	ips-4821
Child Card	1.3.6.1.4.1.1795.1.14.17.3.2	ips-24port-adsl-child-card
Console Port	1.3.6.1.4.1.1795.1.14.17.5.2	ips-rs232-dce-port
Ethernet Downlink Port	1.3.6.1.4.1.1795.1.14.17.5.5	ips-ethernet-port
Ethernet Management Port	1.3.6.1.4.1.1795.1.14.17.5.5	ips-ethernet-port
Ethernet Uplink Port	1.3.6.1.4.1.1795.1.14.17.5.5	ips-ethernet-port
Front Fan	1.3.6.1.4.1.1795.1.14.17.6.1	ips-fan
Main Card	1.3.6.1.4.1.1795.1.14.17.3.1	ips-24port-adsl-main-card
Main Card PLD	1.3.6.1.4.1.1795.1.14.17.6.4	ips-pld
Management Processor	1.3.6.1.4.1.1795.1.14.17.6.3	ips-processor
Management Processor PLD	1.3.6.1.4.1.1795.1.14.17.6.4	ips-pld
Model 4800 Management Module	1.3.6.1.4.1.1795.1.14.17.4.1	ips-mgmt-no-wan
Model 4804 Management Module	1.3.6.1.4.1.1795.1.14.17.4.2	ips-mgmt-with-v35x21wan
Modem Port	1.3.6.1.4.1.1795.1.14.17.5.1	ips-rs232-dte-port
Port Processor 1	1.3.6.1.4.1.1795.1.14.17.6.3	ips-processor
Port Processor 2	1.3.6.1.4.1.1795.1.14.17.6.3	ips-processor
Port Processor 3	1.3.6.1.4.1.1795.1.14.17.6.3	ips-processor
Port Processor 4	1.3.6.1.4.1.1795.1.14.17.6.3	ips-processor
Port Processor 5	1.3.6.1.4.1.1795.1.14.17.6.3	ips-processor
Port Processor 6	1.3.6.1.4.1.1795.1.14.17.6.3	ips-processor
PPP Uplink Port	1.3.6.1.4.1.1795.1.14.17.5.3	ips-v35-dte-port
Rear Fan	1.3.6.1.4.1.1795.1.14.17.6.1	ips-fan
Security Processor	1.3.6.1.4.1.1795.1.14.17.6.3	ips-processor
Stack	1.3.6.1.4.1.1795.1.14.17.1.1	ips-4800
Temperature Sensor	1.3.6.1.4.1.1795.1.14.17.6.2	ips-temperature-sensor
Uplink Processor	1.3.6.1.4.1.1795.1.14.17.6.3	ips-processor
V.35 Processor PLD	1.3.6.1.4.1.1795.1.14.17.6.4	ips-pld

IF-MIB

The IF-MIB is defined in RFC 2863. It comprises the following objects:

Table C-9. Interfaces Group

Object	OID	Syntax	Access	Status	Supported
ifNumber	{ interfaces 1 }	Integer32	read-only	current	Yes
ifTable	{ interfaces 3 }	Sequence of ifEntry	not-accessible	current	Yes
ifXTable	{ ifMIBObjects 1 }	Sequence of ifXEntry	not-accessible	current	Yes
ifStackTable	{ ifMIBObjects 2 }	Sequence of ifStackEntry	not-accessible	current	Yes
ifTestTable	{ ifMIBObjects 3 }	Sequence of ifTestEntry	not-accessible	deprecated	No
ifRcvAddressTable	{ ifMIBObjects 4 }	Sequence of ifRcvAddressTable	not-accessible	current	Yes
ifTableLastChange	{ ifMIBObjects 5 }	TimerTicks	read-only	current	Yes
ifStackLastChange	{ ifMIBObjects 6 }	TimerTicks	read-only	current	Yes

Interfaces

The following interfaces are defined for the BitStorm 4800:

Table C-10. Interfaces

Interface	Location	Quantity
Console Port	External	1 per Stack
Modem Port	External	1 per Stack
Ethernet Management Port (MGMT)	External	1 per Chassis
Ethernet Downlink Port (GigE Downlink) ■ 10/100/1000 Base T ■ 10/100/1000 Small Form-factor Pluggable	External	1 per Chassis
Ethernet Uplink Port (GigE Uplink) ■ 10/100/1000 Base T ■ 10/100/1000 Small Form-factor Pluggable	External	1 per Chassis
IP/PPP Layer 3 Uplink Port or Ethernet/PPP Layer 2 Uplink Port ■ V.35 ■ EIA-530-A ■ X.21	External	1 Port per Stack
PPP Uplink HDLC Interface	External	1 per Stack
PPP Uplink PPP Interface	External	1 per Stack
PPP Uplink Ethernet Interface	Internal	1 per Stack
Layer 2 Switch PPP Uplink Processor Ethernet Interface	Internal	1 per Stack
ADSL Ports	External	24 or 48 per Unit
ATM Interfaces	External	24 or 48 per Unit
Port Processor Ethernet Interfaces	External	24 or 48 per Unit
Port Processor L2 Switch Ethernet Interfaces	Internal	6 per Unit
L2 Switch Port Processor Ethernet Interfaces	Internal	6 per Unit
Management Processor L2 Switch Ethernet Interface	Internal	1 per Stack
L2 Switch Management Processor Ethernet Interface	Internal	1 per Stack

ifTable

All objects except deprecated objects in the ifTable are supported.

Table C-11. ifTable Objects

Object	OID	Syntax	Access	Status	Supported
ifIndex	{ ifEntry 1 }	Interface Index	read-only	current	Yes
ifDescr	{ ifEntry 2 }	DisplayString	read-only	current	Yes
ifType	{ ifEntry 3 }	IANAifType	read-only	current	Yes
ifMtu	{ ifEntry 4 }	Integer32	read-only	current	Yes
ifSpeed	{ ifEntry 5 }	Gauge32	read-only	current	Yes
ifPhysAddress	{ ifEntry 6 }	PhysAddress	read-only	current	Yes
ifAdminStatus	{ ifEntry 7 }	INTEGER	read-write	current	Yes
ifOperStatus	{ ifEntry 8 }	INTEGER	read-only	current	Yes
ifLastChange	{ ifEntry 9 }	TimerTicks	read-only	current	Yes
ifInOctets	{ ifEntry 10 }	Counter32	read-only	current	Yes
ifInUcastPkts	{ ifEntry 11 }	Counter32	read-only	current	Yes
ifInNUcastPkts	{ ifEntry 12 }	Counter32	read-only	deprecated	No
ifInDiscards	{ ifEntry 13 }	Counter32	read-only	current	Yes
ifInErrors	{ ifEntry 14 }	Counter32	read-only	current	Yes
ifInUnknownProtos	{ ifEntry 15 }	Counter32	read-only	current	Yes
ifOutOctets	{ ifEntry 16 }	Counter32	read-only	current	Yes
ifOutUcastPkts	{ ifEntry 17 }	Counter32	read-only	current	Yes
ifOutNUcastPkts	{ ifEntry 18 }	Counter32	read-only	deprecated	N
ifOutDiscards	{ ifEntry 19 }	Counter32	read-only	current	Yes
ifOutErrors	{ ifEntry 20 }	Counter32	read-only	current	Yes
ifOutQLen	{ ifEntry 21 }	Counter32	read-only	deprecated	No
ifSpecific	{ ifEntry 22 }	Counter32	read-only	deprecated	No

ifIndex

The ifIndex identifies an interface. It is encoded as a 10-digit decimal number in the form of:

R R C C S S L P P P

Where:

- **RR** – Is a reserved area implied to be 0
- **CC** – Is the chassis number in the range of 0–99
- **SS** – Is a slot number (always 00, denoting Not Applicable)
- **L** – Is a layer number in the range of 0–9
- **PPP** – Is a port number in the range of 0–999

See Table C-12, Layer and Port/Interface Number Assignments. Zero in any field denotes that it is not applicable.

Table C-12. Layer and Port/Interface Number Assignments

Int/Ext	Interface	Layer (L)	Port/Interface (PPP)
External	Console Port	0	50
External	Modem Port	0	51
External	Ethernet Management Port	1	60
External	Ethernet Downlink Port	1	61
External	Ethernet Uplink Port	1	62
External	Ethernet/PPP Layer 2 Uplink Port (V.35/X.21 port)	1	70
External	PPP Uplink HDLC Interface (V.35/X.21 port)	2	70
External	PPP Uplink PPP Interface (V.35/X.21 port)	3	70
Internal	Uplink Processor Ethernet Interface (V.35/X.21 port)	1	80
Internal	Layer 2 Switch PPP Uplink Processor Ethernet Interface (V.35/X.21 port)	1	81
External	ADSL Ports	1	1–48
External	ATM Interfaces	2	1–48
External	Port Processor Ethernet Interfaces	3	1–48
Internal	Port Processor L2 Switch Ethernet Interfaces	1	91–96
Internal	L2 Switch Port Processor Ethernet Interfaces	1	101–106
Internal	Management Processor L2 Switch Ethernet Interface	1	110
Internal	L2 Switch Management Processor Ethernet Interface	1	111

ifDescr

The ifDescr is a text string containing information about the interface.

Some values in the ifDescr contain “Unit *n*.” The term “Unit” is a synonym for a chassis. In Release 1, there is only one chassis per stack, so the Unit number is always 1. The Unit or chassis number is identical with the chassis number (CC) in the ifIndex.

Table C-13. ifDescr

Location	Interface	Value
External	Console Port	Console Port
External	Modem Port	MODEM Port
External	Ethernet Management Port	Unit *n* Ethernet Management Port
External	Ethernet Downlink Port	Unit *n* Downlink GigE Port
External	Ethernet Uplink Port	Unit *n* Uplink GigE Port
External	Ethernet/PPP Layer 2 Uplink Port	PPP Uplink Port
External	PPP Uplink HDLC Interface	PPP Uplink HDLC Interface
External	PPP Uplink PPP Interface	PPP Uplink PPP Interface
Internal	PPP Uplink Ethernet Interface	PPP Ul En Interface
Internal	Layer 2 Switch PPP Uplink Processor Ethernet Interface	L2 Sw PPP Ul En Interface
External	ADSL Ports	Unit *n* ADSL Port 1 – Unit *n* ADSL Port 48
External	ATM Interfaces	Unit *n* ATM Interface 1 – Unit *n* ATM Interface 48
External	Port Processor Ethernet Interfaces	Unit *n* PP En Interface 1 – Unit *n* PP En Interface 48
Internal	Port Processor L2 Switch Ethernet Interfaces	Unit *n* PP L2 Sw En Interface 1 – Unit *n* PP L2 Sw En Interface 6
Internal	L2 Switch Port Processor Ethernet Interfaces	Unit *n* L2 Sw PP En Interface 1 – Unit *n* L2 Sw PP En Interface 6
Internal	Management Processor L2 Switch Ethernet Interface	Mgmt Processor L2 Sw En Interface
Internal	L2 Switch Management Processor Ethernet Interface	L2 Switch Mgmt Processor En Interface

ifType

The ifType is the numeric interface type as defined by the Internet Assigned Numbers Authority (IANA).

Table C-14. ifType

Location	Interface	Value
External	Console Port	rs232(33)
External	Modem Port	rs232(33)
External	Ethernet Management Port	ethernetCsmacd(6)
External	Ethernet Downlink Port	ethernetCsmacd(6)
External	Ethernet Uplink Port	ethernetCsmacd(6)
External	IP/PPP Layer 3 Uplink Port or Ethernet/PPP Layer 2 Uplink Port	v35(45)
External	PPP Uplink HDLC Interface	hdlc(118)
External	PPP Uplink PPP Interface	ppp(23)
Internal	PPP Uplink Ethernet Interface	ethernetCsmacd(6)
Internal	Layer 2 Switch PPP Uplink Processor Ethernet Interface	ethernetCsmacd(6)
External	ADSL Ports	adsl(94)
External	ATM Interfaces	atmVirtual(149)
External	Port Processor Ethernet Interfaces	ethernetCsmacd(6)
Internal	Port Processor L2 Switch Ethernet Interfaces	ethernetCsmacd(6)
Internal	L2 Switch Port Processor Ethernet Interfaces	ethernetCsmacd(6)
Internal	Management Processor L2 Switch Ethernet Interface	ethernetCsmacd(6)
Internal	L2 Switch Management Processor Ethernet Interface	ethernetCsmacd(6)

ifMtu

The ifMtu is the size of the largest packet which can be sent or received on the interface, specified in octets. For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface.

Table C-15. ifMtu

Location	Interface	Value
External	Console Port	0
External	Modem Port	0
External	Ethernet Management Port	1500
External	Ethernet Downlink Port	1500
External	Ethernet Uplink Port	1500
External	IP/PPP Layer 3 Uplink Port or Ethernet/PPP Layer 2 Uplink Port	1504
External	PPP Uplink HDLC Interface	1504
External	PPP Uplink PPP Interface	1502
Internal	PPP Uplink Ethernet Interface	1500
Internal	Layer 2 Switch PPP Uplink Processor Ethernet Interface	1500
External	ADSL Ports	53
External	ATM Interfaces	53
External	Port Processor Ethernet Interfaces	1500
Internal	Port Processor L2 Switch Ethernet Interfaces	1500
Internal	L2 Switch Port Processor Ethernet Interfaces	1500
Internal	Management Processor L2 Switch Ethernet Interface	1500
Internal	L2 Switch Management Processor Ethernet Interface	1500

ifAdminStatus

The desired state of the interface:

- **up(1)** – The interface is operational and operational packets can be passed
- **down(2)** – When a managed system is initialized, all interfaces start with ifAdminStatus in the down(2) state
- **testing(3)** – The interface is in a test state and no operational packets can be passed

Table C-16. ifAdminStatus

Location	Interface	Value
External	Console Port	Only valid value is up(1)
External	Modem Port	Only valid value is up(1)
External	Ethernet Management Ports	Only valid value is up(1)
External	Ethernet Downlink Ports	Only valid values are up(1) or down(2)
External	Ethernet Uplink Ports	Only valid values are up(1) or down(2)
External	Ethernet/PPP Layer 2 Uplink Port	Only valid values are up(1) or testing(3)
External	PPP Uplink HDLC Interface	Only valid value is up(1)
External	PPP Uplink PPP Interface	Only valid value is up(1)
Internal	PPP Uplink Ethernet Interface	Only valid value is up(1)
Internal	Layer 2 Switch PPP Uplink Processor Ethernet Interface	Only valid value is up(1)
External	ADSL Ports	Only valid value is up(1), down(2), or testing(3)
External	ATM Interfaces	Only valid value is up(1)
External	Port Processor Ethernet Interfaces	Only valid value is up(1)
Internal	Port Processor L2 Switch Ethernet Interfaces	Only valid value is up(1)
Internal	L2 Switch Port Processor Ethernet Interfaces	Only valid value is up(1)
Internal	Management Processor L2 Switch Ethernet Interface	Only valid value is up(1)
Internal	L2 Switch Management Processor Ethernet Interface	Only valid value is up(1)

ifOperStatus

The ifOperStatus is the current operational state of the interface.

- **up(1)** – Ready to pass packets
- **down(2)** – ifAdminStatus is down(2)
- **testing(3)** – The interface is in a test state and no packets can be passed
- **unknown(4)** – Status can not be determined
- **dormant(5)** – The interface is awaiting some external action
- **notPresent(6)** – Some component is missing
- **lowerLayerDown(7)** – Down due to the state of a lower-layer interface

Table C-17. ifOperStatus

Location	Interface	Value
External	Console Port	The port is always up(1)
External	Modem Port	The port is always up(1)
External	Ethernet Management Ports	Any value except down(2)
External	Ethernet Downlink Ports	Any value supported by the syntax
External	Ethernet Uplink Ports	Any value supported by the syntax
External	Ethernet/PPP Layer 2 Uplink Port	Any value except down(2)
External	PPP Uplink HDLC Interface	Any value except down(2)
External	PPP Uplink PPP Interface	Any value except down(2)
Internal	PPP Uplink Ethernet Interface	Any value except down(2)
Internal	Layer 2 Switch PPP Uplink Processor Ethernet Interface	Any value except down(2)
External	ADSL Ports	Any value supported by the syntax
External	ATM Interfaces	Any value supported by the syntax
External	Port Processor Ethernet Interfaces	Any value except down(2)
Internal	Port Processor L2 Switch Ethernet Interfaces	Any value except down(2)
Internal	L2 Switch Port Processor Ethernet Interfaces	Any value except down(2)
Internal	Management Processor L2 Switch Ethernet Interface	Any value except down(2)
Internal	L2 Switch Management Processor Ethernet Interface	Any value except down(2)

ifXTable

All objects in ifXTable are supported except ifHighSpeed.

ifName

The ifName is a text string denoting the name of the interface.

Table C-18. ifName

Location	Interface	Value
External	Console Port	CONSOLE
External	Modem Port	MODEM
External	Ethernet Management Port	MGMT
External	Ethernet Downlink Port	Downlink GigE
External	Ethernet Uplink Port	Uplink GigE
External	Ethernet/PPP Layer 2 Uplink Port	IP/PPP Uplink
External	PPP Uplink HDLC Interface	PPP Uplink HDLC Interface
External	PPP Uplink PPP Interface	PPP Uplink PPP Interface
Internal	PPP Uplink Ethernet Interface	PPP Uplink En Interface
Internal	Layer 2 Switch PPP Uplink Processor Ethernet Interface	L2 Sw PPP En Interface
External	ADSL Ports	ADSL Port
External	ATM Interfaces	ATM Interface
External	Port Processor Ethernet Interfaces	PP En Interface
Internal	Port Processor L2 Switch Ethernet Interfaces	PP L2 Sw En Interface
Internal	L2 Switch Port Processor Ethernet Interfaces	L2 Sw PP En Interface
Internal	Management Processor L2 Switch Ethernet Interface	Mgmt UP L2 Sw En Interface
Internal	L2 Switch Management Processor Ethernet Interface	L2 Sw Mgmt UP En Interface

ifLinkUpDownTrapEnable

The ifLinkUpDownTrapEnable object indicates whether linkUp/linkDown traps should be generated for this interface.

