DIGITAL GIGAswitch GS2000 Line Card

Management

Part Number: AA-R8RDA-TE

November 1997

This manual describes how to configure, monitor, and manage the DIGITAL GIGAswitch GS2000 line card.

Revision/Update Information:	This is a new manual.
Software and Version:	GIGAswitch GS2000 Version 2.0

Digital Equipment Corporation makes no representations that the use of its products in the manner described in this publication will not infringe on existing or future patent rights, nor do the descriptions contained in this publication imply the granting of licenses to make, use, or sell equipment or software in accordance with the description.

Possession, use, or copying of the software described in this publication is authorized only pursuant to a valid written license from DIGITAL or an authorized sublicensor.

© Digital Equipment Corporation 1997. All rights reserved. Printed in U.S.A.

The following are trademarks of Digital Equipment Corporation:

clearVISN, DEC, DECconnect, DEChub, DECnet, DECrepeater, DIGITAL, GIGAswitch, LAT, OpenVMS, PORTswitch, ThinWire, ULTRIX, and the DIGITAL logo.

The following are third-party trademarks:

Apollo is a registered trademark of Apollo Computer Inc., a subsidiary of Hewlett-Packard Company.

Apple and AppleTalk are registered trademarks of Apple Computer, Inc.

NetBIOS is a trademark of Micro Computer Systems, Inc.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Ltd.

All other trademarks and registered trademarks are the property of their respective holders.

Contents

Preface

1 Introduction

2 Operational Basics

3 Adding and Managing Users

4 Configuring and Monitoring Module-wide Parameters

5 Configuring Network Interfaces

6 Monitoring Network Interfaces

7 Configuring the Transparent Bridge

8 Monitoring the Transparent Bridge

9 Configuring Virtual LANs

10 Performing Routine Maintenance

11 Event Logging and Reporting

12 Configuring Remote Management

13 Monitoring Network Activity

A Advanced Console Management

B Plug and Play Default Settings

C Counters

Index

Figures

Tables

Preface

Overview

Purpose of This Manual

This manual provides instructions for configuring, monitoring, and managing the DIGITAL GIGAswitch GS2000 line card.

Intended Audience

This manual is intended for persons who install, configure, and manage computer networks. Although experience with computer networking hardware and software is helpful, you do not need programming experience to configure, monitor, and manage the GIGAswitch GS2000 line card.

Organization

This manual is organized as follows:

Section	Description
Chapter 1	Provides general information about the GIGAswitch GS2000 line card and an overview of what your responsibilities are as a switch administrator. This chapter also provides an introduction to concepts and terminology with which you should be familiar.
Chapter 2	Describes operational basics that are common to many of the configuration and management tasks described throughout the book.
Chapter 3	Provides instructions about assigning login permission and security levels to users who are to manage this line card.
Chapter 4	Provides information about how to manage and monitor functions that affect switchwide operation.
Chapter 5	Provides instructions about how to reconfigure FDDI and ATM interface default settings to maximize network performance, and to accommodate requirements unique to your network environment.
Chapter 6	Provides information about how to monitor FDDI and ATM network interfaces.
Chapter 7	Provides information about how to configure the transparent bridge and how to display information about the current configuration.
Chapter 8	Provides information about how to monitor the transparent bridge and how to configure static addresses. Monitoring includes the ability to display specific information about operational states, activity counters, and various bridge configuration settings.
Chapter 9	Describes how to create, modify, and delete Virtual LANs (VLANs).

Section	Description
Chapter 10	Describes maintenance procedures you may need to perform periodically, and those that you may need to perform regularly.
Chapter 11	Provides information about how to configure an event log to record specific types of operational events and errors and to eliminate others, depending on the level of detail you require.
Chapter 12	Describes how to configure the line card so you can manage the module from a remote device.
Chapter 13	Explains how to configure the mirror port and RMON agent so that you can monitor network activity.
Appendix A	Discusses local and remote console session management tasks that may be of interest to advanced users.
Appendix B	Lists the factory default settings that are used when the switch is first installed. You may need to alter default settings to maximize network performance, to enable special functions such as Virtual Local Area Networks (VLANs), and to set IP addresses for remote management.
Appendix C	Describes module counters and their relationships.

Associated Documents

The following documents provide information relating to the module. To order any of the following documents, refer to the directions in *How to Order Additional Documentation*.

Title and Order Number	Description
DIGITAL GIGAswitch GS2000 Line Card Installation EK-DEFGC-IN	Describes the GIGAswitch GS2000 line card, including features and installation information.
DIGITAL GIGAswitch GS2000 Line Card Router Management AA-R8RE*-TE	Provides instructions for configuring, managing, and monitoring a GIGAswitch GS2000 router.
GIGAswitch/ATM System Installation and Service AA-QCV7*-TE	Describes how to install and service the GIGAswitch/ATM system.
GIGAswitch/ATM 5-Slot System Installation and Service EK-DAGWG-IN	Describes how to install and service the GIGAswitch/ATM 5-slot system.
GIGAswitch/FDDI System Installation and Service Guide EK-GGSVA-IN	Describes how to install and service the GIGAswitch/FDDI system.
DIGITAL ATM Modular PHY Cards Installation EK-DAGGM-IN	Provides installation and operating guidelines for installing, verifying, and removing ATM modular PHY cards. Describes cabling and LED information.
clearVISN Installation	Provides pre- and post-installation information, as well as actual installation procedures for each application .
clearVISN Overview	Provides an overview of clearVISN, an explanation of each application, and descriptions of all concepts necessary to understand and use the application efficiently.
clearVISN User's Guide	Provides information for starting each application, configuring them, and general use information.

Title and Order Number	Description
OPEN DECconnect Applications Guide EC-G6387-42	Provides information to help plan and install networking systems based on DIGITAL OPEN DECconnect System and networking products.
Event Logging System Messages Guide	Describes messages logged by the Event Logging System.
Bridge and Extended LAN Reference	Describes how bridges are used to create extended local area networks (LANs). The descriptions include the use of bridges in extended LAN configurations, information on LAN interconnections, overall bridge operation, spanning tree, bridge management, and solving bridge-related problems in a network.

Conventions

This manual uses the following conventions:

Convention	Description
`Special Type`	This special type in examples indicates system output.
Boldface	Boldface type indicates user input.
Boldface Italics	Boldface type in italics indicates variables for which the user or the system supplies a value.
Boldface **u**nderscore	Underscored boldface characters indicate the least number of characters you must enter to identify a command. The underscored characters are referred to as command shortcuts. For example, the commands for listing users is **li**st **u**sers, and can be entered as **l u**. Similarly, the command for viewing error statistics is **er**ror and can be entered as **er**.
Return	Indicates that you should press the Return key.
Ctrl/*keystroke*	Indicates you should press the key specified by *keystroke* while holding down the Control key. For example, Ctrl/P indicates you should press the P key while holding down the Control key.

Correspondence

Documentation Comments

If you have comments or suggestions about this document, send them to the Network Products Business Organization.

Attn.: Documentation Project Manager

E-MAIL: doc_quality@lkg.mts.dec.com

Online Services

To locate product-specific information, refer to the DIGITAL Network Products Home Page on the World Wide Web. The web page is located at the following addresses:

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

How to Order Additional Documentation

To order additional documentation, use the following information:

To Order:	Contact:
By Telephone	USA (except Alaska, New Hampshire, and Hawaii): 1-800-DIGITAL (1-800-344-4825) Alaska, New Hampshire, and Hawaii: 1-603-884-6660 Canada: 1-800-267-6215
Electronically (USA only)	Dial 1-800-DEC-DEMO (For assistance, call 1-800-DIGITAL)
By Mail (USA and Puerto Rico)	DIGITAL EQUIPMENT CORPORATION P.O. Box CS2008 Nashua, New Hampshire 03061 (Place prepaid orders from Puerto Rico with the local DIGITAL subsidiary: 809-754-7575)
By Mail (Canada)	DIGITAL EQUIPMENT of CANADA LTD. 940 Belfast Road Ottawa, Ontario, Canada K1G 4C2 Attn.: A&SG Business Manager
Internationally	DIGITAL EQUIPMENT CORPORATION Attn.: A&SG Business Manager c/o local DIGITAL subsidiary or approved distributor
Internally	U.S. Software Supply Business (SSB) DIGITAL EQUIPMENT CORPORATION 8 Cotton Road Nashua, New Hampshire 03063

Chapter 1

Introduction

Overview

Introduction

This chapter gives an overview of your responsibilities as a switch administrator. This chapter also provides an introduction to concepts and terminology with which you should be familiar.

In This Chapter

The following topics are covered in this chapter:

Concepts and Terminology

This section presents basic module concepts and terminology with which you should become familiar. Refer to the *DIGITAL VNswitch 900 Series Technical Overview* for a more detailed discussion about specific concepts and terms.

Bridge Plug and Play

The GIGAswitch GS2000 line card features plug-and-play operation. Once installed, a module begins handling network traffic and running transparent bridging on each port, by default. You may need to alter default settings to maximize network performance, to enable special functions such as Virtual Local Area Networks (VLANs), and to set IP addresses for remote management.

The default settings used at installation are listed in Appendix B. The default setting for each configurable parameter is also given when that parameter is discussed in the following chapters.

Switch Console Sessions

You can configure, monitor, and manage a GIGAswitch GS2000 line card by establishing either a local or remote console session with the module or by using the clearVISN network management product from Digital Equipment Corporation.

Local Sessions

A local session is established by connecting a terminal (or a workstation or PC running terminal emulation, for example) directly to the console port of the GIGAswitch GS2000 module.

Remote Sessions

A remote session is established by running Telnet on a remote system and connecting to the module's IP address (if routing is enabled) or the module's IP Host Services IP address (if routing is not enabled). The Telnet client program can be run on a workstation, a PC, or a terminal server, for example. A maximum of two remote sessions can be established with a switch at the same time.

Transparent Bridging

GIGAswitch GS2000 line cards support transparent bridging. Transparent bridging is the ability of the module to automatically "learn" the network addresses and locations of other network devices. The module organizes the addresses in bridge tables in such a way that it is able to determine on which module port the device is located. Transparent bridges are also referred to as *learning* or *adaptive bridges*.