- **enabled(1)** – linkUp/LinkDown traps are generated
- **disabled(2)** – linkUp/LinkDown traps are not generated

Table C-19. ifLinkUpDownTrapEnable

Location	Interface	Value
External	Console Port	Only valid value is disabled(2)
External	Modem Port	Only valid value is disabled(2)
External	Ethernet Management Port	Only valid value is disabled(2)
External	Ethernet Downlink Port	enabled(1) or disabled(2)
External	Ethernet Uplink Port	enabled(1) or disabled(2)
External	Ethernet/PPP Layer 2 Uplink Port	enabled(1) or disabled(2)
External	PPP Uplink HDLC Interface	Only valid value is disabled(2)
External	PPP Uplink PPP Interface	Only valid value is disabled(2)
Internal	PPP Uplink Ethernet Interface	Only valid value is disabled(2)
Internal	Layer 2 Switch PPP Uplink Processor Ethernet Interface	Only valid value is disabled(2)
External	ADSL Ports	enabled(1) or disabled(2)
External	ATM Interfaces	Only valid value is disabled(2)
External	Port Processor Ethernet Interfaces	Only valid value is disabled(2)
Internal	Port Processor L2 Switch Ethernet Interfaces	Only valid value is disabled(2)
Internal	L2 Switch Port Processor Ethernet Interfaces	Only valid value is disabled(2)
Internal	Management Processor L2 Switch Ethernet Interface	Only valid value is disabled(2)
Internal	L2 Switch Management Processor Ethernet Interface	Only valid value is disabled(2)

ifConnectorPresent

The ifConnectorPresent object declares whether there is a physical connector.

- **true(1)** – The interface sublayer has a physical connector
- **false(2)** – The interface sublayer has no physical connector

Table C-20. ifConnectorPresent

Location	Interface	Value
External	Console Port	true(1)
External	Modem Port	true(1)
External	Ethernet Management Port	true(1)
External	Ethernet Downlink Port	true(1)
External	Ethernet Uplink Port	true(1)
External	Ethernet/PPP Layer 2 Uplink Port	true(1)
External	PPP Uplink HDLC Interface	false(2)
External	PPP Uplink PPP Interface	false(2)
Internal	PPP Uplink Ethernet Interface	false(2)
Internal	Layer 2 Switch PPP Uplink Processor Ethernet Interface	false(2)
External	ADSL Ports	true(1)
External	ATM Interfaces	false(2)
External	Port Processor Ethernet Interfaces	false(2)
Internal	Port Processor L2 Switch Ethernet Interfaces	false(2)
Internal	L2 Switch Port Processor Ethernet Interfaces	false(2)
Internal	Management Processor L2 Switch Ethernet Interface	false(2)
Internal	L2 Switch Management Processor Ethernet Interface	false(2)

ifStackTable

The ifStackTable shows the relationships between the multiple sub-layers of network interfaces. All objects are supported.

Table C-21. ifStackTable Values (1 of 2)

	Values*	
	CC SSL PPP CC SSL xxx** CC SSL yyy*****	
Interface	**ifStackHigherLayer**	**ifStackLowerLayer**
Console Port	CC SS0 050	0
	0	CC SS0 050
Modem Port	CC SS0 051	0
	0	CC SS0 051
Ethernet Management Port	CC SS1 060	0
	0	CC SS1 060
Ethernet Downlink Port	CC SS1 061	0
	0	CC SS1 061
Ethernet Uplink Port	CC SS1 062	0
	0	CC SS1 062
Ethernet/PPP Layer 2 Uplink Port	CC SS1 070	0
	CC SS2 070	CC SS1 070
	CC SS3 070	CC SS2 070
	0	CC SS3 070
PPP Uplink Ethernet Interface	CC SS1 080	0
	0	CC SS1 080
Layer 2 Switch PPP Uplink Processor Ethernet Interface	CC SS1 081	0
	0	CC SS1 081
Port Processor	CC SS1 xxx	0
	CC SS2 xxx	CC SS1 xxx
	CC SS3 xxx	CC SS2 xxx
	0	CC SS3 xxx

* See *ifIndex* on page C-16 for a description of the ifIndex encoding scheme. Spaces are added and leading zeroes are dropped for clarification.

** xxx refers to the associated ADSL port number in a stack (001–048)

*** yyy refers to the associated Port Processor number in the stack (001–006)

Table C-21. ifStackTable Values (2 of 2)

	Values*	
	CC SSL PPP CC SSL xxx** CC SSL yyy*****	
Interface	**ifStackHigherLayer**	**ifStackLowerLayer**
Port Processor L2 Switch Ethernet Interfaces	CC SS1 yyy	0
	0	CC SS1 yyy
L2 Switch Port Processor Ethernet Interfaces	CC SS1 yyy	0
	0	CC SS1 yyy
Management Processor L2 Switch Ethernet Interface	CC SS1 110	0
	0	CC SS1 110
L2 Switch Management Processor Ethernet Interface	CC SS1 111	0
	0	CC SS1 111

* See *ifIndex* on page C-16 for a description of the ifIndex encoding scheme. Spaces are added and leading zeroes are dropped for clarification.

** xxx refers to the associated ADSL port number in a stack (001–048)

*** yyy refers to the associated Port Processor number in the stack (001–006)

ATM-MIB

The ATM-MIB is defined in RFC 2515. It comprises the following objects:

Table C-22. ATM MIB

Object	OID	Syntax	Access	Status	Supported
atmInterfaceConf Table	{ atmMIBObjects 2 }	Sequence of atmInterfaceConfEntry	not-accessible	current	No
atmInterfaceDs3Plcp Table	{ atmMIBObjects 3 }	Sequence of atmInterfaceDs3PlcpEntry	not-accessible	current	No
atmInterfaceTCTable	{ atmMIBObjects 4 }	Sequence of atmInterfaceTCEntry	not-accessible	current	Yes
atmTrafficDescr ParamTable	{ atmMIBObjects 5 }	Sequence of atmTrafficDescrParamEntry	not-accessible	current	No
atmVplTable	{ atmMIBObjects 6 }	Sequence of atmVplEntry	not-accessible	current	No
atmVclTable	{ atmMIBObjects 7 }	Sequence of atmVclEntry	not-accessible	current	Yes
atmVpCrossConnect IndexNext	{ atmMIBObjects 8 }	INTEGER	read-only	current	No
atmVpCrossConnect Table	{ atmMIBObjects 9 }	Sequence of atmVpCrossConnectEntry	not-accessible	current	No
atmVcCrossConnect IndexNext	{ atmMIBObjects 10 }	INTEGER	read-only	current	No
atmVcCrossConnect Table	{ atmMIBObjects 11 }	Sequence of atmVcCrossConnectEntry	not-accessible	current	No
aal5VccTable	{ atmMIBObjects 12 }	Sequence of aal5VccTable	not-accessible	current	No
atmTrafficDescr ParamIndexNext	{ atmMIBObjects 13 }	INTEGER	not-accessible	current	No

atmInterfaceTCTable

The ATM Interface TC Sublayer Table contains Transmission Convergence sublayer configuration and state parameters.

Table C-23. atmInterfaceTCTable

Object	OID	Syntax	Access	Status	Supported
atmInterfaceOCDEvents	{ atmInterfaceTCEntry 1 }	Counter32	read-only	current	Yes
atmInterfaceTCAlarm State	{ atmInterfaceTCEntry 2 }	INTEGER	read-only	current	Yes

atmVclTable

The ATM Interface VCL Table contains configuration and state information of a bidirectional Virtual Channel Link at an ATM interface.

Table C-24. atmVclTable

Object	OID	Syntax	Access	Status	Supported
atmVclVpi	{ atmVclEntry 1 }	AtmVpIdentifier	not-accessible	current	Yes
atmVclVci	{ atmVclEntry 2 }	AtmVpIdentifier	not-accessible	current	Yes
atmVclAdminStatus	{ atmVclEntry 3 }	AtmVorXAdminStatus	read-create	current	Yes
atmVclOperStatus	{ atmVclEntry 4 }	AtmVorXOperStatus	read-only	current	Yes
atmVclLastChange	{ atmVclEntry 5 }	AtmVorXLastChange	read-only	current	Yes
atmVclReceiveTraffic DescrIndex	{ atmVclEntry 6 }	AtmTrafficDescrParamIndex	read-create	current	No
atmVclTransmitTraffic DescrIndex	{ atmVclEntry 7 }	AtmTrafficDescrParamIndex	read-create	current	No
atmVccAalType	{ atmVclEntry 8 }	INTEGER	read-create	current	Yes
atmVccAal5Cpcs TransmitSduSize	{ atmVclEntry 9 }	INTEGER	read-create	current	Yes
atmVccAal5Cpcs ReceiveSduSize	{ atmVclEntry 10 }	INTEGER	read-create	current	Yes
atmVccAal5EncapsType	{ atmVclEntry 11 }	INTEGER	read-create	current	Yes
atmVclCrossConnect Identifier	{ atmVclEntry 12 }	INTEGER	read-only	current	No
atmVclRowStatus	{ atmVclEntry 13 }	RowStatus	read-create	current	Yes
atmVclCastType	{ atmVclEntry 14 }	AtmConnCastType	read-create	current	No
atmVclConnKind	{ atmVclEntry 15 }	AtmConnKind	read-create	current	No

ATM-FORUM-SNMP-M4-MIB

The ATM-FORUM-SNMP-M4-MIB is defined in the ATM Forum specification AF-NM-0095.001, “SNMP M4 Network Element View MIB.”

Only the atmfM4TcACellScrambling object, part of the atmfM4TcAdapterTable, is supported.

Table C-25. atmfM4PhysPathTpTable

Object	OID	Syntax	Access	Status	Supported
atmfM4TcACellScrambling	{ atmfM4TcAdapterEntry 1 }	TruthValue	read-write	current	Yes

RS-232-MIB

The RS-232-Like MIB is defined in RFC 1659. In the BitStorm 4800, it applies to the following interfaces:

- Console
- Modem
- PPP Uplink (if used)

It comprises the following objects:

Table C-26. RS-232 MIB

Object	OID	Syntax	Access	Status	Supported
rs232Number	{ rs232 1 }	Integer32	read-only	current	Yes
rs232PortTable	{ rs232 2 }	Sequence of rs232PortEntry	not-accessible	current	Yes
rs232AsyncPortTable	{ rs232 3 }	Sequence of rs232AyncPortEntry	not-accessible	current	Yes
rs232SyncPortTable	{ rs232 4 }	Sequence of rs232SyncPortEntry	not-accessible	current	Yes
rs232InSigTable	{ rs232 5 }	Sequence of rs232InSigEntry	not-accessible	current	Yes
rs232OutSigTable	{ rs232 6 }	Sequence of rs232OutSigEntry	not-accessible	current	Yes

rs232Number

The rs232Number object is 2 or 3, depending on whether the PPP uplink is used.

rs232PortTable

The rs232PortTable contains status and descriptions of the ports.

Table C-27. rs232PortTable

Object	OID	Syntax	Access	Status	Supported
rs232PortIndex	{ rs232PortEntry 1 }	InterfaceIndex	read-only	current	Yes
rs232PortType	{ rs232PortEntry 2 }	INTEGER	read-only	current	Yes
rs232PortInSigNumber	{ rs232PortEntry 3 }	Integer32	read-only	current	Yes
rs232PortOutSigNumber	{ rs232PortEntry 4 }	Integer32	read-only	current	Yes
rs232PortInSpeed	{ rs232PortEntry 5 }	Integer32	read-write	current	Yes
rs232PortOutSpeed	{ rs232PortEntry 6 }	Integer32	read-write	current	Yes
rs232PortInFlowType	{ rs232PortEntry 7 }	INTEGER	read-write	current	Yes
rs232PortOutFlowType	{ rs232PortEntry 8 }	INTEGER	read-write	current	Yes

rs232AsyncPortTable

The rs232AsyncPortTable contains status and descriptions of asynchronous ports (Console and Modem).

Table C-28. rs232AsyncPortTable

Object	OID	Syntax	Access	Status	Supported
rs232AsyncPortIndex	{ rs232AsyncPortEntry 1 }	InterfaceIndex	read-only	current	Yes
rs232AsyncPortBits	{ rs232AsyncPortEntry 2 }	INTEGER	read-write	current	Yes
rs232AsyncPortStopBits	{ rs232AsyncPortEntry 3 }	INTEGER	read-write	current	Yes
rs232AsyncPortParity	{ rs232AsyncPortEntry 4 }	INTEGER	read-write	current	Yes
rs232AsyncPortAutobaud	{ rs232AsyncPortEntry 5 }	INTEGER	read-write	current	Yes
rs232AsyncPortParityErrs	{ rs232AsyncPortEntry 6 }	Counter32	read-only	current	No
rs232AsyncPortFramingErrs	{ rs232AsyncPortEntry 7 }	Counter32	read-only	current	No
rs232AsyncPortOverrunErrs	{ rs232AsyncPortEntry 8 }	Counter32	read-only	current	No

rs232SyncPortTable

The rs232SyncPortTable contains status and descriptions of the synchronous port (PPP Uplink).

Table C-29. rs232SyncPortTable

Object	OID	Syntax	Access	Status	Supported
rs232SyncPortIndex	{ rs232SyncPortEntry 1 }	InterfaceIndex	read-only	current	Yes
rs232SyncPortClockSource	{ rs232SyncPortEntry 2 }	INTEGER	read-write	current	Yes
rs232SyncPortFrame CheckErrs	{ rs232SyncPortEntry 3 }	Counter32	read-only	current	No
rs232SyncPortTransmit UnderrunErrs	{ rs232SyncPortEntry 4 }	Counter32	read-only	current	No
rs232SyncPortReceiveOverrun Errs	{ rs232SyncPortEntry 5 }	Counter32	read-only	current	No
rs232SyncPortInterrupted Frames	{ rs232SyncPortEntry 6 }	Counter32	read-only	current	No
rs232SyncPortAbortedFrames	{ rs232SyncPortEntry 7 }	Counter32	read-only	current	No
rs232SyncPortRole	{ rs232SyncPortEntry 8 }	INTEGER	read-write	current	Yes
rs232SyncPortEncoding	{ rs232SyncPortEntry 9 }	INTEGER	read-write	current	Yes
rs232SyncPortRTSControl	{ rs232SyncPortEntry 10 }	INTEGER	read-write	current	Yes
rs232SyncPortRTSCTSDelay	{ rs232SyncPortEntry 11 }	Integer32	read-write	current	No
rs232SyncPortMode	{ rs232SyncPortEntry 12 }	INTEGER	read-write	current	Yes
rs232SyncPortIdlePattern	{ rs232SyncPortEntry 13 }	INTEGER	read-write	current	No
rs232SyncPortMinFlags	{ rs232SyncPortEntry 14 }	Integer32	read-write	current	No

Ethernet-Like MIB

The Ethernet-Like MIB is defined in RFC 2665. It comprises the following objects:

Table C-30. Ethernet-like MIB

Object	OID	Syntax	Access	Status	Supported
dot3StatsTable	{ dot3 2 }	Sequence of dot3StatsEntry	not-accessible	current	Yes
dot3CollTable	{ dot3 5 }	Sequence of dot3CollEntry	not-accessible	current	No
dot3ControlTable	{ dot3 9 }	Sequence of dot3ControlEntry	not-accessible	current	No
dot3PauseTable	{ dot3 10 }	Sequence of dot3PauseEntry	not-accessible	current	Yes
dot3Tests	{ dot3 6 }	N/A	not-accessible	current	No
dot3Errors	{ dot3 7 }	N/A	not-accessible	current	No

dot3StatsTable

The dot3StatsTable contains statistics for a group of Ethernet devices.

Table C-31. dot3StatsTable

Object	OID	Syntax	Access	Status	Supported
dot3StatsIndex	{ dot3StatsEntry 1 }	InterfaceIndex	read-only	current	Yes
dot3StatsAlignmentErrors	{ dot3StatsEntry 2 }	Counter32	read-only	current	Yes
dot3StatsFCSErrors	{ dot3StatsEntry 3 }	Counter32	read-only	current	Yes
dot3StatsSingleCollisionFrames	{ dot3StatsEntry 4 }	Counter32	read-only	current	Yes
dot3StatsMultipleCollisionsFrames	{ dot3StatsEntry 5 }	Counter32	read-only	current	Yes
dot3StatsSQETestErrors	{ dot3StatsEntry 6 }	Counter32	read-only	current	No
dot3StatsDeferredTransmissions	{ dot3StatsEntry 7 }	Counter32	read-only	current	Yes
dot3StatsLateCollisions	{ dot3StatsEntry 8 }	Counter32	read-only	current	Yes
dot3StatsExcessiveCollisions	{ dot3StatsEntry 9 }	Counter32	read-only	current	Yes
dot3StatsInternalMacTransmitErrors	{ dot3StatsEntry 10 }	Counter32	read-only	current	No
dot3StatsCarrierSenseErrors	{ dot3StatsEntry 11 }	Counter32	read-only	current	No
dot3StatsFrameTooLongs	{ dot3StatsEntry 13 }	Counter32	read-only	current	Yes
dot3StatsInternalMacReceiveErrors	{ dot3StatsEntry 16 }	Counter32	read-only	current	No
dot3StatsEtherChipSet	{ dot3StatsEntry 17 }	Object Identifier	read-only	deprecated	No
dot3StatsSymbolErrors	{ dot3StatsEntry 18 }	Counter32	read-only	current	No
dot3StatsDuplexStatus	{ dot3StatsEntry 19 }	INTEGER	read-only	current	Yes

MAU-MIB

The MAU-MIB is defined in RFC 2668. It comprises the following objects:

Table C-32. 802.3 MIB

Object	OID	Syntax	Access	Status	Supported
rpMauTable	{ dot3RpMauBasicGroup 1 }	Sequence of rpMauEntry	not-accessible	current	No
rpJackTable	{ dot3RpMauBasicGroup 2 }	Sequence of rpJackEntry	not-accessible	current	No
ifMauTable	{ dot3IfMauBasicGroup 1 }	Sequence of ifMauEntry	not-accessible	current	Yes
ifJackTable	{ dot3IfMauBasicGroup 2 }	Sequence of ifJackEntry	not-accessible	current	Yes
ifMauAuto NegTable	{ dot3IfMauAutoNegGroup 1 }	Sequence of ifMauAutoNegEntry	not-accessible	current	Yes
broadMau BasicTable	{ dot3BroadMauBasicGroup 1 }	Sequence of broadMauBasicEntry	not-accessible	deprecated	No

ifMauTable

The ifMauTable is a table of descriptive and status information about Medium Attachment Units (MAUs).