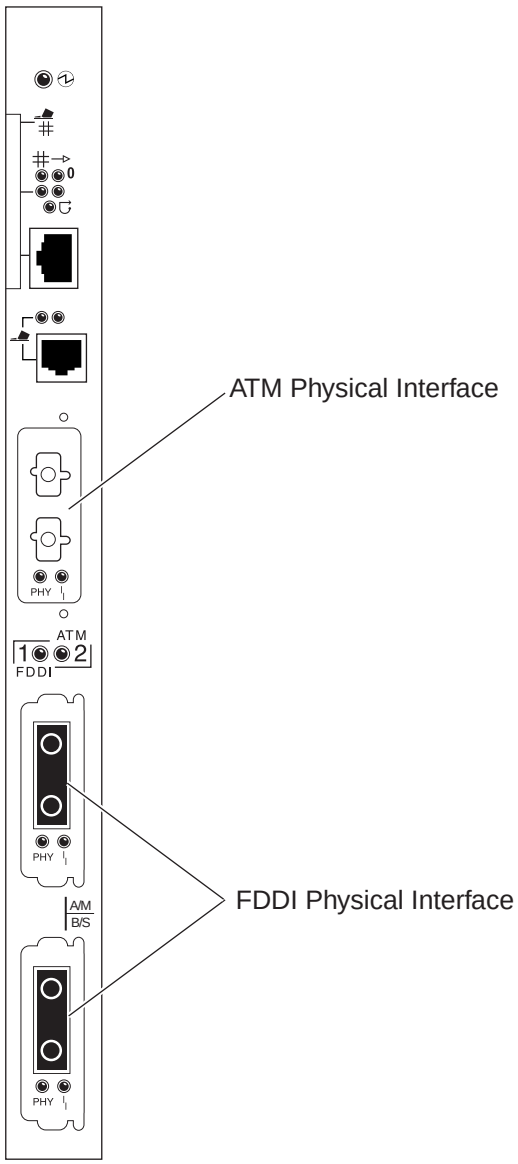
Understanding Network Interfaces and Ports

The module's architectural design applies different definitions to the terms *interface* and *port*. The design further distinguishes among two types of interface: physical and logical.

Physical Interface

A physical interface is the physical point on the module to which a network transmission medium (cable or fiber, for example) is connected. The GIGAswitch GS2000 module has two physical interfaces, one ATM interface and one FDDI interface. Figure 1-1 shows the physical interfaces on the front panel of a GIGAswitch GS2000 line card.

Figure 1-1: Physical Interfaces



LKG-10696-97WI

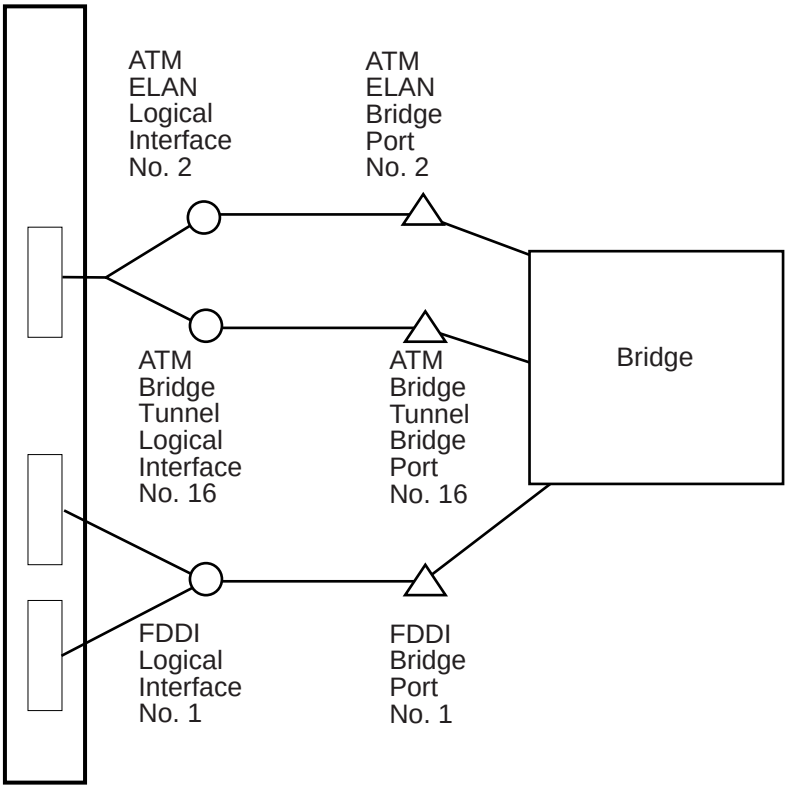
Logical Interface

A logical interface is an abstract connection point, within the system's software, between a physical interface and a bridge port. The FDDI physical interface is associated with one logical interface. The ATM physical interface is associated with 1 to 16 logical interfaces, each of which is the connection point to either an ATM emulated LAN (ELAN), or an ATM bridge tunnel. Each logical interface on a switch is identified by a unique number. Figure 1-2 shows examples of logical interfaces on a GIGAswitch GS2000 line card.

Bridge Port

A bridge port is an abstract connection point, within the system's software, to a transparent bridge. The transparent bridge forwards data to, or receives data from, bridge ports, based on the MAC address associated with the data. Each bridge port on a switch is identified by a unique number. Figure 1-2 shows a GIGAswitch GS2000 line card that includes one port from the FDDI interface, one port from an ELAN interface, and one port from an ATM bridge tunnel interface.

Figure 1-2: Logical Interfaces and Bridge Ports



VLANs and VLAN Secure Domains

A VLAN is a group of bridge ports logically linked to define a LAN.

A VLAN Secure Domain (VSD) is a logical set of one or more VLANs that operate with one spanning tree. A VLAN consists of a set of distinct bridge ports. Each set of bridge ports is isolated from other ports on the same switch by blocking all unicast and multicast traffic between VSDs. GIGAswitch GS2000 line cards presently support one VLAN per VSD, but the VSD concept provides for expanded support of multiple VLANs within a single VSD.

In most respects, each VSD operates as a separate logical bridge within the module. For example, a separate instance of the spanning tree protocol is run on each VSD.

Note

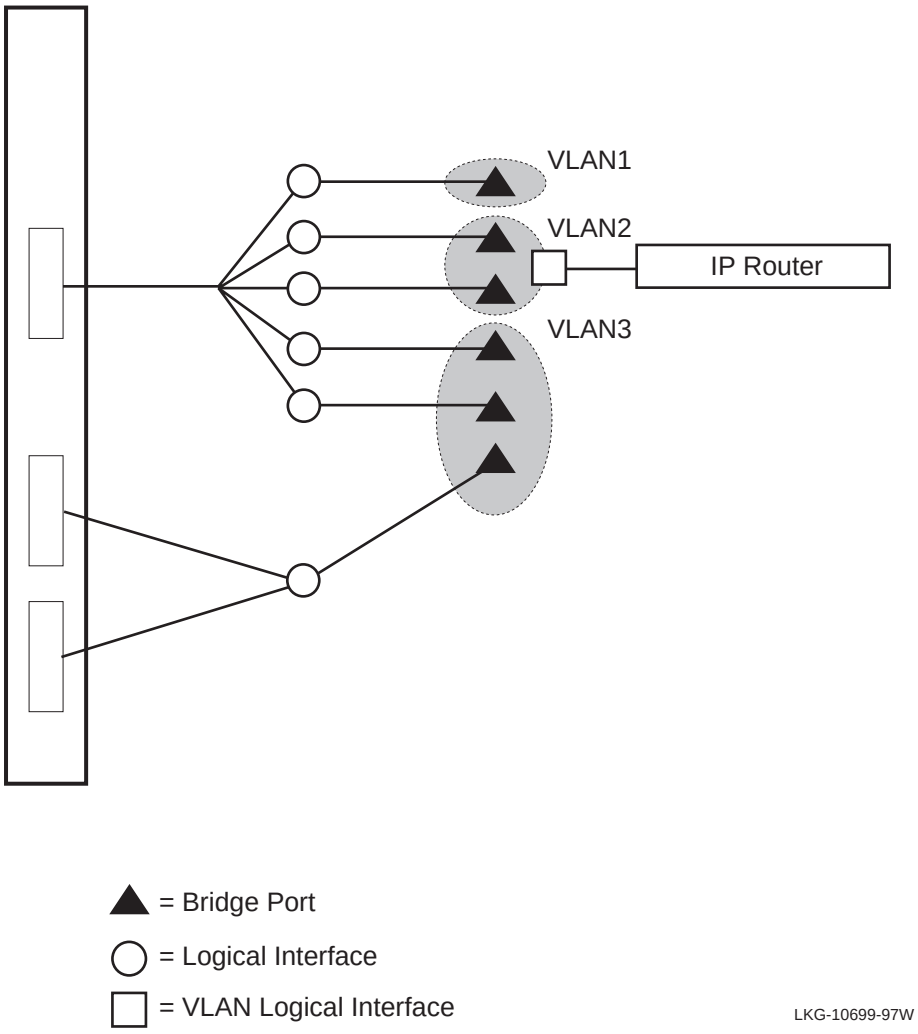
A VLAN is currently equivalent to a VSD because the present implementation supports one VLAN per VSD.

Refer to Chapter 9 for more information about VLANs and VSDs.

VLAN Logical Interface

A VLAN logical interface is an abstract connection between a VLAN and a router, enabling you to connect multiple VLANs through the router. Figure 1-3 shows examples of VLAN logical interfaces on a GIGAswitch GS2000 line card.

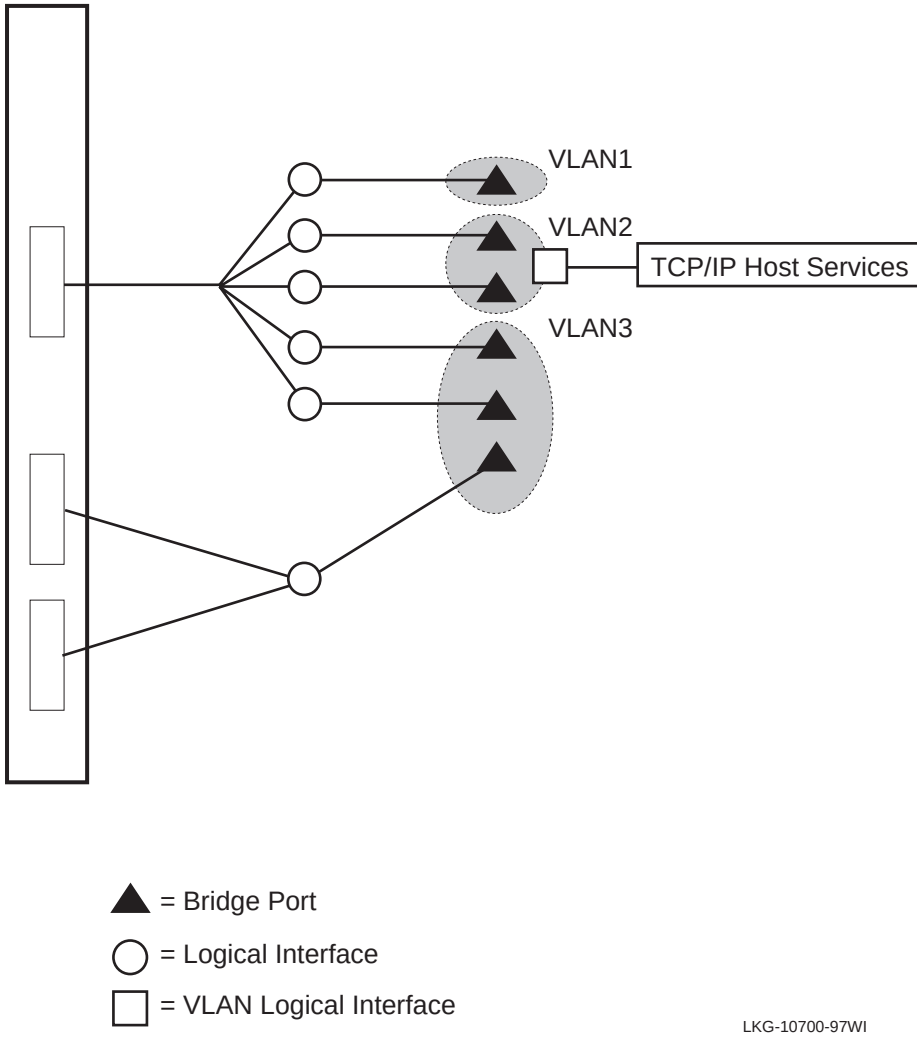
Figure 1-3: VLAN Logical Interfaces



TCP/IP Host Services Logical Interface

A TCP/IP Host Services logical interface is an abstract connection between a VLAN and TCP/IP Host Services. Figure 1-4 shows examples of VLAN logical interfaces on a GIGAswitch GS2000 line card.

Figure 1-4: TCP/IP Host Services Logical Interface



User Interface

You can configure, monitor, and manage GIGAswitch GS2000 line cards using a command line interface (CLI). You can access the CLI through either a local or remote console session.

Note

You can also configure, monitor, and manage GIGAswitch GS2000 line cards through a graphical interface if you install a MIB-based management system such as MultiChassis Manager (optional), a component of the clearVISN network management product from Digital Equipment Corporation. Refer to the documentation accompanying your MIB-based management system for additional information.

The remaining chapters in this manual describe what commands you enter at the CLI to perform specific tasks. The initial steps for most of those tasks involve accessing a CLI prompt.

The GIGAswitch GS2000 line card CLI consists of three components:

- Main Operator's console
- Configuration
- Monitor

To perform a specific task, you access the prompt associated with the task you want to perform. The following describes the GIGAswitch GS2000 components:

Component	Prompt	Description
Main Operator's console	Main>	This component performs certain backup, upgrade, and restoration tasks; manages console sessions; restarts the module; displays nonconfigurable information about the module. You access all lower level prompts from the Main prompt.

Component	Prompt	Description
Configuration	Config>	This component configures parameters that apply to the entire module, rather than to a specific interface or port. These parameters include, for example, adding users who can manage the module, and enabling or disabling prompting for ID and password. You use the Config prompt to access lower level prompts that enable you to configure the module's interfaces, protocols, ports, and parameters pertaining to boot and dump configuration, event logging, error logging, VLANs, remote monitoring, and the mirror port.
Monitor	Monitor>	This component monitors parameters that apply to the entire module, rather than to a specific interface or port. These include, for example, displaying a list of users who can manage the module, and determining whether prompting for ID and password is enabled. You use the Monitor prompt to access lower level prompts that enable you to monitor parameters associated with module interfaces, protocols, and ports.

Instructions about how to access prompts are presented in Chapter 2. Instructions about how to access lower level prompts within each component are presented in the relevant chapters in this manual. Refer to Chapter 11 for information about how to display the event log.

Auto-Prompts

The CLI enables you to perform certain tasks either by entering commands and parameter variables as a string, or by responding to instructional prompts that walk you through each item you must enter. Instructions about how to use auto-prompts are presented in Chapter 2.

Types of Module Memory

GIGAswitch GS2000 line cards store data in the following two types of random access memory (RAM):

Type of RAM	Description
Volatile RAM	Volatile RAM is used to store parameters you enter from the Monitor prompt. It is also used to store various buffers, and information such as network addresses learned by the module, and static address entries entered by you or another network manager. (Refer to the Address Types section for information about the types of addresses stored in Volatile RAM.) Information stored in volatile RAM is lost when the module is powered down or restarted.
Nonvolatile RAM (NVRAM)	NVRAM is used to store parameters you configure from the Config prompt. It is also used to store the module's executable software (also known as the boot or image file). User-configured parameters may include network addresses, referred to as permanent address entries. (Refer to the Address Types section for information about the types of addresses stored in NVRAM.) The configuration database and image remain intact when the module is powered down or power is lost. Refer to Chapter 10 for information about backup and restore.

Configuration Commands Requiring Restart

Some of the commands you use to specify or change configuration settings on the module require that you restart the module for the changes to take effect. The procedures described in this manual indicate when a restart is required. If the procedure does not indicate a restart is required, the configuration parameter you specify takes affect immediately. This is sometimes referred to as dynamic configuration.

All parameters configured from the Config prompt survive restarts and loss of power. The configuration parameters you specify from the Monitor prompt, or lower level prompts under the Monitor prompt, are dynamic. These settings are stored in volatile memory and, therefore, are lost when there is a power outage or the module is restarted.

Address Types

The MAC address of network devices can be added to bridge tables automatically through bridge learning, manually by you or another network manager, or by one or more network devices. Table 1-1 describes the different address types and where they are stored.

Table 1-1: MAC Address Type Descriptions

Address Type	Description
Dynamic address	A MAC address automatically learned by the module. Dynamic address entries are stored in volatile RAM and, therefore, do not survive power cycles or system resets. Dynamic entries are affected by address aging.
Permanent address	A MAC address entered manually by a network manager from the Config prompt. Permanent address entries survive power cycles or system resets. Permanent entries are not affected by address aging.
Static address	A MAC address entered manually by a network manager from the Monitor prompt. Static address entries do not survive power cycles or system resets. Static entries are not affected by address aging.
Reserved address	A MAC address reserved by the IEEE 802.1d standard.
Registered address	A unicast MAC address that belongs to communications hardware attached to the module, or a multicast address enabled by protocol forwarders.
Unknown address	A MAC address that does not fall into any of the other address type categories listed in this table.

System Security

The module software can, optionally, require users to enter a user name and password when logging in at a module console. (Refer to Chapter 3 for information about how to enable and disable ID and password prompts.) It further distinguishes between the following three types of users, each of which is associated with a different level of access privilege to configuration, monitoring, and management functions:

Administrative users — Can access any configuration, monitoring, or management function, including adding and managing users. Only a user with Administrative access can change configuration in NVRAM.

Operations users — Can view any network configuration parameter or statistic, run potentially disruptive tests, dynamically change module operation by reconfiguring parameters via volatile RAM, and restart the module.

Monitor users — Can only view configuration parameters and network statistics.

Overview of Your Responsibilities

The manager of a GIGAswitch GS2000 line card is responsible for the following general activities:

Preinstallation planning — As a GIGAswitch GS2000 line card user, you should be involved in network design or expansion planning. If you are not closely involved in such planning activities, you should receive detailed site preparation instructions as well as instructions about how the various network devices are to be configured. Refer to the *DIGITAL VNswitch 900 Series Technical Overview* for background information about switching and bridging concepts, and examples of network configurations that are based on those concepts. The information in the Technical Overview may be helpful during network design and planning. If you plan to use the routing option, refer to the *DIGITAL GIGAswitch GS2000 Line Card Router Management* manual.

Installing GIGAswitch GS2000 modules — Hardware installation documentation is shipped with each GIGAswitch GS2000 line card. Refer to the appropriate installation document for instructions about how to install each module and run diagnostics. The installation documentation also includes information about hardware requirements such as supported cabling and connectors.

Connecting the switch console — The local console must be connected to the GIGAswitch GS2000 line card after the module is installed. Refer to the GIGAswitch GS2000 installation document for instructions about connecting consoles.

Adding and managing users — You can allow other users to access certain configuration, monitoring, and management functions by adding them to a user list. You can restrict the types of activities the user can perform by assigning them to one of three categories of user. You can also change user passwords, disable the ability to log in from a remote console, and delete users. Refer to Chapter 3 for instructions about adding and managing users.

Configuring a switch — GIGAswitch GS2000 line cards feature bridge plug-and-play configuration. Once installed, a module automatically configures itself with default settings, and begins switching and bridging traffic over the network.

You may typically need to alter default settings to maximize network performance, to enable special functions such as Virtual Local Area Networks (VLANs), and to configure remote management. Refer to Chapter 4, Chapter 5, Chapter 7, Chapter 9, Chapter 12, and Chapter 13 for instructions about the following topics, respectively:

- Configuring module-wide parameters
- Configuring interfaces and the Address Resolution Protocol (ARP)
- Configuring transparent bridging

- Configuring Virtual LANs
- Configuring remote management, the Simple Network Management Protocol (SNMP), and TCP/IP Host Services
- Configuring the RMON agent

Monitoring and managing a switch — You are responsible for ongoing monitoring and maintenance of GIGAswitch GS2000 line cards once they are operational. This responsibility includes such activities as monitoring traffic collision statistics and error counters, and backing up switch configurations. Refer to Chapter 4, Chapter 6, Chapter 8, Chapter 10, Chapter 12, and Chapter 13 for instructions about the following topics, respectively:

- Monitoring module-wide parameters
- Monitoring interfaces and the Address Resolution Protocol (ARP)
- Monitoring and managing bridging
- Performing routine maintenance procedures such as backup and restoration, detecting crashes that may have occurred (followed by automatic recovery), and upgrading module software
- Monitoring remote management, the SNMP, and TCP/IP Host Services
- Monitoring the RMON agent

Chapter 2

Operational Basics

Overview

Introduction

This chapter describes the basic procedures for working with a DIGITAL GIGAswitch GS2000 line card. They are the operational basics that are common to many of the configuration and management tasks described in the following chapters.