Table C-33. ifMauTable

Object	OID	Syntax	Access	Status	Supported
ifMauIfIndex	{ ifMauEntry 1 }	Integer32	read-only	current	Yes
ifMauIndex	{ ifMauEntry 2 }	Integer32	read-only	current	Yes
ifMauType	{ ifMauEntry 3 }	Object Identifier	read-only	current	Yes
ifMauStatus	{ ifMauEntry 4 }	INTEGER	read-only	current	No
ifMauMediaAvailable	{ ifMauEntry 5 }	INTEGER	read-only	current	No
ifMauMediaAvailableStateExits	{ ifMauEntry 6 }	Counter32	read-only	current	No
ifMauJabberState	{ ifMauEntry 7 }	INTEGER	read-only	current	No
ifMauJabberingStateEnters	{ ifMauEntry 8 }	Counter32	read-only	current	No
ifMauFalseCarriers	{ ifMauEntry 9 }	Counter32	read-only	current	No
ifMauTypeList	{ ifMauEntry 10 }	Integer32	read-only	deprecated	No
ifMauDefaultType	{ ifMauEntry 11 }	Object Identifier	read-write	current	Yes
ifMauAutoNegSupported	{ ifMauEntry 12 }	TruthValue	read-only	current	Yes
ifMauTypeListBits	{ ifMauEntry 13 }	Bits	read-only	current	No

ifJackType

The ifJackType object describes the physical connector.

Table C-34. ifJackType

Product Interface	Interface Type	Jack	Return Value
Ethernet Management	10BaseT	Eight Pin Modular	rj45(2)
	100BaseTX		
Gigabit Ethernet Downlink	10BaseT	Eight Pin Modular	rj45(2)
	100BaseTX		
	1000BaseT		
	100BaseFX	Small Form-factor Pluggable (SFP)*	other(1)
	1000BaseSX		
	1000BaseLX		
Gigabit Ethernet Uplink	10BaseT	Eight Pin Modular	rj45(2)
	100BaseTX		
	1000BaseT		
	100BaseFX	Small Form-factor Pluggable (SFP)*	other(1)
	1000BaseSX		
	1000BaseLX		

* When the SFP is installed, it takes precedence over the Eight Pin Modular.

ifMauNegTable

The ifMauNegTable contains objects used for auto-negotiation. Only the ifMauAutoNegAdminStatus object is supported.

Table C-35. ifMauAutoNegTable

Object	OID	Syntax	Access	Status	Supported
ifMauAutoNegAdminStatus	{ ifMauAutoNegEntry 1 }	INTEGER	read-write	current	Y

ADSL-LINE-MIB

The ADSL-LINE-MIB is defined in RFC 2662. It comprises the following objects:

Table C-36. ADSL Line MIB

Object	OID	Syntax (Sequence of)	Access	Status	Supported
adslLineTable	{ adslMibObjects 1 }	adslLineTable	not-accessible	current	Yes
adslAtucPhysTable	{ adslMibObjects 2 }	adslAtucPhysEntry	not-accessible	current	Yes
adslAturPhysTable	{ adslMibObjects 3 }	adslAturPhysEntry	not-accessible	current	Yes
adslAtucChanTable	{ adslMibObjects 4 }	adslAtucChanEntry	not-accessible	current	Yes
adslAturChanTable	{ adslMibObjects 5 }	adslAturChanEntry	not-accessible	current	Yes
adslAtucPerfDataTable	{ adslMibObjects 6 }	adslAtucPerfDataEntry	not-accessible	current	Yes
adslAturPerfDataTable	{ adslMibObjects 7 }	adslAturPerfDataEntry	not-accessible	current	Yes
adslAtucIntervalTable	{ adslMibObjects 8 }	adslAtucIntervalEntry	not-accessible	current	No
adslAturIntervalTable	{ adslMibObjects 9 }	adslAturIntervalEntry	not-accessible	current	No
adslAtucChanPerfData Table	{ adslMibObjects 10 }	adslAtucChanPerfData Entry	not-accessible	current	No
adslAturChanPerf DataTable	{ adslMibObjects 11 }	adslAturChanPerfData Entry	not-accessible	current	No
adslAtucChanInterval Table	{ adslMibObjects 12 }	adslAtucChan IntervalEntry	not-accessible	current	No
adslAturChanInterval Table	{ adslMibObjects 13 }	adslAturChan IntervalEntry	not-accessible	current	No
adslLineConfProfile Table	{ adslMibObjects 14 }	adslLineConfProfile Entry	not-accessible	current	Yes
adslLineAlarmConf ProfileTable	{ adslMibObjects 15 }	adslLineAlarmConf ProfileEntry	not-accessible	current	No

adslLineTable

The adslLineTable describes features common to both ends of the line.

Table C-37. adslLineTable

Object	OID	Syntax	Access	Status	Supported
adslLineCoding	{ adslLineEntry 1 }	AdslLineCodingType	read-only	current	Yes
adslLineType	{ adslLineEntry 2 }	INTEGER	read-only	current	Yes
adslLineSpecific	{ adslLineEntry 3 }	VariablePointer	read-only	current	No
adslLineConfProfile	{ adslLineEntry 4 }	SnmpAdminString	read-only	current	Yes
adslLineAlarmConf Profile	{ adslLineEntry 5 }	SnmpAdminString	read-only	current	No

adslAtucPhysTable

The adslAtucPhysTable contains physical layer parameters for ATU-Cs.

Table C-38. adslAtucPhysTable

Object	OID	Syntax	Access	Status	Supported
adslAtucInvSerialNumber	{ adslAtucPhysEntry 1 }	SnmpAdminString	read-only	current	Yes
adslAtucInvVendorID	{ adslAtucPhysEntry 2 }	SnmpAdminString	read-only	current	Yes
adslAtucInvVersion Number	{ adslAtucPhysEntry 3 }	SnmpAdminString	read-only	current	Yes
adslAtucCurrSnrMgn	{ adslAtucPhysEntry 4 }	INTEGER	read-only	current	Yes
adslAtucCurrAtn	{ adslAtucPhysEntry 5 }	Gauge32	read-only	current	Yes
adslAtucCurrStatus	{ adslAtucPhysEntry 6 }	BITS	read-only	current	Yes
adslAtucCurrOutputPwr	{ adslAtucPhysEntry 7 }	INTEGER	read-only	current	Yes
adslAtucCurrAttainable Rate	{ adslAtucPhysEntry 8 }	Gauge32	read-only	current	Yes

adslAturPhysTable

The adslAturPhysTable contains physical layer parameters for ATU-Rs.

Table C-39. adslAturPhysTable

Object	OID	Syntax	Access	Status	Supported
adslAturInvSerialNumber	{ adslAturPhysEntry 1 }	SnmpAdminString	read-only	current	Yes
adslAturInvVendorID	{ adslAturPhysEntry 2 }	SnmpAdminString	read-only	current	Yes
adslAturInvVersionNumber	{ adslAturPhysEntry 3 }	SnmpAdminString	read-only	current	Yes
adslAturCurrSnrMgn	{ adslAturPhysEntry 4 }	INTEGER	read-only	current	Yes
adslAturCurrAtn	{ adslAturPhysEntry 5 }	Gauge32	read-only	current	Yes
adslAturCurrStatus	{ adslAturPhysEntry 6 }	BITS	read-only	current	Yes
adslAturCurrOutputPwr	{ adslAturPhysEntry 7 }	INTEGER	read-only	current	Yes
adslAturCurrAttainableRate	{ adslAturPhysEntry 8 }	Gauge32	read-only	current	Yes

adslAtucChanTable

The adslAtucChanTable contains information about each ATU-C channel.

Table C-40. adslAutcChanTable

Object	OID	Syntax	Access	Status	Supported
adslAtucChanInterleaveDelay	{ adslAtucChanEntry 1 }	Gauge32	read-only	current	Yes
adslAtucChanCurrTxRate	{ adslAtucChanEntry 2 }	Gauge32	read-only	current	Yes
adslAtucChanPrevTxRate	{ adslAtucChanEntry 3 }	Gauge32	read-only	current	No
adslAtucChanCrcBlockLength	{ adslAtucChanEntry 4 }	Gauge32	read-only	current	No

adslAturChanTable

The adslAturChanTable contains information about each ATU-R channel.

Table C-41. adslAturChanTable

Object	OID	Syntax	Access	Status	Supported
adslAturChanInterleaveDelay	{ adslAturChanEntry 1 }	Gauge32	read-only	current	Yes
adslAturChanCurrTxRate	{ adslAturChanEntry 2 }	Gauge32	read-only	current	Yes
adslAturChanPrevTxRate	{ adslAturChanEntry 3 }	Gauge32	read-only	current	No
adslAturChanCrcBlockLength	{ adslAturChanEntry 4 }	Gauge32	read-only	current	No

adslAtucPerfDataTable

This table contains ATU-C performance data. Only adslAtucPerfESs and adslAtucPerfInits are supported.

Table C-42. adslAtucPerfDataTable

Object	OID	Syntax	Access	Status	Supported
adslAtucPerfESs	{ adslAtucPerfDataEntry 5 }	Counter32	read-only	current	Yes
adslAtucPerfInits	{ adslAtucPerfDataEntry 6 }	Counter32	read-only	current	Yes

adslAturPerfDataTable

This table contains ATU-R performance data. Only adslAturPerfLprs and adslAturPerfESs are supported.

Table C-43. adslAturPerfDataTable

Object	OID	Syntax	Access	Status	Supported
adslAturPerfLprs	{ adslAturPerfDataEntry 3 }	Counter32	read-only	current	Yes
adslAturPerfESs	{ adslAturPerfDataEntry 4 }	Counter32	read-only	current	Yes

adslLineConfProfileTable

This table contains information on the ADSL line configuration. There is one static profile for each DSL port, whose name is the decimal equivalent of its ifIndex (see *ifIndex* on page C-16). Profiles cannot be created or deleted.

Table C-44. adslLineConfProfileTable (1 of 2)

Object	OID	Syntax	Access	Status	Supported
adslLineConfProfileName	{ adslLineConfProfileEntry 1 }	SnmpAdmin String	not-accessible	current	Yes
adslAtucConfRateMode	{ adslLineConfProfileEntry 2 }	INTEGER	read-create	current	Yes
adslAtucConfRateChanRatio	{ adslLineConfProfileEntry 3 }	INTEGER	read-create	current	No
adslAtucConfTargetSnrMgn	{ adslLineConfProfileEntry 4 }	INTEGER	read-create	current	Yes
adslAtucConfMaxSnrMgn	{ adslLineConfProfileEntry 5 }	INTEGER	read-create	current	No
adslAtucConfMinSnrMgn	{ adslLineConfProfileEntry 6 }	INTEGER	read-create	current	No
adslAtucConfDownshiftSnrMgn	{ adslLineConfProfileEntry 7 }	INTEGER	read-create	current	No
adslAtucConfUpshiftSnrMgn	{ adslLineConfProfileEntry 8 }	INTEGER	read-create	current	No
adslAtucConfMinUpshiftTime	{ adslLineConfProfileEntry 9 }	INTEGER	read-create	current	No

Table C-44. adslLineConfProfileTable (2 of 2)

Object	OID	Syntax	Access	Status	Supported
adslAtucConfMinDownshift Time	{ adslLineConfProfileEntry 10 }	INTEGER	read-create	current	No
adslAtucChanConfFastMin TxRate	{ adslLineConfProfileEntry 11 }	Unsigned32	read-create	current	Yes
adslAtucChanConfInterleave MinTxRate	{ adslLineConfProfileEntry 12 }	Unsigned32	read-create	current	Yes
adslAtucChanConfFastMaxT xRate	{ adslLineConfProfileEntry 13 }	Unsigned32	read-create	current	Yes
adslAtucChanConfInterleave MaxTxRate	{ adslLineConfProfileEntry 14 }	Unsigned32	read-create	current	Yes
adslAtucChanConfMax InterleaveDelay	{ adslLineConfProfileEntry 15 }	INTEGER	read-create	current	No
adslAturConfRateMode	{ adslLineConfProfileEntry 16 }	INTEGER	read-create	current	No
adslAturConfRateChanRatio	{ adslLineConfProfileEntry 17 }	INTEGER	read-create	current	No
adslAturConfTargetSnrMgn	{ adslLineConfProfileEntry 18 }	INTEGER	read-create	current	Yes
adslAturConfMaxSnrMgn	{ adslLineConfProfileEntry 19 }	INTEGER	read-create	current	No
adslAturConfMinSnrMgn	{ adslLineConfProfileEntry 20 }	INTEGER	read-create	current	No
adslAturConfDownshiftSnr Mgn	{ adslLineConfProfileEntry 21 }	INTEGER	read-create	current	No
adslAturConfUpshiftSnrMgn	{ adslLineConfProfileEntry 22 }	INTEGER	read-create	current	No
adslAturConfMinUpshiftTime	{ adslLineConfProfileEntry 23 }	INTEGER	read-create	current	No
adslAturConfMinDownshift Time	{ adslLineConfProfileEntry 24 }	INTEGER	read-create	current	No
adslAturChanConfFastMin TxRate	{ adslLineConfProfileEntry 25 }	Unsigned32	read-create	current	Yes
adslAturChanConfInterleave MinTxRate	{ adslLineConfProfileEntry 26 }	Unsigned32	read-create	current	Yes
adslAturChanConfFastMax TxRate	{ adslLineConfProfileEntry 27 }	Unsigned32	read-create	current	Yes
adslAturChanConfInterleave MaxTxRate	{ adslLineConfProfileEntry 28 }	Unsigned32	read-create	current	Yes
adslAturChanConfMax InterleaveDelay	{ adslLineConfProfileEntry 29 }	INTEGER	read-create	current	No
adslLineConfProfileRow Status	{ adslLineConfProfileEntry 30 }	RowStatus	read-create	current	Yes

ADSL-LINE-EXT-MIB

The ADSL-LINE-EXT-MIB is defined in the IETF draft draft-ietf-adslmib-adslext-07.txt, “Definitions of Extension Managed Objects for ADSL Lines.” It comprises the following objects:

Table C-45. ADSL Line Extension MIB

Object	OID	Syntax (Sequence of)	Access	Status	Supported
adslLineExtTable	{ adslMibObjects 17 }	adslLineExt Entry	not-accessible	current	Yes
adslAtucPerfDataExtTable	{ adslMibObjects 18 }	adslAtucPerf DataExtEntry	not-accessible	current	Yes
adslAtucIntervalExtTable	{ adslMibObjects 19 }	adslAtucInterval ExtEntry	not-accessible	current	No
adslAturPerfDataExtTable	{ adslMibObjects 20 }	adslAturPerf DataExtEntry	not-accessible	current	Yes
adslAturIntervalExtTable	{ adslMibObjects 21 }	adslAturInterval ExtEntry	not-accessible	current	No
adslConfProfileExtTable	{ adslMibObjects 22 }	adslConfProfile ExtEntry	not-accessible	current	Yes
adslAlarmConfProfileExtTable	{ adslMibObjects 23 }	adslAlarmConf ProfileExtEntry	not-accessible	current	No

adslLineExtTable

This table contains ADSL line configuration and monitoring information not defined in the adslLineTable in the ADSL Line MIB (RFC 2662).

Table C-46. adslLineExtTable

Object	OID	Syntax	Access	Status	Supported
adslLineTransAtucCap	{ adslLineExtEntry 1 }	AdslTransmission ModeType	read-only	current	Yes
adslLineTransAtucConfig	{ adslLineExtEntry 2 }	AdslTransmission ModeType	read-write	current	Yes
adslLineTransAtucActual	{ adslLineExtEntry 3 }	AdslTransmission ModeType	read-only	current	Yes
adslLineGlitePowerState	{ adslLineExtEntry 4 }	INTEGER	read-only	current	No
adslLineConfProfileDualLite	{ adslLineExtEntry 5 }	SnmpAdminString	read-write	current	No

adslAtucPerfDataExtTable

This table contains ADSL physical line counters information not defined in the adslAtucPerfDataTable in the ADSL Line MIB (RFC 2662).

Table C-47. adslAtucPerfDataExtTable

Object	OID	Syntax	Access	Status	Supported
adslAtucPerfStatFastR	{ adslAtucPerfDataExtEntry 1 }	Counter32	read-only	current	No
adslAtucPerfStatFailedFastR	{ adslAtucPerfDataExtEntry 2 }	Counter32	read-only	current	No
adslAtucPerfStatSesL	{ adslAtucPerfDataExtEntry 3 }	Counter32	read-only	current	Yes
adslAtucPerfStatUasL	{ adslAtucPerfDataExtEntry 4 }	Counter32	read-only	current	Yes
adslAtucPerfCurr15MinFastR	{ adslAtucPerfDataExtEntry 5 }	PerfCurrent Count	read-only	current	No
adslAtucPerfCurr15MinFailed FastR	{ adslAtucPerfDataExtEntry 6 }	PerfCurrent Count	read-only	current	No
adslAtucPerfCurr15MinSesL	{ adslAtucPerfDataExtEntry 7 }	PerfCurrent Count	read-only	current	No
adslAtucPerfCurr15MinUasL	{ adslAtucPerfDataExtEntry 8 }	PerfCurrent Count	read-only	current	No
adslAtucPerfCurr1DayFastR	{ adslAtucPerfDataExtEntry 9 }	AdslPerfCurr DayCount	read-only	current	No
adslAtucPerfCurr1DayFailedFa stR	{ adslAtucPerfDataExtEntry 10 }	AdslPerfCurr DayCount	read-only	current	No
adslAtucPerfCurr1DaySesL	{ adslAtucPerfDataExtEntry 11 }	AdslPerfCurr DayCount	read-only	current	No
adslAtucPerfCurr1DayUasL	{ adslAtucPerfDataExtEntry 12 }	AdslPerfCurr DayCount	read-only	current	No
adslAtucPerfPrev1DayFastR	{ adslAtucPerfDataExtEntry 13 }	AdslPerfPrev DayCount	read-only	current	No
adslAtucPerfPrev1DayFailedF astR	{ adslAtucPerfDataExtEntry 14 }	AdslPerfPrev DayCount	read-only	current	No
adslAtucPerfPrev1DaySesL	{ adslAtucPerfDataExtEntry 15 }	AdslPerfPrev DayCount	read-only	current	No
adslAtucPerfPrev1DayUasL	{ adslAtucPerfDataExtEntry 16 }	AdslPerfPrev DayCount	read-only	current	No

adslAturPerfDataExtTable

This table contains ADSL physical line counters information not defined in the adslAturPerfDataTable in the ADSL Line MIB (RFC 2662).

Table C-48. adslAturPerfDataExtTable

Object	OID	Syntax	Access	Status	Supported
adslAturPerfStatSesL	{ adslAtucIntervalExtEntry 1 }	Counter32	read-only	current	Yes
adslAturPerfStatUasL	{ adslAtucIntervalExtEntry 2 }	Counter32	read-only	current	Yes
adslAturPerfCurr15MinSesL	{ adslAtucIntervalExtEntry 3 }	PerfCurrent Count	read-only	current	No
adslAturPerfCurr15MinUasL	{ adslAtucIntervalExtEntry 4 }	PerfCurrent Count	read-only	current	No
adslAturPerfCurr1DaySesL	{ adslAtucIntervalExtEntry 5 }	AdslPerfCurr DayCount	read-only	current	No
adslAturPerfCurr1DayUasL	{ adslAtucIntervalExtEntry 6 }	AdslPerfCurr DayCount	read-only	current	No
adslAturPerfPrev1DaySesL	{ adslAtucIntervalExtEntry 7 }	AdslPerfPre vDayCount	read-only	current	No
adslAturPerfPrev1DayUasL	{ adslAtucIntervalExtEntry 8 }	AdslPerfPre vDayCount	read-only	current	No

adslConfProfileExtTable

This table contains ADSL line profile configuration information not defined in the adslLineConfProfileTable in the ADSL Line MIB (RFC 2662).

Table C-49. adslConfProfileExtTable

Object	OID	Syntax	Access	Status	Supported
adslConfProfileLineType	{ adslConfProfileExtEntry 1 }	INTEGER	read-create	current	Yes

BRIDGE-MIB

The BRIDGE-MIB is defined in RFC 1483. It defines objects for managing MAC bridges.

The following groups are supported:

- dot1dBase (OID dot1dBridge 1)
- dot1dTp (OID dot1dBridge 4)
- dot1dStatic (OID dot1dBridge 5)

dot1dBase Group

The dot1dBase group contains objects applicable to all types of bridges.

Table C-50. dot1dBase Group

Object	OID	Syntax	Access	Status	Supported
dot1dBaseBridgeAddress	{ dot1dBase 1 }	MacAddress	read-only	mandatory	No
dot1dBaseNumPorts	{ dot1dBase 2 }	INTEGER	read-only	mandatory	Yes
dot1dBaseType	{ dot1dBase 3 }	INTEGER	read-only	mandatory	Yes
dot1dBasePortTable	{ dot1dBase 4 }	Sequence of dot1dBasePortEntry	not-accessible	mandatory	No

dot1dBaseNumPorts

Each chassis has the following bridge ports:

- ADSL Ports: 1–24 or 1–48
- Ethernet Management Port: 49
- Ethernet Downlink Port: 50
- Ethernet Uplink Port: 51
- V.35/X.21 Port (if installed): 52

dot1dTp Group

The dot1dTp group describes an entity's state with respect to transparent bridging.

Table C-51. dot1dTp Group

Object	OID	Syntax	Access	Status	Supported
dot1dTpLearnedEntityDiscards	{ dot1dTp 1 }	Counter	read-only	mandatory	No
dot1dTpAgingTime	{ dot1dTp 2 }	INTEGER	read-write	mandatory	Yes
dot1dTpFdbTable	{ dot1dTp 3 }	Sequence of dot1dTpFdbEntry	not-accessible	mandatory	Yes
dot1dTpPortTable	{ dot1dTp 4 }	Sequence of dot1dTpPortEntry	not-accessible	mandatory	Yes

dot1dStaticTable

The dot1dStaticTable of the dot1dStatic group is fully supported. It is a table containing filtering information configured by local or network management.

Table C-52. dot1dStaticTable

Object	OID	Syntax	Access	Status	Supported
dot1dStaticAddress	{ dot1dStaticEntry 1 }	MacAddress	read-write	mandatory	Yes
dot1dStaticReceivePort	{ dot1dStaticEntry 2 }	INTEGER	read-write	mandatory	Yes
dot1dStaticAllowedToGoTo	{ dot1dStaticEntry 3 }	OCTET STRING	read-write	mandatory	Yes
dot1dStaticStatus	{ dot1dStaticEntry 4 }	INTEGER	read-write	mandatory	Yes

Q-BRIDGE-MIB

The Q-BRIDGE-MIB is defined in RFC 2674. It describes managed objects for virtual LAN bridging enhancements defined by IEEE 802.1Q-1998. The dot1qTp and dot1qVlan groups are supported.

dot1qTpFdbTable

The dot1qTpFdbTable object of the dot1qTp group is fully supported.

Table C-53. dot1qTpFdbTable

Object	OID	Syntax	Access	Status	Supported
dot1qTpFdbAddress	{ dot1qTpFdbEntry 1 }	MacAddress	not-accessible	current	Yes
dot1qTpFdbPort	{ dot1qTpFdbEntry 2 }	INTEGER	read-only	current	Yes
dot1qTpFdbStatus	{ dot1qTpFdbEntry 3 }	INTEGER	read-only	current	Yes

dot1qVlanCurrentTable

Table C-54. dot1qVlanCurrentTable

Object	OID	Syntax	Access	Status	Supported
dot1qVlanTimeMark	{ dot1qVlanCurrentEntry 1 }	TimeFilter	not-accessible	current	Yes
dot1qVlanIndex	{ dot1qVlanCurrentEntry 2 }	VlanIndex	not-accessible	current	Yes
dot1qVlanFdbId	{ dot1qVlanCurrentEntry 3 }	Unsigned32	read-only	current	Yes
dot1qVlanCurrentEgress-Ports	{ dot1qVlanCurrentEntry 4 }	PortList	read-only	current	No
dot1qVlanCurrent-UngaggedPorts	{ dot1qVlanCurrentEntry 5 }	PortList	read-only	current	No
dot1qVlanStatus	{ dot1qVlanCurrentEntry 6 }	INTEGER	read-only	current	No
dot1qVlanCreationTime	{ dot1qVlanCurrentEntry 7 }	TimeTicks	read-only	current	No

dot1qVlanStaticTable

Table C-55. dot1qVlanStaticTable

Object	OID	Syntax	Access	Status	Supported
dot1qVlanStaticName	{ dot1qVlanStaticEntry 1 }	SnmpAdminString	read-create	current	Yes
dot1qVlanStaticEgress-Ports	{ dot1qVlanStaticEntry 2 }	PortList	read-create	current	Yes
dot1qVlanForbidenEgress-Ports	{ dot1qVlanStaticEntry 3 }	PortList	read-create	current	Yes
dot1qVlanStaticUntagged-Ports	{ dot1qVlanStaticEntry 4 }	PortList	read-create	current	Yes
dot1qVlanStaticRowStatus	{ dot1qVlanStaticEntry 5 }	PortList	read-only	current	Yes

PPP-LCP-MIB

The PPP-LCP-MIB is defined in RFC 1471. It describes objects for managing the link control protocol and link quality monitoring on subnetwork interfaces that use point to point protocols. The pppLink (OID pppLcp 1) group is supported.

pppLinkStatusTable

The pppLinkStatusTable contains PPP link-specific variables.

Table C-56. pppLinkStatusTable

Object	OID	Syntax	Access	Status	Supported
pppLinkStatusPhysicalIndex	{ pppLinkStatusEntry 1 }	INTEGER	read-only	mandatory	Yes
pppLinkStatusBadAddresses	{ pppLinkStatusEntry 2 }	Counter	read-only	mandatory	No
pppLinkStatusBadControls	{ pppLinkStatusEntry 3 }	Counter	read-only	mandatory	No
pppLinkStatusPacketTooLongs	{ pppLinkStatusEntry 4 }	Counter	read-only	mandatory	Yes
pppLinkStatusBadFCSs	{ pppLinkStatusEntry 5 }	Counter	read-only	mandatory	No
pppLinkStatusLocalMRU	{ pppLinkStatusEntry 6 }	INTEGER	read-only	mandatory	Yes
pppLinkStatusRemoteMRU	{ pppLinkStatusEntry 7 }	INTEGER	read-only	mandatory	Yes
pppLinkStatusLocalToPeer ACCMap	{ pppLinkStatusEntry 8 }	Octet String	read-only	mandatory	Yes
pppLinkStatusPeerToLocal ACCMap	{ pppLinkStatusEntry 9 }	Octet String	read-only	mandatory	Yes
pppLinkStatusLocalToRemote ProtocolCompression	{ pppLinkStatusEntry 10 }	INTEGER	read-only	mandatory	Yes
pppLinkStatusRemoteToLocal ProtocolCompression	{ pppLinkStatusEntry 11 }	INTEGER	read-only	mandatory	Yes
pppLinkStatusLocalToRemote ACCompression	{ pppLinkStatusEntry 12 }	INTEGER	read-only	mandatory	Yes
pppLinkStatusRemoteToLocal ACCompression	{ pppLinkStatusEntry 13 }	INTEGER	read-only	mandatory	Yes
pppLinkStatusTransmitFcsSize	{ pppLinkStatusEntry 14 }	INTEGER	read-only	mandatory	Yes
pppLinkStatusReceiveFcsSize	{ pppLinkStatusEntry 15 }	INTEGER	read-only	mandatory	Yes

PDN-MPE-DEVICE-CONTROL-MIB

The PDN-MPE-DEVICE-CONTROL-MIB is used to reset the device. The mpeDevControlTable object of the mpeDevHwControl group is supported.

A reset is effected by writing the value reset(2) to the mpeDevControlReset object of mpeDevControlEntry. The value resetToFactoryDefaults(3) is invalid.

PDN-MPE-DSLAM-SYSTEM-MIB

The PDN-MPE-DSLAM-SYSTEM-MIB is used to configure alarms. It is fully supported.

PDN-MPE-HEALTH-AND-STATUS-MIB

The PDN-MPE_HEALTH-AND-STATUS-MIB is used to report device self-test results. It is fully supported.

The mpeDevSelfTestResults object contains the results of self-tests for each circuit card assembly, separated by semi-colons (;). The results are in the format:

Stack=*r*
Chassis=*r*
SecProc=*r*
Port Processor: SEEP=*r* ;CPUReg=*r*,CPUTimer=*r*,SDRAM=*r*
DSL Ports: Memory=*r* ;DataPump=*r*,PHY=*r*
Management Module: CPUReg=*r*,CPUTimer=*r*,SDRAM=*r*,File System=*r*
V.35/X.21 Uplink: CPUReg=*r*,CPUTimer=*r*,SDRAM=*r*,Uplink Interface=*r*
GigE Uplink Interface: MAC=*r* ;PHY=*r*,Device Reg=*r*
GigE Uplink Interface: MAC=*r* ;PHY=*r*,Device Reg=*r*
Management Port: MAC=*r* ;PHY=*r*,Device Reg=*r*
Etherswitch: I2C Bus =*r* ;L2 Switch Memory=*r* ;L2 Switch Reg=*r*

Where:

r is one of:

P = Pass

F = Fail

U = Unknown status

PDN-MPE-ENTITY-SENSOR-MIB

The PDN-MPE-ENTITY-SENSOR-MIB is used to configure and read temperature sensor limits. It is fully supported.

PDN-ARP-MIB

The PDN-ARP-MIB is used in the creation of ARP entries. It comprises the following groups:

Table C-57. PDN-ARP- MIB Objects

Object	OID	Description	Supported
pdnNetToMediaParams	{ pdnNetToMediaGenericMIBObjects 1 }	ARP Parameters Configuration group	No
pdnNetToMediaConfig	{ pdnNetToMediaGenericMIBObjects 2 }	ARP Entry Configuration group	Yes
pdnNetTo8023MediaConfig	{ pdnNetToMediaGenericMIBObjects 3 }	ARP Entry Configuration for 802.3 Media Cards	No
ipNetToMediaConfig	{ pdnNetToMediaConfig 4 }	Proxy ARP Configuration Group	Yes
pdnNetToMediaMIBTraps	{ pdn-arp 2 }	Traps	Yes

pdnNetToMediaConfig Group

The pdnNetToMediaConfig group contanis objects for configuring ARP entries.

Table C-58. pdnNetToMediaConfig Group

Object	OID	Syntax	Access	Status	Supported
	pdnNetToMedia-Config	SEQUENCE of	not-accessible	current	No
pdnNetToMediaClear-AllArp	{ pdnNetToMedia-Config 2 }	INTEGER	read-write	current	Yes
pdnNetToMediaProxy-ArpTable	{ pdnNetToMedia-Config 3 }	SEQUENCE of	not-accessible	current	Yes

ipNetToMediaConfig

The ipNetToMediaConfig group contains objects for configuring proxy ARP entries.

Table C-59. ipNetToMediaConfig Group

Object	OID	Syntax	Access	Status	Supported
ipNetToMediaForward-ingMode	{ ipNetToMediaConfig 1 }	INTEGER	read-write	current	Yes
ipNetToMediaDefault-NHR	{ ipNetToMediaConfig 2 }	IpAddress	read-write	current	Yes
ipNetToMediaExtTable	{ ipNetToMediaConfig 3 }	SEQUENCE OF ipNetToMediaExtEntry	not-accessible	current	Yes
ipNetToMediaLimitTable	{ ipNetToMediaConfig 4 }	SEQUENCE OF ipNetToMediaLimitEntry	not-accessible	current	Yes

PDN-ATMSTATS-MIB

The PDN-ATMSTATS-MIB is used to collect ATM layer statistics for each interface. It comprises the following groups:

Table C-60. PDN-ATMSTATS-MIB Objects

Object	OID	Description	Supported
pdnAtmVplStat	{ pdnAtmStatsMIB 1 }	ATM VPL Statistics	No
pdnAtmVclStat	{ pdnAtmStatsMIB 2 }	ATM VCL Statistics	Yes
pdnAtmStat	{ pdnAtmStatsMIB 3 }	ATM Statistics	Yes

pdnAtmVclStat Group

The pdnAtmVclStat group consists of virtual channel link statistics.

Table C-61. pdnAtmVclStat

Object	OID	Syntax	Access	Status	Supported
pdnAtmVclStatTable	{ pdnAtmVclStat 2 }	SEQUENCE OF pdnAtmVclStatEntry	not-accessible	current	Yes
pdnAtmVclCurrTable	{ pdnAtmVclStat 3 }	SEQUENCE OF pdnAtmVclCurrEntry	not-accessible	current	No
pdnAtmVclHistTable	{ pdnAtmVclStat 4 }	SEQUENCE OF pdnAtmVclHistEntry	not-accessible	current	No

pdnAtmStat Group

The pdnAtmStat group consists of ATM statistics.

Table C-62. pdnAtmStat Group

Object	OID	Syntax	Access	Status	Supported
pdnAtmStatTable	{ pdnAtmVclStat 2 }	SEQUENCE OF pdnAtmStatEntry	not-accessible	current	Yes

PDN-CONFIG-MIB

The PDN-CONFIG-MIB is used to configure the DSL ports. It comprises the following groups:

Table C-63. PDN-CONFIG-MIB Objects

Object	OID	Description	Supported
devConfigArea	{ pdn-devConfig 1 }	The device Configuration Area Group	No
devConfigTestTimer	{ pdn-devConfig 2 }	The Test Timeout Group.	Yes
devConfigClockSrc	{ pdn-devConfig 3 }	The Clock Source Group	No
devConfigTrap	{ pdn-devConfig 4 }	The Trap Configuration Group	No
devConfigAlarm	{ pdn-devConfig 5 }	The System Alarm Group	No
devConfigCardType	{ pdn-devConfig 6 }	The Card Type Table	No
devConfigNetSync	{ pdn-devConfig 7 }	The Device Network Synchronization Group	No
devConfigTime	{ pdn-devConfig 8 }	The Device Configuration Time Group	Yes
devConfigChangeKeys	{ pdn-devConfig 9 }	The Device Configuration Change Key Group	No
devConfiguration	{ pdn-devConfig 10 }	The General Configuration Group	Yes

devConfiguration Group

The devConfiguration group is used for general configuration.

Table C-64. devConfiguration Group

Object	OID	Syntax	Access	Status	Supported
devConfigComDiscTime	{ devConfiguration 1 }	INTEGER	read-write	mandatory	Yes
devConfigPortNumDisplayFormat	{ devConfiguration 2 }	INTEGER	read-write	mandatory	Yes
devConfigDateDisplayFormat	{ devConfiguration 3 }	INTEGER	read-write	mandatory	Yes
devAcceptRemoteResetFrame	{ devConfiguration 4 }	INTEGER	read-write	mandatory	Yes

PDN-CONTROL-MIB

The PDN-CONTROL-MIB is used for device control. It comprises the following groups:

Table C-65. PDN-CONTROL-MIB Objects

Object	OID	Syntax	Access	Status	Supported
pdnControlMIBTrapsV2	{ pdnControl 0 }	OBJECT-IDENTITY	N/A	current	Yes
devHWControlReset	{ pdnControl 1 }	INTEGER	read-write	current	No
devControlTestTable	{ pdnControl 2 }	SEQUENCE OF devControlTestEntry	not-accessible	current	Yes
devControlDownLoadTable	{ pdnControl 3 }	SEQUENCE OF devControlDown-LoadEntry	not-accessible	current	No
devControlRMON	{ pdnControl 4 }	OBJECT IDENTIFIER	N/A	N/A	No
devSNSwitchFirmwareTable	{ pdnControl 5 }	SEQUENCE OF devSNSwitch-FirmwareEntry	not-accessible	current	No
devControlFTP	{ pdnControl 6 }	OBJECT IDENTIFIER	N/A	N/A	Yes
devFileXferMIBObjects	{ pdnControl 7 }	OBJECT IDENTIFIER	N/A	N/A	Yes
devFileXferMIBTraps	{ pdnControl 8 }	OBJECT IDENTIFIER	N/A	N/A	No
devFirmwareControlMIBObjects	{ pdnControl 9 }	OBJECT IDENTIFIER	N/A	N/A	Yes
pdnConfigChangeMgmt	{ pdnControl 10 }	OBJECT IDENTIFIER	N/A	N/A	Yes
pdnControlMIBGroups	{ pdnControl 11 }	OBJECT IDENTIFIER	N/A	N/A	N/A
pdnAutoFw	{ pdnControl 12 }	OBJECT IDENTIFIER	B./A	N/A	No

devFileXferMIBObjects Group

The devFileXferMIBObjects group comprises the following objects:

Table C-66. devFileXferMIBObjects Group

Object	OID	Syntax	Access	Status	Supported
devFileXferConfigTable	{ devFileXfer-MIBObjects 1 }	SEQUENCE OF devFileXferConfigEntry	not-accessible	current	No
pdnDevFileXferTable	{ devFileXfer-MIBObjects 2 }	SEQUENCE OF pdnDevFileXferEntry	not-accessible	current	Yes
pdnDevFileXferSessionIDNext	{ devFileXfer-MIBObjects 3 }	Integer32	read-only	current	Yes

PDN-IPSEC-MANUAL-MIB

The PDN-IPSEC-MANUAL-MIB is used to configure IPsec (IP security). It is fully supported.