In This Chapter

The following topics are covered in this chapter:

These topics are common to most of the procedures described throughout this manual and are frequently referenced by those procedures. For example, you must start a console session and access a CLI prompt before you begin to configure a network interface. Similarly, once logged in, you may want to display Help information about command options you can use.

Starting and Terminating Console Sessions

You can configure, monitor, and manage a GIGAswitch GS2000 line card by establishing either a local or remote console session with a module.

Local sessions are used to configure and manage only the modules to which the terminal is attached. A local session is established by connecting a terminal directly to the console port of a GIGAswitch GS2000 module.

Remote sessions are used to configure and manage any module on the network. Remote sessions are established by running Telnet on a remote system and connecting through any GIGAswitch GS2000 module network interface (FDDI, ATM ELAN, or ATM Bridge Tunnel)

The console port provides out-of-band management. Access through a network interface provides in-band management. In-band management cannot be used when the network is down, and can use up a portion of the network's bandwidth. Out-of-band management remains operational when the network is down and does not affect bandwidth. In-band management traffic is subject to bridge and VLAN filters. Out-of-band management is not subject to bridge and VLAN filters. Refer to Chapter 9 for additional information about VLANs.

The following instructions about starting and terminating sessions assume your terminal is already physically connected to the GIGAswitch GS2000 modules. Refer to the GIGAswitch system installation and configuration documentation for information about installing devices to connect to a GIGAswitch system. Refer to Chapter 12 of this document for information about how to configure the GIGAswitch GS2000 line card for Telnet and OBM connections.

Starting and Terminating Local Sessions

To start a local console session through a console port, perform the following steps:

Step	Action
1	Turn on the power to your terminal. A menu similar to the one shown in Figure 2-1 is displayed.
2	Enter **6** (Go to Local Console) and press Return. A Local Console session is established and the Main prompt (`Main>`) is displayed. **Note:** If ID and password prompting is enabled by the switch administrator, you are prompted for your ID and password before the Main prompt is displayed.

To terminate a console session, enter **logout** at the Main prompt (`Main>`) and press Return. The installation menu shown in Figure 2-1 is displayed.

Figure 2-1: GIGAswitch GS2000 Module Installation Menu

```
GIGAswitch GS2000
=======================================================
               GIGAswitch GS2000 INSTALLATION MENU


           [1] Restart with Factory Defaults
           [2] Restart with Current Settings
           [3] Show Current Settings
           [4] Configure IP ...
           [5] Configure Out-of-Band Port ...
           [6] Go to Local Console
           [7] Product-Specific Options ...
=======================================================

              Enter selection:
```

Starting and Terminating Remote Sessions

Remote console sessions can be established only after configuring the appropriate network connections. Refer to Chapter 12 for information about how to do so. A maximum of two remote sessions can be established with a GIGAswitch GS2000 module at the same time.

To start a session from a remote device (workstation, PC, or terminal server, for example) to the module through a console port or a module's network interface, perform the following steps:

Step	Action
1	Access the operating system prompt from your terminal.
2	Enter **telnet** ***ip-address***, where ***ip-address*** is the IP address of the module you want to access, if attempting to do so through a module's network interface (FDDI or ATM) or the module's console port. Refer to Chapter 12 for information about how to determine the module's IP address.
3	Press Return. The Main prompt (`Main>`) of the remote GIGAswitch GS2000 module is displayed. **Note:** If ID and password prompting is enabled by the switch administrator, you are prompted for your ID and password before the Main prompt is displayed.

To terminate a console session, enter **logout** at the Main prompt (`Main>`) and press Return. The operating system prompt is displayed.

Obtaining an IP Address Automatically

If you have a BootP or DHCP server running on your network and your module is not assigned an IP address, the module takes advantage of BootP client software to automatically obtain an IP address for itself during power-up or restart. Refer to the vendor's BootP or DHCP documentation for configuration information.

A GIGAswitch GS2000 line card (as a BootP client) that does not have an IP address assigned, sends out a BootP (broadcast) request to a BootP or DHCP server. When the server replies with an IP address, the module configures the IP address for HST dynamically. This IP address is stored permanently, so power-cycling the module does not have any impact on the IP address. To change the IP address, you use the configuration menu.

An IP address is required for the GIGAswitch GS2000 line card if you plan to manage it using an SNMP tool such as clearVISN.

Accessing CLI Prompts

The initial steps for most of the tasks discussed throughout this manual involve accessing the CLI prompts (Main, Config, and Monitor). Instructions about how to access the prompts are presented here, rather than repeating them for each task covered later in this manual.

Only one user at a time can access these prompts or the error log. If another user attempts to access the same prompt you are currently using, the message `Current Process has been Redirected` is displayed and you are returned to the Main prompt (`Main>`). If, for example, you access the Monitor prompt from the Main prompt and another user then accesses the Monitor prompt, the message `Current Process has been Redirected` is displayed and you are returned to the Main prompt. The user who accessed the prompt you were using receives all redirected output from those tasks you initiated, but that did not yet display on your screen. Any task you initiated is completed unless the user to whom the output is redirected cancels it.

Accessing the Main Prompt

The Main prompt (`Main>`) is automatically displayed each time you start a console session. (Refer to the Starting and Terminating Console Sessions section.)

Accessing the Config Prompt

To access the Config prompt, perform the following steps:

Step	Action
1	At the Main prompt (`Main>`), enter **Config**.
2	Press Return. The Config prompt (`Config>`) is displayed.
3	If the prompt is not displayed, press Return a second time.

Accessing the Monitor Prompt

To access the Monitor prompt, perform the following steps:

Step	Action
1	At the Main prompt (`Main>`), enter **Monitor**.
2	Press Return. The Monitor prompt (`Monitor>`) is displayed.
3	If the prompt is not displayed, press Return a second time.

Adding the Hostname to a Prompt

You can prefix prompts with the module's hostname. For example, if the hostname is defined as cmtsrv.lkg.dec.com, the new prompt might look like this:

cmtsrv Monitor>

To enable the hostname prefix, enter **enable prompting-with-hostname** at the Config> prompt. To disable the hostname prefix, enter **disable prompting-with-hostname** at the Config> prompt.

Editing Entries on the Command Line

Use the Backspace key to delete the last character typed on the command line. Use Ctrl/U to delete all the characters entered on the command line, allowing you to reenter a command.

You can also use the command line recall feature on a video terminal (VT) or VT emulator, if the bit setting used to define characters is set to 7. Command line recall enables you to use the up and down arrows on your keyboard to redisplay commands previously entered. The up arrow displays successively earlier command line entries. The down arrow displays more recent entries.

Exiting a Prompt

The Config prompt (`Config>`) and the Monitor prompt (`Monitor>`) are accessed from the Main prompt (`Main>`). Tasks you may want to perform using these prompts typically require that you access lower level prompts before you can enter the appropriate commands.

To exit any lower level prompt and return to the next higher level prompt, enter **exit** and press Return. To return to the Config or Monitor prompt from any lower level prompt, enter **exit** and press Return repeatedly until the Config or Monitor prompt is displayed.

To return to the Main prompt from any lower level prompt, press Ctrl/P (the default intercept character). If you use Ctrl/P to skip two or more lower-level prompts and jump to the Main prompt directly, the next time you access either the Config or Monitor prompt, you are returned directly to that lower level prompt from which you previously exited. This can be convenient if you are performing a task at some lower level prompt under `Config>`, for example, and to move back and forth from that prompt level to the Monitor prompt.

The Ctrl/P key combination is called the intercept character. You can change the intercept character, if necessary. (Refer to the Changing the Intercept Character section for instructions.)

Changing the Intercept Character

The intercept character is used to return to the Main prompt from another prompt. The default intercept character is Ctrl/P. To change the intercept character, perform the following steps:

Step	Action
1	At the Main prompt, enter **intercept**.
2	Press Return. The following message is displayed: `Control character to use as intercept character:`
3	Enter the desired character (**x**, for example). The following message is displayed: `Intercept character is now control-X`

Entering Commands and Command Shortcuts

You perform tasks by entering commands at a CLI prompt. For example, if you want to view a list of all users, you must access the Config prompt (`Config>`) and enter **list users**. Similarly, if you want to view error statistics for the network, you access the Monitor prompt (`Monitor>`) and enter **error**.

Most tasks can also be initiated by entering only part of a command as a shortcut, rather than entering the whole command. In the following chapters, that portion of the command that can be entered as a shortcut is indicated with an underscore. For example, the commands for listing users is shown as **list users**, and can be entered at the Config prompt as **l u**. Similarly, the command for viewing error statistics is shown as **error** and can be entered at the Monitor prompt as **er**.

Entering Subsystem Commands

Although the CLI is tree-structured, you can bypass that structure when you are familar with the commands for various subsytems. For example, if you are at the Monitor (Monitor>) prompt, you can check bridge information without going first to the Bridge console prompt (Bridge>). At the Monitor prompt you enter:

Monitor> **monitor bridge list all**

The Monitor prompt remains, but the data displayed is from the Bridge console subsystem. This shortcut allows you to execute a single command for a subsystem without leaving the Monitor or Config prompt.

You can also use this shortcut to enter commands for other GIGAswitch GS2000 module subsystems without leaving the current subsystem. For example, while at the Monitor IP> prompt, you can find out about bridge counters by entering the following command:

Monitor IP> **monitor bridge list counters summary**

Note

You cannot use this shortcut to execute a Config command while at the Monitor prompt. Nor can you execute a Monitor command while at the Config prompt. In either of these cases, you must enter the Config or Monitor component first, then enter the desired command.

Using Auto-Prompts

You can perform certain tasks either by entering commands and parameter variables as a string, or by responding to instructional prompts that walk you through each item you must enter.

Examples

To back up a switch's configuration database by entering the command and variables as a string, you enter a string similar to the following example:

`Boot config>`**tftp put config 11.22.33.44 /usr/local/tftp/switch11.cfg**

Alternatively, to back up a switch's configuration database in response to auto-prompts, you perform the following steps:

Step	Action
1	At the Boot config prompt, enter **tftp put**.
2	Press Return. The following message is displayed: `local filename [CONFIG]?` CONFIG is the default file name. It cannot be changed.
3	Press Return. The following message is displayed: `remote host [0.0.0.0]?`
4	Enter the IP address of the host to which you want to copy the configuration database. The default (`0.0.0.0`) is an invalid address, and is meant only to show the format of the address.
5	Press Return. The following message is displayed: `host filename [0B070706.cfg]?`
6	Enter the path, followed by a unique file name, to identify the location on the remote system where you want to back up the configuration database. The default is `0B070706.cfg`. It is recommended that you give the file a name that is descriptive of the switch from which it originates. By doing so, you should more easily be able to distinguish between backup files derived from multiple modules. **Example: /usr/local/tftp/switch11.cfg**
7	Press Return. The following message is displayed when the transfer is completed: `TFTP transfer complete, status: OK`

Note

Auto-prompts are not supported for all GIGAswitch GS2000 commands.