Table C-67. PDN-IPSEC-MANUAL-MIB Objects

Object	OID	Description	Supported
pdnVpnConfig	{ pdnIpSec 1 }	VPN Tunnel Configuration Group	Yes
pdnIPSecConfig	{ pdnVpnConfigGroups 1 }	IP Sec Configuration Group	Yes
pdnIPSecKeyConfig	{ pdnIPSecConfigGroups 1 }	IP Sec Global Key Configuration Group	Yes
pdnIPSecSPDConfig	{ pdnIPSecConfigGroups 2 }	Security Policy Database	Yes
pdnIPSecConnectionConfig	{ pdnIPSecConfigGroups 3 }	Security Policy Associated with each Connection	Yes

PDN-IF-EXT-CONFIG-MIB

The PDN-IF-EXT-CONFIG-MIB is used to configure interface-related objects. It is fully supported.

Table C-68. PDN-IF-EXT-CONFIG-MIB Objects

Object	OID	Description	Supported
pdnIfExtEncapConfig	{ pdnIfExt 3 }	Interface Configuration Group	Yes

PDN-SECURITY-MIB

The PDN-SECURITY-MIB is used to implement access security. It comprises the following groups:

Table C-69. PDN-SECURITY-MIB Objects

Object	OID	Syntax	Access	Status	Supported
devSecurityMgrValidation	{ pdn-security 1 }	INTEGER	read-write	mandatory	Yes
devSecurityMgrMaxNumber	{ pdn-security 2 }	INTEGER	read-only	mandatory	No
devSecurityMgrCurrent-Number	{ pdn-security 3 }	INTEGER	read-only	mandatory	No
devSecurityMgrTable	{ pdn-security 4 }	SEQUENCE OF devSecurityMgrEntry	not-accessible	deprecated	No
newSecurityMgrTable	{ pdn-security 5 }	SEQUENCE OF newSecurityMgrEntry	not-accessible	deprecated	No
devSecurityTelnetSource-Validation	{ pdn-security 6 }	INTEGER	read-write	mandatory	No
devSecurityFtpSource-Validation	{ pdn-security 7 }	INTEGER	read-write	mandatory	No
securityMgrTable	{ pdn-security 8 }	SEQUENCE OF securityMgrEntry	not-accessible	mandatory	Yes
devSecuritySNMPMgrAccess	{ pdn-security 9 }	INTEGER	read-write	mandatory	Yes

securityMgrTable

The securityMgrTable comprises the following objects:

Table C-70. securityMgrTable

Object	OID	Syntax	Access	Status	Supported
securityMgrIpAddress	{ securityMgrEntry 1 }	IpAddress	read-only	mandatory	Yes
securityMgrSubnetMask	{ securityMgrEntry 2 }	IpAddress	read-only	mandatory	Yes
securityMgrSnmpAccess	{ securityMgrEntry 3 }	INTEGER	read-write	mandatory	Yes
securityMgrTelnetAccess	{ securityMgrEntry 4 }	INTEGER	read-write	mandatory	No
securityMgrFtpAccess	{ securityMgrEntry 5 }	INTEGER	read-write	mandatory	No
securityMgrTrapAccess	{ securityMgrEntry 6 }	INTEGER	read-write	mandatory	Yes
securityMgrRowStatus	{ securityMgrEntry 7 }	RowStatus	read-write	mandatory	Yes

PDN-SYNCPORTSTATS-MIB

The PDN-SYNCPORTSTATS-MIB augments rs232SyncPortTable. It comprises the following objects. The rs232SyncPortExtTable object of the rs232SyncPortExtMIBObject group is supported.

Table C-71. PDN-SYNCPORTSTATS-MIB Objects

Object	OID	Description	Supported
syncPortStats	{ syncPort 5 }	Device Sync Port Statistics Group	No
rs232SyncPortExtMIBObject	{ syncPort 6 }	RS-232 Sync Port Group	Yes

PDN-DIAGNOSTICS-MIB

The PDN-DIAGNOSTICS-MIB is used to configure tests. Only the diagTestMIBTraps group is supported.

For a description of traps supported by the BitStorm 4800, see Appendix B, *SNMP Traps*.

PDN-DSLAM-SYSTEM-MIB

The PDN-DSLAM-SYSTEM-MIB is used to configure and collect statistics for line cards. It comprises the following groups:

Table C-72. PDN-DSLAM-SYSTEM-MIB Objects

Object	OID	Description	Supported
sysDevStats	{ sysDevDslamMIBObjects 1 }	The Statistics Group	No
sysDevConfig	{ sysDevDslamMIBObjects 2 }	The Configuration Group	Yes

sysDevConfig Group

The sysDevConfig group is used for configuration.

Table C-73. sysDevConfig

Object	OID	Syntax	Access	Status	Supported
enablePowerSourceFailure-Alarm	{ sysDevConfig 1 }	INTEGER	read-write	current	No
devIfTable	{ sysDevConfig 2 }	SEQUENCE OF devIfTableEntry	not-accessible	current	No
communityTrapAddressInfo-Table	{ sysDevConfig 3 }	SEQUENCE OF communityTrap-AddressInfoTableEntry	not-accessible	current	No
entCommunityTable	{ sysDevConfig 4 }	SEQUENCE OF entCommunityTable-Entry	not-accessible	current	Yes
sysDevUserAccountTable	{ sysDevConfig 5 }	SEQUENCE OF sysDevUserAccount-Entry	not-accessible	current	No
sysDevIDSLConfigTable	{ sysDevConfig 6 }	SEQUENCE OF sysDevIdslConfigEntry	not-accessible	current	No
sysDevDslamSyslog	{ sysDevConfig 7 }	OID	N/A	N/A	No
sysDevConfigUserAccount-Table	{ sysDevConfig 8 }	SEQUENCE OF sysDevConfigUser-AccounntEntry	not-accessible	current	Yes
sysDevConfigUserAccount-IndexNext	{ sysDevConfig 9 }	Integer32	read-only	current	Yes

PDN-ETHER-MIB

The PDN-ETHER-MIB is used to configure Ethernet interfaces.

Table C-74. PDN-ETHER-MIB Objects

Object	OID	Description	Supported
pdnPortConfigEthernet	{ pdnPortConfigMIBObjects 1 }	Ethernet Port Configuration Group	No
pdnPortConfigMauExtMIBObjects	{ pdnPortConfigMIBObjects 3 }	MAU Configuration Group	Yes
pdnPortConfigIfJackMIBObject	{ pdnPortConfigMIBObjects 4 }	Jack Configuration Group	Yes

PDN-FILTER-MIB

The PDN-FILTER-MIB is used to configure filters. The sysDevFilter group is supported.

sysDevFilter Group

The sysDevFilter group comprises the following objects:

Table C-75. sysDevFilter Group

Object	OID	Syntax	Access	Status	Supported
sysDevSNInjectionType	{ sysDevFilter 1 }	Integer	not-accessible	mandatory	No
sysDevSNInjectionVnid	{ sysDevFilter 2 }	VnidRange	not-accessible	mandatory	No
sysDevFilterConfigTable	{ sysDevFilter 3 }	SEQUENCE OF sysDevFilterConfig-TableEntry	not-accessible	mandatory	Yes
sysDevL2FilterRuleConfig-Table	{ sysDevFilter 4 }	SEQUENCE OF sysDevL2FilterRule-ConfigTableEntry	not-accessible	mandatory	Yes
sysDefFilterBindingTable	{ sysDevFilter 5 }	SEQUENCE OF sysDefFilterBinding-TableEntry	not-accessible	mandatory	Yes
sysDevFilterIndexNext	{ sysDevFilter 6 }	INTEGER	read-only	mandatory	Yes
sysDevL2FilterRuleIndex-Next	{ sysDevFilter 7 }	INTEGER	read-only	mandatory	Yes
sysDevFilterToRuleBinding-Table	{ sysDevFilter 8 }	SEQUENCE OF sysDevFilterToRule-BindingTableEntry	not-accessible	mandatory	Yes

PDN-INET-CONFIG-MIB

The PDN-INET-CONFIG-MIB is used to configure the IP address of an interface.

Table C-76. PDN-INET-MIB Objects

Object	OID	Syntax	Access	Status	Supported
pdnInetTelnetServerPort	{ pdnInetMIBObjects 1 }	INTEGER	read-write	current	No
pdnInetFtpServerControlPort	{ pdnInetMIBObjects 2 }	INTEGER	read-write	current	No
pdnInetFtpServerDataPort	{ pdnInetMIBObjects 3 }	INTEGER	read-write	current	No
pdnInetIpAddressTableMaxIp-Subnets	{ pdnInetMIBObjects 4 }	Integer32	read-only	current	No
pdnInetIpAddressTable-CurrentIpSubnets	{ pdnInetMIBObjects 5 }	Integer32	read-only	current	No
pdnInetIpAddressTable	{ pdnInetMIBObjects 6 }	SEQUENCE OF pdnInetIpAddress-TableEntry	not-accessible	current	Yes

pdnInetIpAddressTable Group

The pdnInetIpAddressTable comprises the following objects:

Table C-77. pdnInetIpAddressTable

Object	OID	Syntax	Access	Status	Supported
pdnInetIpAddress	{ pdnInetIpAddress-TableEntry 1 }	IpAddress	not-accessible	current	Yes
pdnInetIpSubnetMask	{ pdnInetIpAddress-TableEntry 2 }	IpAddress	read-create	current	Yes
pdnInetIpAddressType	{ pdnInetIpAddress-TableEntry 3 }	INTEGER	read-create	current	Yes
pdnInetIpRowStatus	{ pdnInetIpAddress-TableEntry 4 }	RowStatus	read-create	current	Yes
pdnInetIpGateway	{ pdnInetIpAddress-TableEntry 5 }	IpAddress	read-create	current	Yes

PDN-SYSLOG-MIB

The PDN-SYSLOG-MIB is used to implement a system log.

Table C-78. PDN-SYSLOG-MIB Objects

Object	OID	Syntax	Access	Status	Supported
pdnSyslogStatus	{ pdnSyslog 1 }	INTEGER	read-write	current	Yes
pdnSyslogIPAddr	{ pdnSyslog 2 }	IpAddress	read-write	current	Yes
pdnSyslogLevel	{ pdnSyslog 3 }	INTEGER	read-write	deprecated	Yes
pdnSyslogPort	{ pdnSyslog 4 }	Integer32	read-write	deprecated	Yes
pdnSyslogSeverityThreshold	{ pdnSyslog 5 }	INTEGER	read-write	current	Yes
pdnSyslogRemoteDaemon	{ pdnSyslog 6 }	INTEGER	read-write	current	No
pdnSyslogTable	{ pdnSyslog 7 }	SEQUENCE OF pdnSyslogEntry	not-accessible	current	Yes
pdnSyslogNumOfMsgInTable	{ pdnSyslog 8 }	Integer32	read-only	current	Yes
pdnSyslogMaxTableSize	{ pdnSyslog 9 }	Integer32	read-only	current	Yes
pdnSyslogClearTable	{ pdnSyslog 10 }	INTEGER	read-write	current	Yes
pdnSyslogMsgToConsole	{ pdnSyslog 11 }	INTEGER	read-write	current	Yes
pdnSyslogRateLimiting	{ pdnSyslog 12 }	INTEGER	read-write	current	Yes

PDN-UPLINK-TAGGING-MIB

The PDN-UPLINK-TAGGING-MIB describes the objects used to configure uplink tagging. See Table A-20, VLAN Tag Ranges, in Appendix A, *CLI Command Descriptions*, for the possible values of ultBaseVlanTag (Base) and ultIndex (Index).

PDN-STACKABLE-MIB

The PDN-STACKABLE-MIB defines objects used to administer a stackable product. The wanInterface object is supported, and may be one of:

- stackLink1 (0) – The WAN interface is the GigE Uplink port.
- plugInModule (2) – The WAN interface is the one supplied by the Management Module.

PDN-DEVICE-TIME-MIB

The PDN-DEVICE-TIME-MIB contains objects used to procure the date and time using SNTP. The devNTP group is fully supported.

OID Cross Reference

D

OID Numbers

The following table shows the OID Numbers for supported objects, in order by tag name.

Table D-1. OIDs for Supported Objects (1 of 4)

Tag	OID Number	MIB
adslAtucChanTable	1.3.6.1.2.1.10.94.1.1.4	ADSL Line MIB (RFC 2662)
adslAtucPerfDataExtTable	1.3.6.1.2.1.10.94.3.1.18	ADSL Line Extension MIB
adslAtucPerfDataTable	1.3.6.1.2.1.10.94.1.1.6	ADSL Line MIB (RFC 2662)
adslAtucPhysTable	1.3.6.1.2.1.10.94.1.1.2	ADSL Line MIB (RFC 2662)
adslAturChanTable	1.3.6.1.2.1.10.94.1.1.5	ADSL Line MIB (RFC 2662)
adslAturPerfDataExtTable	1.3.6.1.2.1.10.94.3.1.20	ADSL Line Extension MIB
adslAturPerfDataTable	1.3.6.1.2.1.10.94.1.1.7	ADSL Line MIB (RFC 2662)
adslAturPhysTable	1.3.6.1.2.1.10.94.1.1.3	ADSL Line MIB (RFC 2662)
adslConfProfileExtTable	1.3.6.1.2.1.10.94.3.1.22	ADSL Line Extension MIB
adslLineConfProfileTable	1.3.6.1.2.1.10.94.1.1.14	ADSL Line MIB (RFC 2662)
adslLineExtTable	1.3.6.1.2.1.10.94.3.1.17	ADSL Line Extension MIB
adslLineTable	1.3.6.1.2.1.10.94.1.1.1	ADSL Line MIB (RFC 2662)
atmfM4TcACellScrambling	1.3.6.1.4.1.353.5.1.3.1.1.7.1.1	SNMP M4 Network Element View MIB
atmInterfaceTCTable	1.3.6.1.2.1.37.1.4	ATM MIB (RFC 2515)
atmVclTable	1.3.6.1.2.1.37.1.7	ATM MIB (RFC 2515)
devConfigTestTimer	1.3.6.1.4.1.1795.2.24.2.7.2	pdn_Config
devConfigTime	1.3.6.1.4.1.1795.2.24.2.7.8	pdn_Config
devConfiguration	1.3.6.1.4.1.1795.2.24.2.7.10	pdn_Config
devControlFTP	1.3.6.1.4.1.1795.2.24.2.10.6	pdn_Control

Table D-1. OIDs for Supported Objects (2 of 4)

Tag	OID Number	MIB
devFileXferMIBObjects	1.3.6.1.4.1.1795.2.24.2.10.7	pdn_Control
devFirmwareControlMIBObjects	1.3.6.1.4.1.1795.2.24.2.10.9	pdn_Control
devNTP	1.3.6.1.4.1.1795.2.24.2.20.1.2	pdn_device_time
diagTestMibTraps	1.3.6.1.4.1.1795.2.24.2.16.2	pdn_diagnostics
dot1dBaseNumPorts	1.3.6.1.2.1.17.1.2	Bridge MIB (RFC 1483)
dot1dBaseType	1.3.6.1.2.1.17.1.3	Bridge MIB (RFC 1483)
dot1dTpAgingTime	1.3.6.1.2.1.17.4.2	Bridge MIB (RFC 1483)
dot1dTpFdbTable	1.3.6.1.2.1.17.4.3	Bridge MIB (RFC 1483)
dot1dTpPortTable	1.3.6.1.2.1.17.4.4	Bridge MIB (RFC 1483)
dot3PauseTable	1.3.6.1.2.1.10.7.10	Ethernet-Like MIB (RFC 2665)
dot3StatsTable	1.3.6.1.2.1.10.7.2	Ethernet-Like MIB (RFC 2665)
entAliasMappingTable	1.3.6.1.2.1.47.1.3.2	Entity MIB (RFC 2737)
entLastChangeTime	1.3.6.1.2.1.47.1.4.1	Entity MIB (RFC 2737)
entPhysicalContainsTable	1.3.6.1.2.1.47.1.3.3	Entity MIB (RFC 2737)
entPhysicalTable	1.3.6.1.2.1.47.1.1.1	Entity MIB (RFC 2737)
ifJackTable	1.3.6.1.2.1.26.2.2	802.3 MAU MIB (RFC 2668)
ifMauAutoNegTable	1.3.6.1.2.1.26.5.1	802.3MAU MIB (RFC 2668)
ifMauTable	1.3.6.1.2.1.26.2.1	802.3 MAU MIB (RFC 2668)
ifNumber	1.3.6.1.2.1.2.1	Interfaces Group MIB (RFC 2863)
ifRcvAddressTable	1.3.6.1.2.1.31.1.4	Interfaces Group MIB (RFC 2863)
ifStackLastChange	1.3.6.1.2.1.31.1.6	Interfaces Group MIB (RFC 2863)
ifStackTable	1.3.6.1.2.1.31.1.2	Interfaces Group MIB (RFC 2863)
ifTable	1.3.6.1.2.1.2.2	Interfaces Group MIB (RFC 2863)
ifTableLastChange	1.3.6.1.2.1.31.1.5	Interfaces Group MIB (RFC 2863)
ifXTable	1.3.6.1.2.1.31.1.1	Interfaces Group MIB (RFC 2863)
ipAddrTable	1.3.6.1.2.1.4.20	SNMPv2 MIB for IP (RFC 2011)
ipCidrRouteAge	1.3.6.1.2.1.4.24.4.1.8	IP Forwarding Table MIB (RFC 2096)
ipCidrRouteDest	1.3.6.1.2.1.4.24.4.1.1	IP Forwarding Table MIB (RFC 2096)
ipCidrRouteIfIndex	1.3.6.1.2.1.4.24.4.1.5	IP Forwarding Table MIB (RFC 2096)
ipCidrRouteInfo	1.3.6.1.2.1.4.24.4.1.9	IP Forwarding Table MIB (RFC 2096)
ipCidrRouteMask	1.3.6.1.2.1.4.24.4.1.2	IP Forwarding Table MIB (RFC 2096)
ipCidrRouteNextHop	1.3.6.1.2.1.4.24.4.1.4	IP Forwarding Table MIB (RFC 2096)

Table D-1. OIDs for Supported Objects (3 of 4)

Tag	OID Number	MIB
ipCidrRouteNextHopAS	1.3.6.1.2.1.4.24.4.1.10	IP Forwarding Table MIB (RFC 2096)
ipCidrRouteProto	1.3.6.1.2.1.4.24.4.1.7	IP Forwarding Table MIB (RFC 2096)
ipCidrRouteStatus	1.3.6.1.2.1.4.24.4.1.16	IP Forwarding Table MIB (RFC 2096)
ipCidrRouteType	1.3.6.1.2.1.4.24.4.1.6	IP Forwarding Table MIB (RFC 2096)
ipDefaultTTL	1.3.6.1.2.1.4.2	SNMPv2 MIB for IP (RFC 2011)
ipForwarding	1.3.6.1.2.1.4.1	SNMPv2 MIB for IP (RFC 2011)
ipInReceives	1.3.6.1.2.1.4.3	SNMPv2 MIB for IP (RFC 2011)
mpeDevHealthAndStatusMIBObjects	1.3.6.1.4.1.1795.2.24.12.7.1	mpe_HealthAndStatus
mpeDevHealthAndStatusMIBTraps	1.3.6.1.4.1.1795.2.24.12.7.2	mpe_HealthAndStatus
mpeDevHwControl	1.3.6.1.4.1.1795.2.24.12.10.1.1	mpe_Control
mpeEntExtAlarms	1.3.6.1.4.1.1795.2.24.12.24.1.1	mpe_dslam
mpeEntitySensorMIBNotifications	1.3.6.1.4.1.1795.2.24.2.35.2.0	mpe_sensor
mpeEntSensorThresholds	1.3.6.1.4.1.1795.2.24.2.35.1.2	mpe_sensor
mpeEntSensorValues	1.3.6.1.4.1.1795.2.24.2.35.1.1	mpe_sensor
mpeSysDevDslamMIBTraps	1.3.6.1.4.1.1795.2.24.12.24.2	mpe_dslam
pdn_security	1.3.6.1.4.1.1795.2.24.2.8	pdn_security
pdnAtmStat	1.3.6.1.4.1.1795.2.24.2.6.11.3.3	pdn_AtmStats
pdnConfigChangeMgmt	1.3.6.1.4.1.1795.2.24.2.10.10	pdn_Control
pdnControl	1.3.6.1.4.1.1795.2.24.2.10	pdn_Control
pdnControlMIBTrapsV2	1.3.6.1.4.1.1795.2.24.2.10.0	pdn_Control
pdnIfExtEncapConfig	1.3.6.1.4.1.1795.2.24.2.6.12.3	pdnIfExt
pdnInetMIBObjects	1.3.6.1.4.1.1795.2.24.2.26.1	pdn_inet
pdnIPSecConfig	1.3.6.1.4.1.1795.2.24.2.34.1.1.1	pdn_IPSec
pdnIPSecConnectionConfig	1.3.6.1.4.1.1795.2.24.2.34.1.1.1.1.3	pdn_IPSec
pdnIPSecKeyConfig	1.3.6.1.4.1.1795.2.24.2.34.1.1.1.1.1	pdn_IPSec
pdnIPSecSPDConfig	1.3.6.1.4.1.1795.2.24.2.34.1.1.1.1.2	pdn_IPSec
pdnNetToMediaConfig	1.3.6.1.4.1.1795.2.24.2.27.1.2	pdn_Arp
pdnNetToMediaMIBTraps	1.3.6.1.4.1.1795.2.24.2.27.2	pdn_Arp
pdnPortConfigMauExtMIBObject	1.3.6.1.4.1.1795.2.24.2.18.1.3	pdn_ether
pdnSyslog	1.3.6.1.4.1.1795.2.24.2.31.1	pdn_syslog
pdnUplinkTaggingObjects	1.3.6.1.4.1.1795.2.24.2.37.1	pdn_uplink_tagging
pdnVpnConfig	1.3.6.1.4.1.1795.2.24.2.34.1	pdn_IPSec

Table D-1. OIDs for Supported Objects (4 of 4)

Tag	OID Number	MIB
pppLinkStatusTable	1.3.6.1.2.1.10.23.1.1.1	PPP/LCP MIB (RFC 1471)
rs232AsyncPortTable	1.3.6.1.2.1.10.33.3	RS-232-Like MIB (RFC 1659)
rs232InSigTable	1.3.6.1.2.1.10.33.5	RS-232-Like MIB (RFC 1659)
rs232Number	1.3.6.1.2.1.10.33.1	RS-232-Like MIB (RFC 1659)
rs232OutSigTable	1.3.6.1.2.1.10.33.6	RS-232-Like MIB (RFC 1659)
rs232PortTable	1.3.6.1.2.1.10.33.2	RS-232-Like MIB (RFC 1659)
rs232SyncPortExtMIBObject	1.3.6.1.4.1.1795.2.24.2.6.6.6	pdn_SyncPortStats
rs232SyncPortTable	1.3.6.1.2.1.10.33.4	RS-232-Like MIB (RFC 1659)
snmpInASNParseErrs	1.3.6.1.2.1.11.6	MIB for SNMPv2 (RFC 1907)
snmpInBadCommunityNames	1.3.6.1.2.1.11.4	MIB for SNMPv2 (RFC 1907)
snmpInBadCommunityUses	1.3.6.1.2.1.11.5	MIB for SNMPv2 (RFC 1907)
snmpInBadVersions	1.3.6.1.2.1.11.3	MIB for SNMPv2 (RFC 1907)
snmpInPkts	1.3.6.1.2.1.11.1	MIB for SNMPv2 (RFC 1907)
snmpProxyDrops	1.3.6.1.2.1.11.32	MIB for SNMPv2 (RFC 1907)
snmpSilentDrops	1.3.6.1.2.1.11.31	MIB for SNMPv2 (RFC 1907)
sysContact	1.3.6.1.2.1.1.4	MIB for SNMPv2 (RFC 1907)
sysDescr	1.3.6.1.2.1.1.1	MIB for SNMPv2 (RFC 1907)
sysDevDslamMIBObjects	1.3.6.1.4.1.1795.2.24.2.24.1	pdn_dslam
sysDevDslamMIBTraps	1.3.6.1.4.1.1795.2.24.2.24.2	pdn_dslam
sysDevFilter	1.3.6.1.4.1.1795.2.24.2.23.1.1	pdn_filter
sysLocation	1.3.6.1.2.1.1.6	MIB for SNMPv2 (RFC 1907)
sysName	1.3.6.1.2.1.1.5	MIB for SNMPv2 (RFC 1907)
sysObjectID	1.3.6.1.2.1.1.2	MIB for SNMPv2 (RFC 1907)
sysServices	1.3.6.1.2.1.1.7	MIB for SNMPv2 (RFC 1907)
sysUpTime	1.3.6.1.2.1.1.3	MIB for SNMPv2 (RFC 1907)
wanInterface	1.3.6.1.4.1.1795.2.24.2.36.1.1	pdn_stackable

CLI to MIB Object Cross Reference

E

The following table shows the MIB objects used to implement CLI parameters.

Table E-1. CLI Command to Object ID Cross Reference (1 of 17)

CLI Command	Element	MIB Object	MIB
Clear management snmp *nms-address*	nms-address	securityMgrIpAddress	pdn_security
Clear management snmp *nms-traps*	nms-traps	devSecurityTrapIpAddress	pdn_security
Clear syslog	Clear syslog	pdnSyslogClearTable	pdn_syslog
Configure bridge clear	Clear	dot1dStaticStatus	RFC 1493
Configure *bridge mode*	Mode	ipNetToMediaForwardingMode	pdn_Arp
Configure *bridge timeout*	Bridge timeout	dot1dTpAgingTime	RFC 1493
Configure date	DateAndTime	devConfigTimeOfDay	pdn_Config
Configure date-timezone	Time zone	devConfigTimeOfDay	pdn_Config
Configure *factory*	Default nvram settings	pdnCCMOperation	pdn_control
Configure filter	Status	sysDevFilterBinidngAdminStatus	pdn_filter
Configure filter create/modify *def_action*	Default Action	sysDevDefFilterAction	pdn_filter
Configure filter create/modify *filter_name*	Name	sysDevFilterName	pdn_filter
Configure filter delete	Delete	sysDevFilterRowStatus	pdn_filter
Configure filter *rule-name*	Rule name	sysDevLayerTwoFilterRuleName OR sysDevLayerThreeFilterRuleName	pdn_filter
Configure filter-binding create *filter_name*	Name	sysDevFilterName (through sysDevFilterBindingIndex that is mapped to sysDevFilterIndex)	pdn_filter
Configure filter-binding create *filter-direction*	Direction	sysDevFilterBindingDirection	pdn_filter

Table E-1. CLI Command to Object ID Cross Reference (2 of 17)

CLI Command	Element	MIB Object	MIB
Configure filter-binding create *port-id*	Interface	ifIndex	RFC 2233
Configure filter-binding delete	Delete	sysDevFilterBindingRowStatus	pdn_filter
Configure filter-rule create/modify *options*	Options	sysDevLayerTwoFilterRuleEther-TypeRangeStarts (and sysDevLayerTwoFilterRuleEther-TypeRangeEnds)	pdn_filter
Configure filter-rule create/modify *rule_action*	Action	sysDevLayerTwoFilterRuleAction Or sysDevLayerThreeFilterRuleAction	pdn_filter
Configure filter-rule create/modify *rule_name*	Rule name	sysDevLayerTwoFilterRuleName OR sysDevLayerThreeFilterRuleName	pdn_filter
Configure filter-rule create/modify *rule-type*	EtherType	sysDevLayerTwoFilterRuleEther-FrameType	pdn_filter
Configure filter-rule delete	Delete	sysDevLayerTwoFilterRuleRowStatus Or sysDevLayerThreeFilterRuleRowStatus	pdn_filter
Configure interface console *data-bits*	DataBits	rs232AsyncPortBits	RFC 1659
Configure interface console *parity*	Parity	rs232AsyncPortParity	RFC 1659
Configure interface console *rate*	Speed	rs232PortOutSpeed	RFC 1659
Configure interface console *stop-bits*	StopBits	rs232AsyncStopBits	RFC 1659
Configure interface dsl	State	ifAdminStatus	RFC 2233
Configure interface dsl *behavior*	Behavior	adslAtucConfRateMode	ADSL Line MIB
Configure interface dsl atm *data-connection (VCI)*	VCI	atmVclVci	Atm Management Objects MIB
Configure interface dsl atm *data-connection (VPI)*	VPI	atmVclVpi	Atm Management Objects MIB
Configure interface dsl atm *encapsulation*	Encapsulation	atmVccAal5EncapType	ATM management Objects MIB
Configure interface dsl *latency*	Latency	adslConfProfileLineType	Ext to ADSL Line MIB
Configure interface dsl *line code*	Line Code	adslLineTransAtucConfig	Ext to ADSL Line MIB
Configure interface dsl l*ink Up/Down Trap*	Link Up/Down trap	ifLinkUpDownTrapEnable	Ext to MIB-II

Table E-1. CLI Command to Object ID Cross Reference (3 of 17)

CLI Command	Element	MIB Object	MIB
Configure interface dsl *max-downstream speed*	Maximum Downrate for fast ADSL ifType	adslAtucChanConfFastMaxTxRate	ADSL Line Mib
Configure interface dsl *max-downstream speed*	Maximum Downrate for interleave ADSL ifType	adslAtucChanConfInterleaveMaxTx-Rate	ADSL Line Mib
Configure interface dsl *max-upstream speed*	Maximum Uprate for fast ADSL ifType	adslAturChanConfFastMaxTxRate	ADSL Line Mib
Configure interface dsl *max-upstream speed*	Maximum Uprate for interleave ADSL ifType	adslAturChanConfInterleaveMaxTx-Rate	ADSL Line Mib
Configure interface dsl *min-downstream speed*	Minimum Downrate for fast ADSL ifType	adslAtucChanConfFastMinTxRate	ADSL Line Mib
Configure interface dsl *min-downstream speed*	Minimum Downrate for interleave ADSL ifType	adslAtucChanConfInterleaveMinTx-Rate	ADSL Line Mib
Configure interface dsl *minimum margin*	Minimum Margin	adslAturMinSnrMargin	ADSL Line Mib
Configure interface dsl *min-upstream speed*	Minimum Uprate for interleave ADSL ifType	adslAturChanConfInterleaveMinTxRate	ADSL Line Mib
Configure interface dsl *min-upstream speed*	Minimum Uprate for fast ADSL ifType	adslAturChanConfFastMinTxRate	ADSL Line Mib
Configure interface dsl *name*	name	ifAlias	RFC 2233
Configure interface dsl *target downstream margin*	Target downstream Margin	adslAturConfTargetMargin	ADSL Line Mib
Configure interface dsl *target upstream margin*	Target upstream Margin	adslAtucConfTargetMargin	ADSL Line Mib
Configure interface ethernet *mode*	Mode	ifMauDefaultType	RFC 2668
Configure interface ethernet *auto-neg*	Autonegotia-tion enabled/ disabled	ifMauAutoNegAdminStatus	RFC 2668
Configure interface ethernet *connector*	Connector	pdnActiveJack	pdn_ether MIB

Table E-1. CLI Command to Object ID Cross Reference (4 of 17)

CLI Command	Element	MIB Object	MIB
Configure interface ethernet *flow-control*	Flow	dot3PauseAdminMode	RFC 2665
Configure interface ethernet *xover*	MDI/MDIX	pdnPortConfigXover	pdn_ether
Configure interface modem *data-bits*	DataBits	rs232AsyncPortBits	RFC 1659
Configure interface modem *parity*	Parity	rs232AsyncPortParity	RFC 1659
Configure interface modem *rate*	Speed	rs232PortOutSpeed	RFC 1659
Configure interface modem *stop-bits*	StopBits	rs232AsyncStopBits	RFC 1659
Configure interface v35	Status	ifAdminStatus	RFC 2233
Configure interface v35 *clock source*	Clock source	rs232SyncPortClockSource	RFC 1659
Configure interface v35 *flag*	Flag	Rs232SyncPortIdlePatter	RFC 1659
Configure interface v35 *flow-control*	Flow-control	rs232PortOutFlowType	RFC 1659
Configure interface v35 *invert-tx-clock*	Invert-Tx-Clock	rs232SyncPortInvertTxClk	pdn_SyncPortStats
Configure interface v35 *link type*	Link Type	rs232PortType	RFC 1659
Configure interface v35 *rate*	Speed	rs232PortOutSpeed	RFC 1659
Configure ip nhr *ip-address*	ip-address	ipNetToMediaDefaultNHR	pdn_Arp MIB
Configure management *gateway*	gateway	pdnInetIpGateway	pdn_inet MIB
Configure management *address*	IP address	pdnInetIpAddress	pdn_inet MIB
Configure management connection default *des-key*	des-key	pdnUsrConfigIpSecKey	pdn_IpSecManual.mib
Configure management connection default *ah-alg*	ah-alg	pdnUsrIpSecKeySetupAlg	pdn_IpSecManual.mib
Configure management connection default *ah-md5-key*	ah-md5-key	pdnUsrConfigIpSecKey	pdn_IpSecManual.mib
Configure management connection default *ah-sha1-key*	ah-sha1-key	pdnUsrConfigIpSecKey	pdn_IpSecManual.mib
Configure management connection default *encryption*	encryption	pdnUsrIpSecKeySetupAlg	pdn_IpSecManual.mib
Configure management connection default *esp-alg*	esp-alg	pdnUsrIpSecKeySetupAlg	pdn_IpSecManual.mib
Configure management connection default *esp-md5-key*	esp-md5-key	pdnUsrConfigIpSecKey	pdn_IpSecManual.mib

Table E-1. CLI Command to Object ID Cross Reference (5 of 17)

CLI Command	Element	MIB Object	MIB
Configure management connection default *esp-sha1-key*	esp-sha1-key	pdnUsrConfigIpSecKey	pdn_IpSecManual.mib
Configure management connection modify *algoirithm*	algorithm	pdnIPSecConnectionIPSecAH-InboundAuthenticationAlg OR pdnIPSecConnectionIPSecAH-OutboundAuthenticationAlg OR pdnIPSecConnectionIPSecESP-InboundAuthenticationAlg OR pdnIPSecConnectionIPSecESP-OutboundAuthenticationAlg	pdn_IpSecManual.mib
Configure management connection modify *algorithm-key*	algorithm-key	pdnIPSecConnectionIPSecAH-InboundAuthenticationKey OR pdnIPSecConnectionIPSecAH-OutboundAuthenticationKey OR pdnIPSecConnectionIPSecESP-InboundAuthenticationKey OR pdnIPSecConnectionIPSecESP-OutboundAuthenticationKey	pdn_IpSecManual.mib
Configure management connection modify *antireplay*	antireplay	pdnIPSecConnectionAntiReplay	pdn_IpSecManual.mib
Configure management connection modify *encryption*	encryption	pdnIPSecConnectionIPSecESP-InboundEncryptionAlg OR pdnIPSecConnectionIPSecESP-OutboundEncryptionAlg	pdn_IpSecManual.mib
Configure management connection modify *encryption-key*	encryption-key	pdnIPSecConnectionIPSecESP-InboundEncryptionKey OR pdnIPSecConnectionIPSecESP-OutboundEncryptionKey	pdn_IpSecManual.mib
Configure management connection modify *protocol*	protocol	pdnIPSecConnectionTransform	pdn_IpSecManual.mib
Configure management connection modify *remote-host-address*	Remote-host-address	pdnIPSecConnectionRemoteHost-Address	pdn_IpSecManual.mib
Configure management connection modify *remote-tunnel-address*	Remote-tunnel-address	pdnIPSecConnectionTunnelEndpoint-RemoteIpAddr	pdn_IpSecManual.mib
Configure management connection modify *spi*	spi	pdnIPSecConnectionIPSecAH-InboundSPI OR pdnIPSecConnectionIPSecAH-OutboundSPI OR pdnIPSecConnectionIPSecESP-InboundSPI OR pdnIPSecConnectionIPSecESP-OutboundSPI	pdn_IpSecManual.mib

Table E-1. CLI Command to Object ID Cross Reference (6 of 17)