Displaying Help

You can obtain help at any of the GIGAswitch GS2000 prompts (Main, Config, or Monitor) and at most of the subsystem prompts (`Bridge Config>`, `VSD Config>`, and so on) by entering **?**, followed by pressing Return. Help is displayed as a list of the commands available at that prompt level. Use **?** (Help) to list the commands that are available from the current prompt level. You can also enter **?** after a specific command name to list its options.

Chapter 3

Adding and Managing Users

Overview

Introduction

This chapter provides instructions about assigning login permission and security levels to users who are to manage a DIGITAL GIGAswitch GS2000 module.

Users who are assigned administrative permission control access to module configuration and monitoring tasks. In addition, a user with any of the three security levels (administrative, operations, or monitor) can display a list of users and change their own password.

Caution

Login IDs and passwords are not required at installation. You can, however, configure the GIGAswitch GS2000 module to require users to enter a login ID and password. Refer to the Enabling and Disabling Prompting for ID and Password section for additional information.

In This Chapter

The following topics are covered in this chapter:

Adding Users

If a switch administrator enables prompting for ID and password, an individual cannot access module configuration and management functions unless the user's name is added to a user list, assigned a password, and given one of three security levels (administrative, operations, or monitor). Refer to the Enabling and Disabling Prompting for ID and Password section for information about requiring the entry of an ID and password. Refer to Chapter 1 for a description of the three security levels and the access privileges that each provides.

To add an individual to the user list, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **add user**.
2	Press Return. The following message is displayed: `Enter user name:  []?`
3	Enter the name of the user (**Mary**, for example). The name can be a maximum of eight characters and is case sensitive. Spaces are permitted. If the maximum of eight characters is exceeded, the entry is truncated.
4	Press Return. The following message is displayed: `Password:`
5	Enter a password for the user. The password can be a maximum of eight characters and is case sensitive.
6	Press Return. The following message is displayed: `Enter password again:`
7	Reenter the password you entered in step 5 to confirm that it is correct.
8	Press Return. The following message is displayed: `Enter permission: (A)dmin, (O)perations, or (M)onitor  [A]?`
9	Enter either an **A**, an **O**, or an **M** (for administrative, operations, or monitor, respectively) to designate one of the three possible permission levels you can assign. (Refer to Chapter 1 for a description of the three security levels and the access privileges that each provides.)

Step	Action
10	Press Return. The following message and the Config prompt are displayed: `User 'Mary' has been added` If prompting for ID and password mode (enable or disable console log-in) was changed prior to this procedure, a notification message to this effect is also displayed.

Note

You cannot enable ID and password prompting unless at least one user having administrative permission is added to the user list on the module you are configuring. The message, `Warning: Console login is disabled until an administrative user is added`, is displayed if you attempt to enable password prompting on a module for which there is no administrative user. Refer to the Enabling and Disabling Prompting for ID and Password section for additional information.

Displaying a List of All Users

You can display a list of all users, including the security (permission) levels to which they are assigned.

To view the list of users, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **list users**.

2	Press Return. A list of users is displayed, including the security (permission) level to which they are assigned.
	Example:
	`USER PERMISSION`
	`joe Operations`
	`mary Admin`
	`peter Monitor`
	`Console login-prompting is enabled`

Changing a User's Name, Password, and Security Level

You can change the name, password, and security level of another user, or change your own password.

Changing Your Own Password

You can change your own password, regardless of the security level to which you are assigned. To change your password, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **change password**.
2	Press Return. The following message is displayed: `Enter current password:`
3	Enter your current password.
4	Press Return. The following message is displayed: `Password:`
5	Enter your new password. The password can be a maximum of eight characters and is case sensitive.
6	Press Return. The following message is displayed: `Enter password again:`
7	Reenter the password you entered in step 5 to confirm that it is entered correctly. If the confirmation entry does not match the password you entered in step 5, your old password remains in effect.

Changing Another User's Password or Security Level

You must be assigned to the administrative security level to change another user's password or security level. To change another user's password or security level, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **change user**.
2	Press Return. The following message is displayed: `Enter user name: [ ]?`
3	Enter the name of the user whose information you want to change.
4	Press Return. The following message is displayed: `Change password? (Yes or [No]):`
5	Enter **Yes** if you want to change the user's password. Enter **No** if you do not want to change the user's password. **No** is the default.

6	Press Return.
	If you entered **No** in step 5, the following message is displayed:
	`Change permission? (Yes or [No]):`
	Go to step 11.
	If you entered **Yes** in step 5, the following message is displayed:
	`Password:`
	Go to step 7.

7	Enter the user's new password. The password can be a maximum of eight characters and is case sensitive.
8	Press Return. The following message is displayed: `Enter password again:`
9	Reenter the password you entered in step 7 to confirm that it is entered correctly.
10	Press Return. The following message is displayed: `Change permission? (Yes or [No]):`
11	Enter **Yes** if you want to change the permission level. Enter **No** if you do not want to change the permission level.

Step	Action
12	Press Return. If you entered **No**, the Config prompt (`Config>`) is displayed. If you entered **Yes**, the following message is displayed: `Enter permission: (A)dmin, (O)perations, or (M)onitor  [A]?`
13	Enter either an **A**, an **O**, or an **M** (for administrative, operations, or monitor, respectively) to designate one of the three possible permission levels you can assign. (Refer to Chapter 1 for a description of the three security levels and the access privileges that each provides.)
14	Press Return. The specified changes are made and the Config prompt (`Config>`) is displayed.

Enabling and Disabling Prompting for ID and Password

You can configure the module so that users are required to enter an ID and password before the CLI is displayed. You can also choose to disable ID and password prompts. If ID and password prompting is disabled, full access to all functions is available to any individual who logs in. That is, there are no restrictions to access of functions based on administrative, operations, and monitor privileges. Disabled is the default.

To enable and disable prompting for ID and password, perform the following steps:

Step	Action
1	If you want to enable ID and password prompting, at the Config prompt (`Config>`), enter **enable console-login-prompting**. If you want to disable ID and password prompting, at the Config prompt (`Config>`), enter **disable console-login-prompting**.
2	Press Return. ID and password prompting is enabled or disabled as specified.
3	Restart the module for the new setting to take effect.

Note

You cannot enable ID and password prompting unless at least one user having administrative permission is added to the user list on the module you are configuring. The message, `Warning: Console login is disabled until an administrative user is added`, is displayed if you attempt to enable password prompting on a module for which there is no administrative user.

Deleting Users

You can delete individuals from the list of users who have access to module configuration and management functions. You must be assigned to the administrative security level to do so. You can delete users either by deleting one user at a time using the **delete user** command, or by deleting all users from the list using the **clear users** command.

Deleting a Single User

To delete a single user, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **delete user**.
2	Press Return. The following message is displayed: `Enter user name: [ ]?`
3	Enter the name (**Mary**, for example) of the user you want to delete.
4	Press Return. The following message is displayed: `Delete 'Mary'? (Yes or [No]):`
5	Enter **Yes** if you want to delete the user. Enter **No** if you do not want to delete the user.
6	Press Return. If you entered **Yes**, the following message and the Config prompt are displayed: `User 'Mary' has been deleted` If you entered **No**, the Config prompt is displayed.

Deleting (Clearing) All Users

Deleting all users resets the user list to its factory default, deleting the names, passwords, and associated security levels of all individuals from the list. You must log in using a local console after you clear all users. If ID and password prompting (enabling and disabling remote console login) is currently enabled, the console login setting is temporarily disabled until a new user with administrative privileges is added.

Deleting Users

To delete all individuals from the list of users, perform the following steps:

Step	Action
1	At the `Config>` prompt, enter **clear user**.

2	Press Return. The following message is displayed:
	`You are about to clear all User configuration information`
	`Are you sure you want to do this (Yes or [No]):`

3	Enter **y** if you want to clear all user configuration information to the factory default. Enter **n** if you do not want to clear all user configuration information to the factory default.

4	Press Return. If you entered **y**, the following message and the `Config>` prompt are displayed:
	`User configuration cleared`
	If you entered **n**, the following message and the Config prompt (`Config>`) are displayed:
	`Aborted`

Chapter 4

Configuring and Monitoring Module-wide Parameters

Overview

Introduction

DIGITAL GIGAswitch GS2000 line card functional components can be divided into those that provide and affect specific network operations such as transparent bridging and interface-dependent functions, and those that provide and affect module-wide operation. This chapter provides information about how to manage and monitor functions that affect module-wide operation.

In This Chapter

This chapter discusses the following topics.

Resetting (Clearing) NVRAM to Default Values

You can reset nonvolatile memory (NVRAM) configuration parameters to their factory default values for one or all of the following functional components:

- Transparent bridging, including VLANs
- Backup (installation and dump) file locations
- Protocols (ARP, SNMP, and TCP/IP Host Services)
- ATM interface configuration settings
- Event Logging System (ELS)
- Users and passwords
- Time of day

You cannot reset FDDI interface configuration settings to factory defaults using the CLI. You must use the Reset with Factory Defaults option from the GIGAswitch GS2000 module installation menu. Refer to your GIGAswitch GS2000 module installation and configuration documentation for information about how to do so.

Refer to Appendix B for complete lists of default values for all functional components.

To reset the current configuration parameters for one or all functional components to their default values, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **clear** ***command-option***, where ***command-option*** is the command you must enter to specify the components for which you want to reset defaults. Refer to Table 4-1 for a list of commands, and for a description of the functional component for which you reset defaults when you enter the command.

Step	Action

2	Press Return.
	If you use either the **bridge** or the **all** command option, the following message is displayed:
	`You are about to clear all Bridge configuration information`
	`*** WARNING *** This will invoke an automatic RESTART`
	`Are you sure you want to do this (Yes or [No]):`
	If you use any of the other command options, the following message is displayed:
	`You are about to clear all SNMP configuration information`
	`Are you sure you want to do this (Yes or [No]):`

3	Enter **y** if you want to reset parameters for the specified functional component to their defaults. Enter **n** if you want to abort the command.
4	Press Return. If you are resetting parameters for all functional components or for boot configurations, the module is automatically restarted and the Main prompt (`Main>`) is displayed. If you are resetting parameters for any functional component other than for all functional components or for boot configurations, the parameters are reset in memory and the Config prompt (`Config>`) is again displayed. The operational state of the module may not immediately reflect a cleared configuration. You should restart the module to ensure that the changes take effect.

Table 4-1: Clear Command Options and Descriptions

Command	Description
bridge	Resets all NVRAM configuration parameters to factory defaults, such that transparent bridging is run on each port. All static or permanent address filters, as well as protocol filters are removed. All ports are reassigned to the default VLAN.
boot	Resets NVRAM parameters for the backup file locations of all image (installation), configuration, and dump files.
arp	Resets the Address Resolution Protocol.
snmp	Resets the SNMP Protocol.
tcp/ip	Resets Host Services (HST). IP addresses are removed, disabling remote management of the module.
atm	Resets all ATM physical and logical interface settings.
els	Resets all Event Logging System NVRAM configuration parameters.
time	Resets the time of day clock (module-wide parameter).
user	Resets user access and passwords. If ID and password prompting (enabling and disabling remote console login) is currently enabled, the console login setting is temporarily disabled until a new user with administrative privileges is added. (Refer to Chapter 3 for information about enabling and disabling prompting for ID and password.)
all	Resets NVRAM configuration parameters for most functional components including transparent bridging, VLANs, protocols, backup file locations, ATM interface settings, users and passwords, time of day, and ELS. You cannot reset FDDI interface configuration settings to factory defaults using the CLI. You must use the Reset with Factory Defaults option from the GIGAswitch GS2000 module installation menu. Refer to your GIGAswitch GS2000 module installation and configuration documentation for information about how to do so.

Setting the Session Inactivity Timer

You can set the amount of time a local or remote console is inactive before the module automatically logs out a user. This setting affects only those consoles linked to modules on which an ID and password is required to log in. (Refer to Chapter 3 for information about enabling and disabling prompting for ID and password.) The default setting of 0 (zero) turns off the inactivity timer, so that an established session remains active no matter how long a console is inactive.

To set the maximum amount of time a console can remain inactive, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **set inactivity-timer**.
2	Press Return. The following message is displayed: `Console inactivity timer in minutes [0]?`
3	Enter the maximum number of minutes you want a session to remain inactive before a user is automatically logged out. The value entered must be a whole number, and must be in the range of 1 through 65535. The default setting of 0 (zero) turns off the inactivity timer, so that an established session remains active no matter how long a console is inactive.
4	Press Return. The value you entered is set.
5	Restart the module. Refer to Chapter 10 for information about how to restart the module.

Example

`Config>`**set inactivity-timer 6**

Assigning a Host Name to the Module

You can identify the GIGAswitch GS2000 module by assigning it a host name. The name is used only for descriptive or informational purposes and does not affect or change the address of the module.

To assign a host name to the module, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **set hostname**.
2	Press Return. The following message is displayed: `What is the new host name []?`
3	Enter a name for the module. The name can be composed of alphanumeric characters and can be up to 80 characters long. Spaces are permitted.
4	Press Return. The name you specified is assigned to the module and the `Config>` prompt is displayed.
5	Restart the module. Refer to Chapter 10 for information about how to restart the module.

Example

`Config>`**set hostname Bldg 3-2**

Displaying General Information About the Module

You can display two reports that include general information about the module. One report is accessed from the Config prompt (`Config>`), and the other is accessed from the Monitor prompt (`Monitor>`).

Information Displayed from the Config Prompt

The report you display from the Config prompt (`Config>`) includes the name of the responsible contact person and the location of the module. It also includes such module-wide parameters and values as the maximum packet size and the amount of available configuration memory.

To view general information about the module from the Config prompt, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **list configuration**.
2	Press Return. A report that includes general information about the module is displayed.

Example

Config>**list configuration**

```
GIGAswitch GS2000, 1 ATM 1 FDDI,HW=04f1E1,RO=V1.5.5,#1083,SW=V2.0
Hostname: [none]
Routing: Not available
Maximum packet size: [autoconfigured]
Maximum number of global buffers: [autoconfigured]
Logging disposition: detached
Console inactivity timer (minutes): 0
Physical console login prompting: enabled
Prompting with hostname: disabled
Contact person for this node: [none]
Location of this node: [none]

Configurable Protocols:
Num Name  Protocol
3   ARP   Address Resolution
11  SNMP  Simple Network Management Protocol
23  BRIDGE Adaptive Source Routing Transparent Bridging
24  HST   TCP/IP Host Services

Configurable Features:
Num Name  Feature
5   RMON  Remote Monitoring
```

Information Displayed from the Monitor Prompt

The report you display from the Monitor prompt (Monitor>) includes information about module interfaces and protocols and the setup port baud rate used by local consoles.

To view general information about the module from the Monitor prompt, perform the following steps:

Step	Action
1	At the Monitor prompt (Monitor>), enter **list all**.
2	Press Return. A report that includes general information about the module is displayed.

Example

The following is an example of the information displayed for a module. The report is divided into three sections. The first section includes module identification information and the setup port baud rate used by the local console. Refer to Table 4-2 for a description of the last two sections of the report (protocols and interfaces).

`Monitor>`**list all**

```
GIGAswitch GS2000, 1 ATM 1 FDDI,HW=04f1E1,RO=V1.5.5,#1083,SW=V2.0
Hostname: GS2000
Console baud rate: 9600

Num Name   Protocol
3   ARP    Address Resolution Protocol
11  SNMP   Simple Network Management Protocol
23  BRIDGE Adaptive Source Routing Transparent Enhanced Bridge
24  HST    TCP/IP Host Services

Num Name   Feature
5   RMON   Remote Monitoring

18 Interfaces:
Ifc Name       MAC/Data-Link         Hardware       State
0   VNbus/0    VNbus-encapsulation   VNbus          Not present
1   FDDI/1     FDDI/IEEE 802.2       FDDI           Up
2   ALEC/2     ATM LAN Emulation C   ATM            Testing
3   ALEC/3     ATM LAN Emulation C   ATM            Testing
4   ALEC/4     ATM LAN Emulation C   ATM            Testing
5   ALEC/5     ATM LAN Emulation C   ATM            Testing
6   ALEC/6     ATM LAN Emulation C   ATM            Testing
7   ALEC/7     ATM LAN Emulation C   ATM            Testing
8   ALEC/8     ATM LAN Emulation C   ATM            Testing
9   ALEC/9     ATM LAN Emulation C   ATM            Testing
10  ALEC/10    ATM LAN Emulation C   ATM            Testing
11  ALEC/11    ATM LAN Emulation C   ATM            Testing
12  ALEC/12    ATM LAN Emulation C   ATM            Testing
13  ALEC/13    ATM LAN Emulation C   ATM            Testing
14  ALEC/14    ATM LAN Emulation C   ATM            Testing
15  ALEC/15    ATM LAN Emulation C   ATM            Testing
16  AFBT/16    ATM F Bridge Tunnel   ATM            Testing
17  AEBT/17    ATM E Bridge Tunnel   ATM            Down
```

Table 4-2: Description of the Configuration Report from the Monitor Prompt

Information Displayed	Description
Num	Number associated with the protocol.
Name	Protocol's short name.
Protocol	Full name of the protocol.
Ifc	Physical and logical interface number.
Name	Interface type (FDDI, ATM LEC, ATM FDDI Bridge Tunnel, and so on), followed by a number indicating the instance within this type. Instance numbering starts at zero.
MAC/Data Link	The type of MAC/data link configured for the interface.
Hardware	Interface hardware type.
State	Current state of the interface. The following states are possible: • `Up` — The interface is connected and operational. • `Down` — The interface is not operational and failed self-test. • `Disabled` — The interface is either temporarily or permanently disabled. • `Testing` — The interface is in the process of completing a self-test. • `Not present` — Power-up (restart) diagnostics detected a fault on the interface.

Setting and Viewing Clock Time

You can set the following time-related parameters for the module:

- Current time
- Time zone offset (from GMT)
- Frequency with which the module synchronizes with the time host when using a Network Time Protocol (NTP) server

You can also view the current settings to verify that they are set as desired.

Setting the Time

You can set the current time on the module clock in one of the following two ways:

- Manually
- Using a Network Time Protocol (NTP) server

Setting the Time Manually

You can set the module clock manually, based on the current wall clock time. To set the time, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **time set**.
2	Press Return. The following message is displayed: `year [0]?`
3	Enter the numeric representation for the current year using the full four digits. **Example: 1996**
4	Press Return. The following message is displayed: `month [0]?`
5	Enter the numeric representation for the current month. Do not use leading zeros. **Examples: 5** (for May) or **11** (for November)
6	Press Return. The following message is displayed: `date [0]?`

Step	Action
7	Enter the current day of the month. **Example: 22**
8	Press Return. The following message is displayed: `hour [0]?`
9	Enter the current hour of the day in military time. **Examples: 5** (for 5 AM) or **17** (for 5 PM)
10	Press Return. The following message is displayed: `minute [0]?`
11	Enter the current minute of the hour. **Example: 45**
12	Press Return. The following message is displayed: `second [0]?`
13	Enter the current second of the minute. **Example: 00**
14	Press Return. The clock is set.

Note

Alternatively, the above time can be entered using the following syntax:
time set 1996 11 22 17 45 00

Setting the Time Using an NTP Server

An NTP server provides a single-source location from which multiple devices can derive their clock settings. This helps ensure time synchronization among the various participating devices. The NTP server time is based on Greenwich Mean Time (GMT).

To set the time using an NTP server, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **time host**.

Step	Action
2	Press Return. The following message is displayed: `IP address of time host [0.0.0.0]?`
3	Enter the IP address of the NTP server from which you want to derive the current time.
4	Press Return. The clock is set and the Config prompt is displayed.
5	Restart the module if you want the new configuration settings to take effect.

Setting the Time Zone Offset

You can specify the time zone by setting the number of minutes that the current time is offset from Greenwich Mean Time (GMT). Values west of GMT are entered as negative values. For example, Eastern Standard Time (EST) in the United States is 5 hours earlier than GMT. Therefore, the offset for EST is –300 (5 hours x 60 minutes/hour). The default of 0 (zero) indicates no offset from GMT.

To set the time zone offset, perform the following steps:

Step	Action
1	At the `Config>` prompt, enter **time offset**.
2	Press Return. The following message is displayed: `minutes from GMT (-720 to 720) [0]?`
3	Enter the number of minutes the time zone is offset from GMT.
4	Press Return. The time zone offset is configured and the `Config>` prompt is displayed.