CLI Command	Element	MIB Object	MIB
Configure management ipsec connection *create*	create	pdnIPSecConnectionRowStatus	pdn_IpSecManual.mib
Configure management ipsec connection *delete*	delete	pdnIPSecConnectionRowStatus	pdn_IpSecManual.mib
Configure management ipsec *disable*	disable	pdnUsrConfigIPSec	pdn_IpSecManual.mib
Configure management ipsec *enable*	enable	pdnUsrConfigIPSec	pdn_IpSecManual.mib
Configure management ipsec *local-tunnel-address*	Local-tunnel-address	pdnUsrConfigLocalTunnelEndpoint-IPAddr	pdn_IpSecManual.mib
Configure management snmp *access-validation*	Access validation	devSecurityMgrValidation	pdn_security
Configure management snmp *nms-address*	Nms address	securityMgrIpAddress	pdn_security
Configure management snmp *nms-traps*	Nms traps destination	devSecurityTrapIpAddress	pdn_security
Configure management snmp *private-string*	Private community string	communityName and communityType	pdn_dslam
Configure management snmp *public-string*	Public community string	entCommunityName and entCommunityType	pdn_dslam
Configure management snmp *state*	state	securityMgrAccess	pdn_security
Configure management *subnet*	subnet	pdnInetIpSubnetMask	pdn_inet
Configure management *vlan*	mgmt-vlan	dot1qVlanIndex	RFC 2674
Configure scheduler	State	pdnCCMAutoBackupType	pdn_control
Configure scheduler dymanic *time*	Time Dymanic	pdnCCMAutoBackupDynamicTime	pdn_control
Configure scheduler fixed *day-of-week*	Day-of-week	pdnCCMAutoBackupFixedDay	pdn_control
Configure scheduler fixed *time*	Time fixed	pdnCCMAutoBackupFixedTime	pdn_control
Configure scheduler ftp *filename*	filename	pdnCCMAutoBackupFilename	pdn_control
Configure scheduler ftp *ip-address*	IP addres	pdnCCMAutoBackupServerIpAddress	pdn_control
Configure scheduler ftp *password*	password	pdnCCMAutoBackupUserPassword	pdn_control
Configure scheduler ftp *user-name*	User name	pdnCCMAutoBackupUserName	pdn_control

Table E-1. CLI Command to Object ID Cross Reference (7 of 17)

CLI Command	Element	MIB Object	MIB
Configure scheduler timestamp	timestamp	pdnCCMAutoBackupAppendTime-StampToFilename	pdn_control
Configure security ip	State	ipNetToMediaLimitEnabled	pdn_Arp
Configure security ip add *nhr*	nhr	ipNetToMediaNHR	pdn_Arp
Configure security ip add/delete *adress*	Ip address	ipNetToMediaNetAddress	RFC 2011
Configure security ip delete	delete	ipNetToMediaType	RFC 2011
Configure security ip *max-ip*	Max-ip	ipNetToMediaMaxIPAddresses	pdn_Arp
Configure security mac add/delete *mac-address*	Add mac address	dot1dStaticAddress	RFC 1493
Configure security mac delete	Delete Mac address	dot1dStaticStatus	RFC 1493
Configure sntp	State	devNTPEnable	pdn_time MIB
Configure sntp *interval*	interval	devNTPSynchronised	pdn_time MIB
Configure sntp *ip-address*	ip-address	devNTPServerIp	pdn_time MIB
Configure syslog *rate-limiting*	Rate limiting	pdnSyslogRateLimiting	pdn_syslog
Configure syslog *threshold*	Syslog threshold	pdnSyslogSeverityThreshold	pdn_syslog
Configure system information *system-location*	System Location	sysLocation	RFC 1213
Configure system information *system-name*	System name	sysName	RFC 1213
Configure system options *date-display-format*	Date display format	devConfigDateDisplayFormat	pdn_Config
Configure system options *inactivity timeout*	Inactivity timeout	devConfigComDiscTime	pdn_Config
Configure system options *port-display-format*	Port display format	devConfigPortNumDisplayFormat	pdn_Config
Configure system options *test-timeout*	Test timeout	devConfigTestDuration	pdn_Config
Configure uplink	uplink	wanInterface	PDN-STACKABLE-MIB
Configure uplink-tag *base*	base	ultBaseVlanTag	PDN-UPLINK-TAGGING-MIB
Configure uplink-tag *index*	index	ultIndex	PDN-UPLINK-TAGGING-MIB
Copy ftp startup-config *filename*	filename	pdnDevFileXferFileName	pdn_control
Copy ftp startup-config *ip-address*	Ip address	pdnDevFileXferServerIpAddress	pdn_control

Table E-1. CLI Command to Object ID Cross Reference (8 of 17)

CLI Command	Element	MIB Object	MIB
Copy ftp startup-config *password*	Password	pdnDevFileXferUserPassword	pdn_control
Copy ftp startup-config *user-name*	User name	pdnDevFileXferUserName	pdn_control
Copy startup-config running-config	Reset	pdnCCMOperation	pdn_control
Copy starup-config ftp *filename*	filename	pdnDevFileXferFileName	pdn_control
Copy starup-config ftp *ip-address*	Ip address	pdnDevFileXferServerIpAddress	pdn_control
Copy starup-config ftp *password*	password	pdnDevFileXferUserPassword	pdn_control
Copy starup-config ftp *user-name*	User-name	pdnDevFileXferUserName	pdn_control
Firmware download *apply*	apply	pdnDevFileXferApply	pdn_control
Firmware download *filename*	filename	pdnDevFileXferFileName	pdn_control
Firmware download *ip-address*	Ip address	pdnDevFileXferServerIpAddress	pdn_control
Firmware download *password*	password	pdnDevFileXferUserPassword	pdn_control
Firmware download *username*	username	pdnDevFileXferUserName	pdn_control
Firmware download-status	status	pdnDevFileXferStatus	pdn_control
firmware revision	revision	devFirmwareControlRelease	pdn_control
firmware switch	switch	devFirmwareControlAdminStatus	pdn_control
restart unit	restart	mpeDevControlReset	mpe_control
save	Save	pdnCCMOperation	pdn_control
Show bridge *interface*	ifIndex	IfIndex	RFC 1213
Show bridge *mac*	MAC address	dot1dTpFdbAddress	RFC 1493
Show bridge *status*	Status	dot1dTpFdbStatus	RFC 1493
Show bridge *timeout*	Timeout	dot1dTpAgingTime	RFC 1493
Show *date*	Date and Time	devConfigTimeOfDay	pdn_Config
Show filter *default action*	Action	sysDevDefFilterAction	pdn_filter
Show filter *filter-name*	Filter name	sysDevFilterName	pdn_filter
Show filter *type*	Type	sysDevFilterType	pdn_filter
Show filter-binding *direction*	Direction	sysDevFilterBindingDirection	pdn_filter
Show filter-binding *filter-name*	Filter Name	sysDevFilterName (through sysDevFilterBindingIndex that is mapped to ifIndex)	pdn_filter
Show filter-binding *port-id*	Interface	ifIndex	MIB-II

Table E-1. CLI Command to Object ID Cross Reference (9 of 17)

CLI Command	Element	MIB Object	MIB
Show filter-rule *action*	Action	sysDevLayerTwoFilterRuleAction OR sysDevLayerThreeFilterRuleAction	pdn_filter
Show filter-rule *ifIndex*	Interface	ifIndex	MIB-II
Show filter-rule *rule*	Rule	sysDevLayerTwoFilterRuleEtherType-RangeStarts and sysDevLayerTwoFilterRuleEtherType-RangeEnds	pdn_filter
Show filter-rule *rule-name*	Rule-name	sysDevLayerTwoFilterRuleName OR sysDevLayerThreeFilterRuleName	pdn_filter
Show information *FW revision*	Fw rev	entPhysicalFirmwareRev	RFC 2737
Show interface console *data-bits*	DataBits	rs232AsyncPortBits	RFC 1659
Show interface console *link rate*	Speed	rs232PortOutSpeed	RFC 1659
Show interface console *parity*	Parity	rs232AsyncPortParity	RFC 1659
Show interface console *stop-bits*	StopBits	rs232AsyncStopBits	RFC 1659
Show interface console *uptime*	Current link up time	SysUpTime - ifLastChange	RFC 1213
Show interface dsl *latency*	Latency	adslLineType	ADSL Line MIB
Show interface dsl *link*	Oper state	ifOperStatus	MIB-II
Show interface dsl atm *data-connection VCI*	VCI	atmVclVci	Atm Management Objects MIB
Show interface dsl atm *data-connection VPI*	VPI	atmVclVpi	Atm Management Objects MIB
Show interface dsl atm *encapsulation*	Encapsulation	atmVccAal5EncapType	ATM management Objects MIB
Show interface dsl down *attainable rate*	Attainable speed	adslAturCurrAttainableRate	ADSL Line MIB
Show interface dsl *down attenuation*	Down attenuation	adslAturCurrAtn	ADSL Line MIB
Show interface dsl *down rate*	Downstream Speed	adslAtucChanCurrTxRate	RFC 2662
show interface dsl *index*	Port Index	ifIndex	ADSL Line MIB
Show interface dsl *line-code*	Line Code	adslLineCoding	ADSL Line MIB
Show interface dsl *link Up/Down Trap*	Link Up/Down trap	ifLinkUpDownTrapEnable	Ext to MIB-II
Show interface dsl *name*	name	ifAlias	RFC 2233
Show interface dsl statistics atm *curr cells RX*	Total Cells Received	pdnAtmVclStatTotalCellIns	pdn_atmstat MIB

Table E-1. CLI Command to Object ID Cross Reference (10 of 17)

CLI Command	Element	MIB Object	MIB
Show interface dsl statistics atm *curr cells TX*	Total Cells Sent	pdnAtmVclStatTotalCellOuts	pdn_atmstat MIB
Show interface dsl statistics atm *curr OCD*	OCD Events	pdnAtmStatLCDErrors	pdn_atmstat MIB
Show interface dsl statistics atm *up HEC*	Total up HEC	pdnAtmStatHECErrors	pdn_atmstat MIB
Show interface dsl *statistics down ES*	Down Error Seconds (ES)	adslAturPerfESs	ADSL Line MIB
Show interface dsl *statistics up ES*	Up Error Seconds (ES)	adslAtucPerfESs	ADSL Line MIB
Show interface dsl *statistics up SES*	Up Severely Error Seconds (SES)	adslAtucPerfStatSesL	Ext to ADSL Line MIB
Show interface dsl *statistics up UAS*	Up unavailable seconds (UAS)	adslAtucPerfStatUasL	Ext to ADSL Line MIB
Show interface dsl *statistics day LPRS*	Sn Loss of Power	adslAturPerfLprs	ADSL Line MIB
Show interface dsl *statistics down SES*	Down Severely Error Seconds (SES)	adslAturPerfStatSesL	Ext to ADSL Line MIB
Show interface dsl *statistics down UAS*	Down Unavailable Error Seconds (UAS)	adslAturPerfStatUasL	Ext to ADSL Line MIB
Show interface dsl up *attainable rate*	Attainable speed	adslAtucCurrAttainableRate	ADSL Line MIB
Show interface dsl *up attenuation*	Up attenuation	adslAtucCurrAtn	ADSL Line MIB
Show interface dsl *up margin*	Up Margin	adslAtucCurrSnrMgn	ADSL Line MIB
Show interface dsl *up rate*	Upstream speed	adslAturChanCurrTxRate	RFC 2662
Show interface dsl *uptime*	Current link up time	SysUpTime - ifLastChange	RFC 1213
Show interface ethernet *link*	Link status	ifOperStatus	RFC 2233
Show interface ethernet *connector*	Connector Type	ifJackType	RFC 2668
Show interface ethernet *flow*	Flow	dot3PauseOperMode	RFC 2665
Show interface ethernet *frames discarded*	Total frames discarded	iInDiscards + ifOutDiscards	RFC 2233

Table E-1. CLI Command to Object ID Cross Reference (11 of 17)

CLI Command	Element	MIB Object	MIB
Show interface ethernet *frames Rx broadcast*	Total broadcast Rx	ifInBroadcastPkts	RFC 2233
Show interface ethernet *frames Rx multicast*	Total multicast Rx	ifInMulticastPkts	RFC 2233
Show interface ethernet *link up time*	Link up time	SysUpTime - ifLinkChange	RFC 1213
Show interface ethernet *mode*	Mode	dot3StatsDuplexStatus	RFC 2665
Show interface ethernet *rate*	Speed	ifSpeed	RFC 2233
Show interface ethernet *total bytes Rx*	Total bytes Rx	ifInOctets	RFC 2233
Show interface ethernet *total bytes Tx*	Total bytes Tx	IfOutOctets	RFC 2233
Show interface ethernet *total frames Rx*	Total Frames Rx	IfInUnicastPkts + ifInBroadcastPkts + ifInMulticastPkts	RFC 2233
Show interface ethernet *total frames Tx*	Total Frames Tx	IfOutcastPkts + ifOutastPkts + ifOutticastPkts	RFC 2233
Show interface ethernet *xover*	Xover	pdnPortConfigXover	pdn_ether
Show interface modem *data-bits*	DataBits	rs232AsyncPortBits	RFC 1659
Show interface modem *link rate*	Speed	rs232PortOutSpeed	RFC 1659
Show interface modem *parity*	Parity	rs232AsyncPortParity	RFC 1659
Show interface modem *stop-bits*	StopBits	rs232AsyncStopBits	RFC 1659
Show interface modem *uptime*	Current link up time	xdslDevIfStatsElapsedTimeLinkUp	hot_xdsl
Show interface v35 *clock source*	Clock source	rs232SyncPortClockSource	RFC 1659
Show interface v35 *CRC Errors*	CRC Errors	rs232SyncPortFrameCheckErrs	RFC 1659
Show interface v35 *flag*	Flag	rs232SyncPortMinFlags	RFC 1659
Show interface v35 *flow-control*	Flow-control	rs232PortOutFlowType	RFC 1659
Show interface v35 *interrupted frames*	Interrupted Frames	rs232SyncPortInterruptedFrames	RFC 1659
Show interface v35 *invert-tx-clock*	invert-tx-clock	rs232SyncPortInvertTxClock	pdn_SyncPortStats MIB
Show interface v35 *link rate*	Speed	rs232PortOutSpeed	RFC 1659
Show interface v35 *link status*	Link Status	ifOperStatus	RFC 1213
Show interface v35 *link type*	Link Type	rs232PortType	RFC 1659
Show interface v35 *Rx overrun erros*	Rx Overrun Errors	rs232SyncPortReceiveOverrunErrors	RFC 1659
Show interface v35 *signals*	Signals	rs232InSigName	RFC 1659

Table E-1. CLI Command to Object ID Cross Reference (12 of 17)

CLI Command	Element	MIB Object	MIB
Show interface v35 *Tx underrun errors*	Tx Underrun Errors	rs232SyncTransmitUnderrunErrors	RFC 1659
Show interface v35 *uptime*	Current link up time	SysUpTime - ifLastChange	RFC 1213
Show management arp ip-address	IP address	ipNetToMediaNetAddr	RFC 2011
Show management arp mac-address	MAC address	ipNetToMediaPhysAddress	RFC 2011
Show management arp type	Arp Type	ipNetToMediaType	RFC 2011
Show management connection default *ah-alg*	ah-alg	pdnUsrIpSecKeySetupAlg	pdn_IpSecManual.mib
Show management connection default *ah-md5-key*	ah-md5-key	pdnUsrConfigIpSecKey	pdn_IpSecManual.mib
Show management connection default *ah-sha1-key*	ah-sha1-key	pdnUsrConfigIpSecKey	pdn_IpSecManual.mib
Show management connection default *des-key*	des-key	pdnUsrConfigIpSecKey	pdn_IpSecManual.mib
Show management connection default *encryption*	encryption	pdnUsrIpSecKeySetupAlg	pdn_IpSecManual.mib
Show management connection default *esp-alg*	esp-alg	pdnUsrIpSecKeySetupAlg	pdn_IpSecManual.mib
Show management connection default *esp-md5-key*	esp-md5-key	pdnUsrConfigIpSecKey	pdn_IpSecManual.mib
Show management connection default *esp-sha1-key*	esp-sha1-key	pdnUsrConfigIpSecKey	pdn_IpSecManual.mib
Show management connection modify *algoirithm*	algorithm	pdnIPSecConnectionIPSecAH-InboundAuthenticationAlg OR pdnIPSecConnectionIPSecAH-OutboundAuthenticationAlg OR pdnIPSecConnectionIPSecESP-InboundAuthenticationAlg OR pdnIPSecConnectionIPSecESP-OutboundAuthenticationAlg	pdn_IpSecManual.mib
Show management connection modify *algorithm-key*	algorithm-key	pdnIPSecConnectionIPSecAH-InboundAuthenticationKey OR pdnIPSecConnectionIPSecAH-OutboundAuthenticationKey OR pdnIPSecConnectionIPSecESP-InboundAuthenticationKey OR pdnIPSecConnectionIPSecESP-OutboundAuthenticationKey	pdn_IpSecManual.mib

Table E-1. CLI Command to Object ID Cross Reference (13 of 17)

CLI Command	Element	MIB Object	MIB
Show management connection modify *antireplay*	antireplay	pdnIPSecConnectionAntiReplay	pdn_IpSecManual.mib
Show management connection modify *encryption*	encryption	pdnIPSecConnectionIPSecESP-InboundEncryptionAlg OR pdnIPSecConnectionIPSecESP-OutboundEncryptionAlg	pdn_IpSecManual.mib
Show management connection modify *encryption-key*	encryption-key	pdnIPSecConnectionIPSecESP-InboundEncryptionKey OR pdnIPSecConnectionIPSecESP-OutboundEncryptionKey	pdn_IpSecManual.mib
Show management connection modify *protocol*	protocol	pdnIPSecConnectionTransform	pdn_IpSecManual.mib
Show management connection modify *remote-host-address*	Remote-host-address	pdnIPSecConnectionRemoteHost-Address	pdn_IpSecManual.mib
Show management connection modify *remote-tunnel-address*	Remote-tunnel-address	pdnIPSecConnectionTunnelEndpoint-RemoteIpAddr	pdn_IpSecManual.mib
Show management connection modify *spi*	spi	pdnIPSecConnectionIPSecAH-InboundSPI OR pdnIPSecConnectionIPSecAH-OutboundSPI OR pdnIPSecConnectionIPSecESP-InboundSPI OR pdnIPSecConnectionIPSecESP-OutboundSPI	pdn_IpSecManual.mib
Show management ip *address*	Ip address	pdnInetIpAddress	pdn_inet MIB
Show management ip *subnet mask*	Subnet mask	pdnInetIpSubnetMask	pdn_inet MIB
Show management ipsec connection *create*	create	pdnIPSecConnectionRowStatus	pdn_IpSecManual.mib
Show management ipsec connection *delete*	delete	pdnIPSecConnectionRowStatus	pdn_IpSecManual.mib
Show management ipsec *disable*	disable	pdnUsrConfigIPSec	pdn_IpSecManual.mib
Show management ipsec *enable*	enable	pdnUsrConfigIPSec	pdn_IpSecManual.mib
Show management ipsec *local-tunnel-address*	Local-tunnel-address	pdnUsrConfigLocalTunnelEndpoint-IPAddr	pdn_IpSecManual.mib
Show management snmp *access-validation*	Access	devSecurityMgrValidation	pdn_security
Show management snmp *nms-address*	NMS ip addr	securityMgrIpAddress	pdn_security