Note

Alternatively, the time zone offset can be entered using the following syntax:
time offset –300

Setting Time Host Synchronization

You can set the frequency, in seconds, with which the module polls the time host for the current time. This function is applicable only if you are using an NTP server to synchronize the module clock. The default of 0 (zero) indicates the module is not to poll the time host to synchronize clocks. You must configure TCP/IP Host Services for this functionality to be operational. Refer to Chapter 12 for information about configuring TCP/IP Host Services.

To set the frequency with which the module polls the time host for the current time, perform the following steps:

Step	Action
1	At the `Config>` prompt, enter **time sync**.
2	Press Return. The following message is displayed: `seconds between time syncs [0]?`
3	Enter the number of seconds that is to pass between polling attempts.
4	Press Return. The frequency is set and the `Config>` prompt is displayed.
5	Restart the module if you want the new configuration settings to take effect.

Note

Alternatively, the time host polling frequency can be entered using the following syntax: `Config>`**time sync 10**

Viewing Clock Time Parameters

You can view the current time settings to verify that they are set as desired. The information includes information about who or what last set the time (either the operator, or the IP address of the time host).

To view the current settings, perform the following steps:

Step	Action
1	At the `Config>` prompt, enter **time list**.
2	Press Return. A report of the current time settings is displayed, and the `Config>` prompt is displayed.

Example

`Config>`**time list**

```
11:21:21  Friday September 5, 1997
Set by: 110.110.110.157
Time Host:  110.110.110.157          Sync Interval: 1200 seconds
GMT Offset:  -240 minutes
```

Monitoring Module Memory

You can display a report that contains information about module CPU memory, number of buffers, and packet sizes. The information provided by the memory report reflects activity occurring on the module's management processor only. It does not include data about memory in the module's forwarding subsystem.

Note

Sufficient free memory must be available to display this report. The number of free packet buffers may drop to zero (0), resulting in the loss of some incoming packets. However, this does not adversely affect module operations.

To display the report, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **memory**.
2	Press Return. The report and the Monitor prompt are displayed.

Example

```
Monitor>memory

                Total  Reserve    Never     Perm     Temp     Prev
                                  Alloc    Alloc    Alloc    Alloc
Heap memory     6232191    24784  2926207  3271888    28464     5632
Number of global buffers: Total = 400, Free = 367, Fair = 77, Low = 80
Global buff size: Data = 4478, Hdr = 25, Wrap = 0, Trail = 8, Total = 4516
```

Refer to Table 4-3 for a description of the information.

Table 4-3: Description of the Memory Report

Information Displayed	Description
Heap memory	Memory available for dynamically allocated data structures including, for example, ARP database entries.

Information Displayed	Description
Heap memory: Total	Original amount of space available for allocation of memory (heap size total).
Heap memory: Reserve	Minimum amount of memory required by the currently configured protocols.
Heap memory: Never Alloc	Amount of memory that has never been allocated.
Heap memory: Perm Alloc	Amount of memory requested for permanent allocation.
Heap memory: Temp Alloc	Amount of memory temporarily allocated.
Heap memory: Prev Alloc	Amount of memory temporarily allocated and then returned.
Number of Global Buffers: Total	Original number of global buffers on the system.
Number of Global Buffers: Free	Current number of global buffers available.
Number of Global Buffers: Fair	Fair number of buffers for each interface. (Refer to Number of Global Buffers: Low in this table.)
Number of Global Buffers: Low	Number of free buffers at which the allocation strategy changes to conserve buffers. If the value of Free is less than Low, then buffers are not placed on any queue containing more than the Fair number of buffers.
Global buff size: Data	Maximum data link packet size of all interfaces.
Global buff size: Hdr	Sum of the maximum hardware, MAC, and data link headers of all interfaces.
Global buff size: Wrap	This parameter is always zero and is not currently used by the module.
Global buff size: Trail	Sum of the largest MAC and hardware trailers for interfaces.
Global buff size: Total	Size of the largest packet buffer.

Monitoring Crash Counts and Restart or Reload Data

You can display the following information about module crashes and module restarts or reloads:

- Number of restarts
- Number of known crashes
- Whether the module was last reloaded or restarted
- Time elapsed since the last reload
- Time elapsed since the last restart

To display information about crash counts and module restarts or reloads, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **uptime**.
2	Press Return. Information about crash counts and module restarts or reloads is displayed, and the Monitor prompt is redisplayed.

Example

```
Monitor>uptime

1 Start, (0 known crashes)
Last Power Up:  41 minutes ago
Last Restart:  41 minutes ago
```

Chapter 5

Configuring Network Interfaces

Overview

Introduction

DIGITAL GIGAswitch GS2000 modules support FDDI and ATM network interfaces. All interfaces are automatically added and configured when a module is installed. The configuration settings used are the factory defaults listed in the following sections and in Appendix B. You may need to alter the default settings to maximize network performance, and to accommodate requirements unique to your network environment. This chapter provides information about how to do so.

In This Chapter

The following topics are covered in this chapter:

Displaying the Interface Number and Type

You can display the number assigned to an interface and the interface type (FDDI or ATM). You may typically need to do so before you perform other tasks discussed in this chapter.

To list a module's interface numbers and types, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **list interfaces**.
2	Press Return. A list of the interfaces on the module is displayed, including the interface's assigned number.

Example

The following example applies to the GIGAswitch GS2000 module:

`Config>`**list interfaces**

```
Ifc  Type
 0   GIGAswitch VNbus
 1   GIGAswitch FDDI
 2   GIGAswitch ATM
 3   GIGAswitch ATM
 4   GIGAswitch ATM
 5   GIGAswitch ATM
 6   GIGAswitch ATM
 7   GIGAswitch ATM
 8   GIGAswitch ATM
 9   GIGAswitch ATM
10   GIGAswitch ATM
11   GIGAswitch ATM
12   GIGAswitch ATM
13   GIGAswitch ATM
14   GIGAswitch ATM
15   GIGAswitch ATM
16   GIGAswitch ATM
17   GIGAswitch ATM
```

Enabling and Disabling an Interface

You can enable and disable a logical interface (FDDI or ATM). You may need to disable an interface, for example, if you want to logically disconnect a portion of a network while making significant changes to the network segment's physical environment. Enabled is the default.

Enabling and disabling an interface does not require that you restart the module for the setting to take effect. The setting is effective immediately. These settings survive power outages and module restarts.

Note

You can also enable and disable the ATM logical interface through volatile memory from the `ATM/n Config>` prompt, as described in the Configuring ATM Physical and Logical Interfaces section later in this chapter. Enabling or disabling the ATM interface from the `ATM/n Config>` prompt allows you to do so without accessing the Monitor prompt and then returning to `ATM/n Config>`.

The following sections describe how to disable and enable an interface.

Disabling an Interface

To disable an interface, perform the following steps:

Step	Action
1	At the `Config>` prompt, enter **disable interface** ***interface#***, where ***interface#*** is the number of the interface you want to disable. Refer to the Displaying the Interface Number and Type section for information about how to determine the number assigned to an interface.
2	Press Return. The interface is disabled as specified.

Enabling an Interface

To enable an interface, perform the following steps:

Step	Action
1	At the `Config>` prompt, enter **enable interface *interface#***, where ***interface#*** is the number of the interface you want to enable. Refer to the Displaying the Interface Number and Type section for information about how to determine the number assigned to an interface.

2	Press Return.
	The state of the interface is first tested and the following message is displayed:
	`Testing interface 1 FDDI/1...`
	If the test is successful, the following message is displayed and the interface is enabled:
	`Testing interface 1 FDDI/1...successful`
	If the test failed, the following message is displayed:
	`Testing interface 1 FDDI/1...failed`
	If testing takes longer that 30 seconds, the Config process may time out and display the following message:
	`Testing interface 1 FDDI/1...still testing`

Accessing and Exiting an Interface Prompt

Each type of interface (FDDI and ATM) has its own configuration prompt that you must access to configure the interface or to view configuration information associated with the interface. The prompts are accessed from the Config prompt (`Config>`).

Accessing an Interface Prompt

To access an interface prompt, perform the following steps:

Step	Action
1	Determine the network interface numbers for which the module is currently configured. Refer to the Displaying the Interface Number and Type section.
2	Record the desired interface numbers.
3	At the Config prompt, enter **interface**, followed by a space and the number of the logical interface you want to configure. **Example:** `Config>`**interface 1**
4	Press Return. The configuration prompt for the selected interface is displayed on the console. The *n* refers to the number of the selected interface. The following is a list of possible interface configuration prompts: • `FDDI/`*n* `Config>` (for an FDDI interface) • `ATM/`*n* `Config>` (for an ATM interface)

Exiting an Interface Prompt

To exit an interface prompt, type **exit** and then press Return. You exit an interface prompt to return to the next higher level prompt. For example, to return to the Config prompt (`Config>`) from the ATM interface configuration prompt (`ATM/`*n* `Config>`), enter **exit**, and then press Return.

Configuring an FDDI Logical Interface

The GIGAswitch GS2000 line card (GS2000) module includes 1 FDDI interface pair. You can perform the following tasks when configuring an FDDI logical interface:

- Set the station type.
- Set Link Error Rate alarm and cutoff values.
- Enable and disable SMT notification.
- Set token passing and frame timing parameters.
- Enable and disable purging of bad frames.
- Set the interface for a full- or half-duplex circuit.
- Reset all configuration parameters to default values.
- Display current FDDI interface configuration parameters.

Caution

It is recommended that the only configuration tasks you perform on an FDDI interface is setting the station type, setting the interface for full- or half-duplex mode, resetting parameters to defaults, and displaying current parameters. It is recommended that you alter the remaining settings *only* if you fully understand the effect the change will have on the entire network.

Supported Station Types

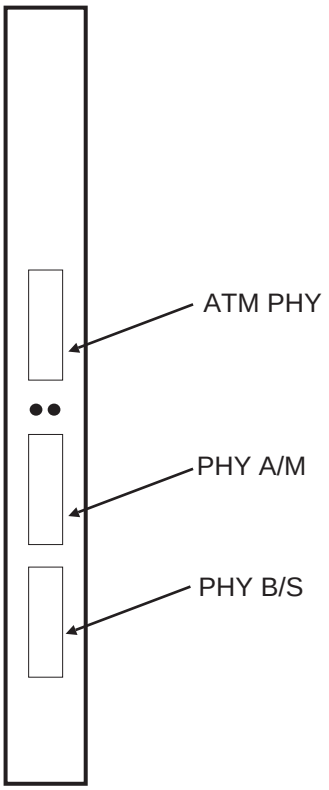
GIGAswitch GS2000 modules can serve as any one of the following FDDI station types:

- Dual Attachment Station (DAS)
- Single Attachment Concentrator (SAC)

PHY Port Identification

The GIGAswitch GS2000 FDDI interface is composed of two PHY ports labeled A/M and B/S (Figure 5-1).