Table E-1. CLI Command to Object ID Cross Reference (14 of 17)

CLI Command	Element	MIB Object	MIB
Show management snmp *nms-traps*	NMS traps	devSecurityTrapIpAddress	pdn_security
Show management snmp *private-string*	Private	entCommunityName and entCommunityType	pdn_dslam
Show management snmp *public-string*	Public	entCommunityName and entCommunityType	pdn_dslam
Show management snmp *state*	State	newSecurityMgrAccess	pdn_security
Show management *vlan*	mgmt-vlan	dot1qVlanIndex	RFC 2674 MIB
Show managemetn ip *gateway*	Gateway	pdnInetIpGateway	pdn_inet MIB
Show scheduler *filename*	Filename	pdnCCMAutoBackupFilename	pdn_Control
Show scheduler *mode*	mode	pdnCCMAutoBackupType	pdn_Control
Show scheduler *server*	Server	pdnCCMAutoBackupServerIpAddress	pdn_Control
Show scheduler *state*	State	pdnCCMAutoBackupType	pdn_Control
Show scheduler *time*	Time	pdnCCMAutoBackupFixedDay	pdn_Control
Show scheduler *time*	Time	pdnCCMAutoBackupFixedTime or pdnCCMAutoBackupDynamicTime	pdn_Control
Show security ip *address*	Ip address	ipNetToMediaNetAddress	RFC 2011
Show security ip *interface*	interface	ifIndex	RFC 1213
Show security ip *max-ip*	Max ip addresses	ipNetToMediaMaxIPAddresses	pdn_Arp
Show security ip *nhr*	nhr	ipNetToMediaNHR	pdn_Arp
Show security ip *state*	state	ipNetToMediaLimitEnabled	pdn_Arp
Show security ip *type*	Type	ipNetToMediaType	RFC 2011
Show security mac	status	dot1dStaticStatus	RFC 1493
Show security mac *address*	Mac address	dot1dStaticAddress	RFC 1493
Show sntp *interval*	interval	devNTPSynchronised	pdn_time MIB
Show sntp *ip-address*	ip-address	devNTPServerIp	pdn_time MIB
Show sntp *state*	State	devNTPEnable	pdn_time MIB
Show syslog *message*	message	pdnSyslogMesage	pdn_syslog
Show syslog *rate-limiting*	Rate limiting	pdnSyslogRateLimiting	pdn_syslog
Show syslog *threshold*	Threshold	pdnSyslogSeverityThreshold	pdn_syslog
Show system information *description*	Description	sysDescr	RFC 1213
Show system information *location*	Location	sysLocation	RFC 1213

Table E-1. CLI Command to Object ID Cross Reference (15 of 17)

CLI Command	Element	MIB Object	MIB
Show system information *name*	Name	sysName	RFC 1213
Show system information unit *location*	Unit Location	sysLocation	RFC 1213
Show system information unit *Model*	Model	entPhysicalModelName	RFC 2737
Show system information unit *name*	Unit Name	sysName	RFC 1213
Show system information unit *serial num*	Serial Number	entPhysicalSerialNum	RFC 2737
Show system information *uptime*	Unit Up Time	sysUpTime	RFC 1213
Show system options *date-display-format*	Date display format	devConfigDateDisplayFormat	pdn_Config
Show system options *port-number-display-format*	Port num display format	devConfigPortNumDisplayFormat	pdn_Config
Show system options *test-time-out*	Test timeout	devConfigTestTimeout and devConfigTestDuration	pdn_Config
Show system revisions *child card HW revision*	Child card hw revision	entPhysicalHardwareRev	RFC 2737
Show system revisions *description*	Unit description	sysDescr	RFC 1213
Show system revisions *location*	Unit location	sysLocation	RFC 1213
Show system revisions *main card HW revision*	Main card hardware revision	entPhysicalHardwareRev	RFC 2737
Show system revisions management module *hw revision*	Management hw revision	entPhysicalHardwareRev	RFC 2737
Show system revisions management module *model*	Management model	entPhysicalModelName	RFC 2737
Show system revisions management module *PLD (mgmt)*	PLD revision management	entPhysicalFirmwareRev	RFC 2737
Show system revisions management module *PLD (v.35)*	PLD revision v.35	entPhysicalFirmwareRev	RFC 2737
Show system revisions management module *revision*	Management revision	entPhysicalFirmwareRev	RFC 2737
Show system revisions management module *serial number*	Management serial number	entPhysicalSerialNum	RFC 2737
Show system revisions *model*	model	entPhysicalModelName	RFC 2737

Table E-1. CLI Command to Object ID Cross Reference (16 of 17)

CLI Command	Element	MIB Object	MIB
Show system revisions *PLD (main) revision*	PLD revision	entPhysicalFirmwareRev	RFC 2737
Show system revisions *revision*	revision	entPhysicalFirmwareRev	RFC 2737
Show system revisions *serial number*	Serial number	entPhysicalSerialNum	RFC 2737
Show system revisions *system description*	Description	sysDescr	RFC 1213
Show system revisions *system location*	Location	sysLocation	RFC 1213
Show system revisions *system name*	Name	sysName	RFC 1213
Show system revisions *unit-name*	Unit name	sysName	RFC 1213
Show system revisions *uptime*	Uptime	SysUpTime	RFC 1213
Show system *self-test results*	Self-test results	mpeDevSelfTestResults	mpe_HealthAndStatus
Show system status *fan1*	Fan1	fanModuleFailure Trap	pdn_dslam
Show system status *fan2*	Fan2	fanModuleFailure Trap	pdn_dslam
Show system status *fan3*	Fan3	fanModuleFailure Trap	pdn_dslam
Show system status *selftest*	selftest	mpeDeviceSelfTestFailure Trap	mpe_HealthAndStatus
Show system status *temp reading*	Temp reading	mpeEntSensorValue	mpe-sensor mib
Show system status *temperature*	Temperature	mpeEntSensorThresholdNotification	mpe-sensor mib
Show system status *uplink*	uplink	linkDown Trap	RFC 1573
Show system unit information *hardware rev*	Hardware Rev	entPhysicalHardwareRev	RFC 2737
Show system unit information *line code rev*	Line Code Rev	entPhysicalFirmwareRev	RFC 2737
Show system unit information *pld rev*	PLD Revision	entPhysicalFirmwareRev	RFC 2737
Show uplink	uplink	wanInterface	PDN-STACKABLE-MIB
Show uplink-tag *base*	base	ultBaseVlanTag	PDN-UPLINK-TAGGING-MIB
Show uplink-tag *index*	index	ultIndex	PDN-UPLINK-TAGGING-MIB

Table E-1. CLI Command to Object ID Cross Reference (17 of 17)

CLI Command	Element	MIB Object	MIB
show user-accounts *privilege*	Privilege	SysDevUserAccountPrivileged-Password (not displayed but accessed to verify that there is a password, in which case the user is an Administrator)	pdn_dslam
show user-accounts *user_name*	User Name	sysDevConfigUserAccountUserId	pdn_dslam
Show *users*	User id	loginUserId	pdn_dslam
Show *users line*	line	loginAccessApp	pdn_dslam
Show *users location*	location	loginAccessHost	pdn_dslam
Show vlans *hardware-address*	hardware-address	dot1qTpFdbAddress	RFC 2674 MIB
Show vlans *port-id*	port-id	dot1qTpFdbPort	RFC 2674 MIB
Show vlans *vlan-id*	vlan-id	dot1qVlanIndex	RFC 2674 MIB
Test dte-loopback *start*	Start	devControlTestCmd	pdn_Control mib
Test dte-loopback *stop*	Stop	devControlTestCmd	pdn_Control mib
Test *leds*	led test	devControlTest, devControlTestStatus, and devControlTestCmd	pdn_Control

Reference Tables

F

Time Zones

The following values are used by the **configure date** command. See *Configure Date* in Appendix A, *CLI Command Descriptions*.

Table F-1. Time Zone Names (1 of 3)

Time Zone Name	Description
gmt	Greenwich Mean Time, No Daylight Savings Time
us-eastern	GMT – 5, Subject to U.S. Daylight Savings Time Rules
us-indiana	GMT – 6, No Daylight Savings Time
us-central	GMT – 6, Subject to U.S. Daylight Savings Time Rules
us-mountain	GMT – 7, Subject to U.S. Daylight Savings Time Rules
us-arizona	GMT – 7, No Daylight Savings Time
us-pacific	GMT – 8, Subject to U.S. Daylight Savings Time Rules
us-alaska	GMT – 9, Subject to U.S. Daylight Savings Time Rules
us-aleutian	GMT – 10, Subject to U.S. Daylight Savings Time Rules
us-hawaii	GMT – 10, No Daylight Savings Time
us-samoa	GMT – 11, No Daylight Savings Time
canada-newfoundland	GMT – 3.5, Subject to Canadian Daylight Savings Time Rules
canada-atlantic	GMT – 4, Subject to Canadian Daylight Savings Time Rules
canada-eastern	GMT – 5, Subject to Canadian Daylight Savings Time Rules
canada-central	GMT – 6, Subject to Canadian Daylight Savings Time Rules
canada-east-saskatchewan	GMT – 6, No Daylight Savings Time
canada-mountain	GMT – 7, Subject to Canadian Daylight Savings Time Rules

Table F-1. Time Zone Names (2 of 3)

Time Zone Name	Description
canada-pacific	GMT – 8, Subject to Canadian Daylight Savings Time Rules
canada-yukon	GMT – 9, Subject to Canadian Daylight Savings Time Rules
mexico-bajanorte	GMT – 8, Subject to U.S. Daylight Savings Time Rules
mexico-bajasur	GMT – 7, No Daylight Savings Time
mexico-general	GMT – 6, No Daylight Savings Time
brazil-denoronha	GMT – 2, Subject to Brazilian Daylight Savings Time Rules
brazil-east	GMT – 3, Subject to Brazilian Daylight Savings Time Rules
brazil-west	GMT – 4, Subject to Brazilian Daylight Savings Time Rules
brazil-acre	GMT – 5, Subject to Brazilian Daylight Savings Time Rules
chile-continental	GMT – 4, Subject to Chilean Daylight Savings Time Rules
chile-easterisland	GMT – 6, Subject to Chilean Daylight Savings Time Rules
cuba	GMT – 5, Subject to Cuban Daylight Savings Time Rules
gb-erie	GMT, Subject to British Daylight Savings Time Rules
europe-western	GMT, Subject to Western European Daylight Savings Time Rules
europe-central	GMT + 1, Subject to Central European Daylight Savings Time Rules
europe-eastern	GMT + 2, Subject to Eastern European Daylight Savings Time Rules
australia-nsw	GMT + 10, Subject to Australian New South Wales Daylight Savings Time Rules
australia-yancowinna	GMT + 9.5, Subject to Australian New South Wales Daylight Savings Time Rules
australia-tasmania	GMT + 10, Subject to Tasmanian Daylight Savings Time Rules
australia-victoria	GMT + 10, Subject to Australian New South Wales Daylight Savings Time Rules
australia-queensland	GMT + 10, No Daylight Savings Time
australia-north	GMT + 9.5, No Daylight Savings Time
australia-west	GMT + 8, No Daylight Savings Time
australia-south	GMT + 9.5, Subject to Southern Australian Daylight Savings Time Rules
new-zealand	GMT + 12, Subject to New Zealand Daylight Savings Time Rules
israel	GMT + 3, Subject to Israeli Daylight Savings Time Rules

Table F-1. Time Zone Names (3 of 3)

Time Zone Name	Description
turkey	GMT + 3, Subject to Turkish Daylight Savings Time Rules
egypt	GMT + 2, Subject to Egyptian Daylight Savings Time Rules
iran	GMT + 3.5, Subject to Iranian Daylight Savings Time Rules
libya	GMT + 2, Subject to Libyan Daylight Savings Time Rules
japan	GMT + 9, No Daylight Savings Time
korea	GMT + 9, Subject to Korean Daylight Savings Time Rules
singapore	GMT + 8, No Daylight Savings Time
china-prc	GMT + 8, Subject to Chinese Daylight Savings Time Rules
china-roc	GMT + 8, No Daylight Savings Time
china-hongkong	GMT + 8, No Daylight Savings Time

Ethertypes

The following values are used by the **configure filter-rule** command. See *Configure Filter-Rule* in Appendix A, *CLI Command Descriptions*.

Table F-2. Ethertypes (1 of 6)

Ether Type	Description
0000-05DC	IEEE 802.3 Length Field
0101-01FF	Experimental
0200	XEROX PUP (see 0A00)
0201	PUP Addr Trans (see 0A01)
0400	Nixdorf
0600	XEROX NS IDP
0660	DLOG
0661	DLOG
0800	Internet IP (IPv4)
0801	X.75 Internet
0802	NBS Internet
0803	ECMA Internet
0804	Chaosnet
0805	X.25 Level 3
0806	ARP
0807	XNS Compatibility
081C	Symbolics Private
0888-088A	Xyplex
0900	Ungermann-Bass net debugr
0A00	Xerox IEEE802.3 PUP
0A01	PUP Addr Trans
0BAD	Banyan Systems
1000	Berkeley Trailer nego
1001-100F	Berkeley Trailer encap/IP
1600	Valid Systems
4242	PCS Basic Block Protocol
5208	BBN Simnet
6000	DEC Unassigned (Exp.)

Table F-2. Ethertypes (2 of 6)

Ether Type	Description
6001	DEC MOP Dump/Load
6002	DEC MOP Remote Console
6003	DEC DECNET Phase IV Route
6004	DEC LAT
6005	DEC Diagnostic Protocol
6006	DEC Customer Protocol
6007	DEC LAVC, SCA
6008-6009	DEC Unassigned
6010-6014	3Com Corporation
7000	Ungermann-Bass download
7002	Ungermann-Bass dia/loop
7020-7029	LRT
7030	Proteon
7034	Cabletron
8003	Cronus VLN
8004	Cronus Direct
8005	HP Probe
8006	Nestar
8008	AT&T
8010	Excelan
8013	SGI diagnostics
8014	SGI network games
8015	SGI reserved
8016	SGI bounce server
8019	Apollo Computers
802E	Tymshare
802F	Tigan, Inc.
8035	Reverse ARP
8036	Aeonic Systems
8038	DEC LANBridge
8039-803C	DEC Unassigned
803D	DEC Ethernet Encryption

Table F-2. Ethertypes (3 of 6)

Ether Type	Description
803E	DEC Unassigned
803F	DEC LAN Traffic Monitor
8040-8042	DEC Unassigned
8044	Planning Research Corp.
8046	AT&T
8047	AT&T
8049	ExperData
805B	Stanford V Kernel exp.
805C	Stanford V Kernel prod.
805D	Evans & Sutherland
8060	Little Machines
8062	Counterpoint Computers
8065	Univ. of Mass. @ Amherst
8066	Univ. of Mass. @ Amherst
8067	Veeco Integrated Auto.
8068	General Dynamics
8069	AT&T
806A	Autophon
806C	ComDesign
806D	Computgraphic Corp.
806E-8077	Landmark Graphics Corp.
807A	Matra
807B	Dansk Data Elektronik
807C	Merit Internodal
807D-807F	Vitalink Communications
8080	Vitalink TransLAN III
8081-8083	Counterpoint Computers
809B	Appletalk
809C-809E	Datability
809F	Spider Systems Ltd.
80A3	Nixdorf Computers
80A4-80B3	Siemens Gammasonics Inc.

Table F-2. Ethertypes (4 of 6)

Ether Type	Description
80C0-80C3	DCA Data Exchange Cluster
80C4	Banyan Systems
80C5	Banyan Systems
80C6	Pacer Software
80C7	Applitek Corporation
80C8-80CC	Intergraph Corporation
80CD-80CE	Harris Corporation
80CF-80D2	Taylor Instrument
80D3-80D4	Rosemount Corporation
80D5	IBM SNA Service on Ether
80DD	Varian Associates
80DE-80DF	Integrated Solutions TRFS
80E0-80E3	Allen-Bradley
80E4-80F0	Datability
80F2	Retix
80F3	AppleTalk AARP (Kinetics)
80F4-80F5	Kinetics
80F7	Apollo Computer
80FF-8103	Wellfleet Communications
8107-8109	Symbolics Private
8130	Hayes Microcomputers
8131	VG Laboratory Systems
8132-8136	Bridge Communications
8137-8138	Novell, Inc.
8139-813D	KTI
8148	Logicraft
8149	Network Computing Devices
814A	Alpha Micro
814C	SNMP
814D	BIIN
814E	BIIN
814F	Technically Elite Concept

Table F-2. Ethertypes (5 of 6)

Ether Type	Description
8150	Rational Corp
8151-8153	Qualcomm
815C-815E	Computer Protocol Pty Ltd
8164-8166	Charles River Data System
817D-818C	Protocol Engines
818D	Motorola Computer
819A-81A3	Qualcomm
81A4	ARAI Bunkichi
81A5-81AE	RAD Network Devices
81B7-81B9	Xyplex
81CC-81D5	Apricot Computers
81D6-81DD	Artisoft
81E6-81EF	Polygon
81F0-81F2	Comsat Labs
81F3-81F5	SAIC
81F6-81F8	VG Analytical
8203-8205	Quantum Software
8221-8222	Ascom Banking Systems
823E-8240	Advanced Encryption Syste
827F-8282	Athena Programming
8263-826A	Charles River Data System
829A-829B	Inst Ind Info Tech
829C-82AB	Taurus Controls
82AC-8693	Walker Richer & Quinn
8694-869D	Idea Courier
869E-86A1	Computer Network Tech
86A3-86AC	Gateway Communications
86DB	SECTRA
86DE	Delta Controls
86DF	ATOMIC
86E0-86EF	Landis & Gyr Powers
8700-8710	Motorola

Table F-2. Ethertypes (6 of 6)

Ether Type	Description
8A96-8A97	Invisible Software
9000	Loopback
9001	3Com(Bridge) XNS Sys Mgmt
9002	3Com(Bridge) TCP-IP Sys
9003	3Com(Bridge) loop detect
FF00	BBN VITAL-LanBridge cache
FF00-FF0F	ISC Bunker Ramo

Index

D

E

F

G

H

I

K

L

M

N

P

Q

R

S

T

U

V

W