Figure 5-1: GS2000 PHY Ports



LKG-10701-97WI

The PHY A/M port functions as either an A port or an M port, depending on the module's station type. Similarly, the PHY B/S port functions as either a B port or an S port. Table 5-1 shows the relationship between station type and PHY ports.

Note

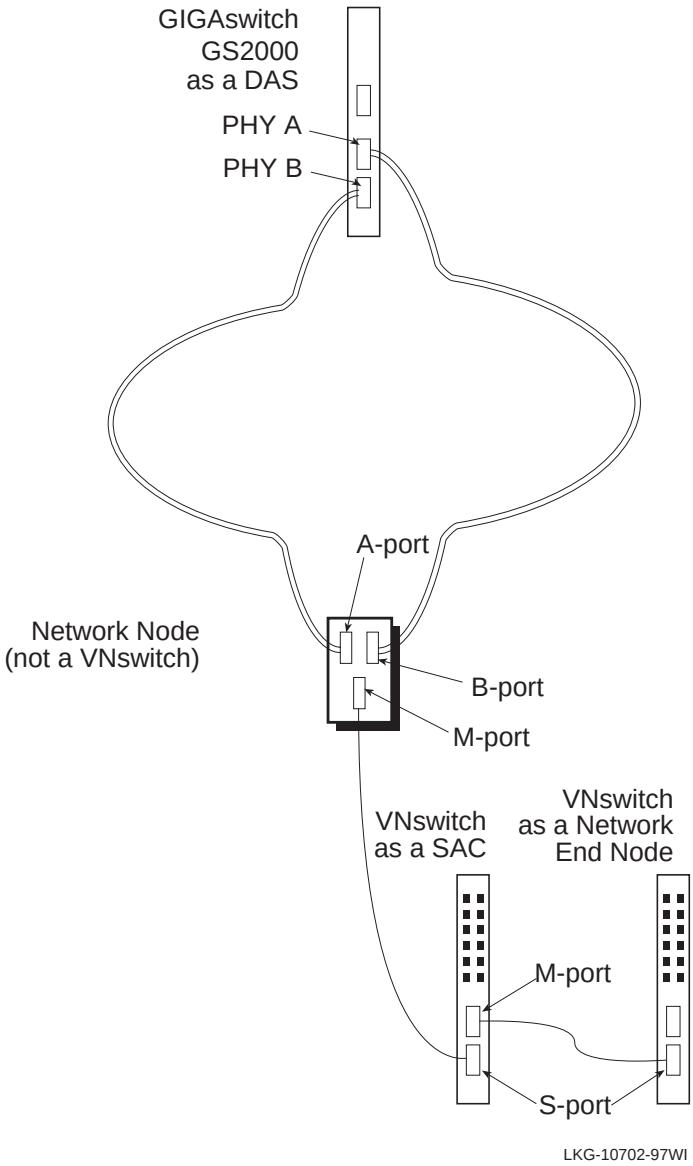
The FDDI logical interface on a GIGAswitch GS2000 module is assigned interface number 1, and bridge port number 1. These numeric assignments cannot be changed.

Table 5-1: Station Types and PHY Ports

If. . .	Then. . .
The GIGAswitch GS2000 module is cabled as a DAS	PHY A/M can be used either as an A port connected to the FDDI ring, or to the M port of a DAC if in a dual homing topology. PHY B/S can be used either as a B port connected to the FDDI ring, or to the M port of a DAC if in a dual homing topology.
The GIGAswitch GS2000 module is cabled as a SAC	PHY A/M is used as an M port connected to the S port of a SAS. PHY B/S is an S port connected to the M port of a Dual Attachment Concentrator (DAC).
The GIGAswitch GS2000 module is cabled as a SAS	PHY B/S is an S port connected to the M port of either a SAC or DAC. PHY A/M is not used.

Figure 5-2 illustrates the PHY port connections when the GIGAswitch GS2000 module serves as a DAS or SAC.

Figure 5-2: Sample FDDI Configuration and Associated PHY Ports



Setting the Station Type

The FDDI interface must be configured to reflect the station type for which the physical cables are connected. For example, if the GIGAswitch GS2000 module is cabled to function as a Single Attachment Concentrator, you must set the station type for the interface to SAC. The default installation setting is DAS.

To set or change the station type, perform the following steps:

Step	Action
1	At the `FDDI/1 Config>` prompt, enter **set station *station-type***, where ***station-type*** is **das** for a Dual Attachment Station, or **sac** for either a Single Attachment Concentrator or a Single Attachment Station. The default is **das**.
2	Press Return. The interface is set as specified, and the `FDDI/1 Config>` prompt is displayed.

Setting the Link Error Rate Alarm

The GIGAswitch GS2000 module monitors the number of link errors that occur over each PHY port's link. The types of link errors it monitors includes, for example, line state violations. Notification messages are sent to the SMT management station when the link error rate exceeds a number referred to as the alarm value. You can set the alarm value that triggers notification messages sent to the management station. The value is set independently for each of the module's PHY ports. For example, the value for PHY port A is set independently of the value for PHY port B on a DAS.

Note

Link error rate is expressed as a negative exponential value of base 10. For example, an error rate of 10^{-4} is equal to 0.0001 bits per second, 10^{-5} is equal to 0.00001 bits per second, and so on.

To set the link error alarm, perform the following steps:

Step	Action
1	At the `FDDI/1 Config>` prompt, enter **set phy *port* ler-alarm**, where ***port*** is either **a/m** for an A/M PHY port, or **b/s** for a B/S PHY port.
2	Press Return. The following message is displayed: `Link error alarm rate in -Log10: [8]?`

Step	Action
3	Enter a whole number from 4 through 12, where the number is a negative exponential value of base 10. Therefore, for example, entering a **4** sets the value at 10^{-4} (0.0001 bits per second), entering a **5** sets the value at 10^{-5} (0.00001 bits per second), and so on. The default value is 8.
4	Press Return. The link error rate alarm is set as specified, and the `FDDI/1 Config>` prompt is displayed.

Automatically Disconnecting Nodes Causing Excessive Link Errors

The GIGAswitch GS2000 module monitors the number of link errors that occur over each PHY port's link. The types of link errors it monitors includes, for example, line state violations. The neighbor node connected to a link is disconnected from the network if the error rate exceeds a number referred to as the cutoff value. You can set the cutoff value that triggers disconnection of a neighbor node. The value is set independently for each of the module's PHY ports. For example, the value for PHY port A is set independently of the value for PHY port B on a DAS.

If disconnection of a neighbor node is triggered, the FDDI network establishes a loopback (wrap) onto the secondary ring at the node that initiated the disconnect. The connection is automatically reestablished when the link is again active.

Note

Link error rate is expressed as a negative exponential value of base 10. For example, an error rate of 10^{-4} is equal to 0.0001 bits per second, 10^{-5} is equal to 0.00001 bits per second, and so on.

To set the link error cutoff, perform the following steps:

Step	Action
1	At the `FDDI/1 Config>` prompt, enter **set phy** ***port*** **ler-cutoff**, where ***port*** is either **a/m** for an A/M PHY port, or **b/s** for a B/S PHY port.
2	Press Return. The following message is displayed: `Link error cutoff rate in -Log10: [8]?`

Step	Action
3	Enter a whole number from 4 through 15, where the number is the exponential value of base 10. Therefore, for example, entering a **4** sets the value at 10^{-4} (0.0001 bits per second), entering a **5** sets the value at 10^{-5} (0.00001 bits per second), and so on. The default value is 8.
4	Press Return. The link error rate cutoff is set as specified, and the `FDDI/1 Config>` prompt is displayed.

Enabling and Disabling SMT Notification

FDDI stations use Status Report Frames (SRFs) to notify the SMT management station about certain events or conditions. The events and conditions can include, for example, ring wrap, exceeding thresholds such as link error alarm and cutoff values, and the detection of an illegal port type configuration.

To set the status report policy, perform the following steps:

Step	Action
1	At the `FDDI/1 Config>` prompt, enter **set status-report-policy *state***, where ***state*** is either **on** or **off**. Enter **on** if you want the module to send SRFs to the management station. Enter **off** if you do not want the module to send SRFs. The default is **on**.
2	Press Return. SMT notification is enabled or disabled, as specified, and the `FDDI/1 Config>` prompt is displayed.

Setting Token Passing and Frame Timing Parameters

FDDI uses token passing to control which station has access to the network at any given time. When a station that is ready to transmit data receives the token, the station removes the token from the ring and transmits its data. When data transmission is complete, the station places the token back on the ring.

A token can, occasionally, become lost or corrupted. FDDI stations use a configurable setting called the Maximum Token Rotation Time (tmax-lower-bound) to regenerate a token if this situation occurs. The Maximum Token Rotation Time is the length of time a station waits to receive the token, since the last time it had possession. If the Maximum Token Rotation Time is exceeded, the station then uses a second value, the Requested Token Rotation Time (t_req) to negotiate for token possession. The node

with the lowest Requested Token Rotation Time wins the bid for the token. If more that one station has the same Requested Token Rotation Time, the station with the highest MAC address wins.

Similarly, FDDI stations use a configurable setting called the Valid Transmission Time (tvx-timer) to determine the maximum amount of time the interface waits to receive a *valid* data frame. The absence of valid data frames for an extended period of time might be caused by conditions such as babble errors, repeated partial frames, or loss of the token. If the Valid Transmission Time is exceeded, the token claim process is reinitiated.

Setting the Maximum Token Rotation Time

To set the Maximum Token Rotation Time (tmax-lower-bound), perform the following steps:

Step	Action
1	At the `FDDI/1 Config>` prompt, enter **set tmax-lower-bound *#-of-milliseconds***, where ***#-of-milliseconds*** is equal to the maximum number of milliseconds the interface waits for a token. The ***#-of-milliseconds*** can be a number from 8 through 1331 milliseconds. The default is 167 milliseconds. **Note:** The software rounds the specified value to the nearest multiple of 5.24288 milliseconds. For example, the default value of 167 milliseconds is interpreted by the software as 167.77216 milliseconds.
2	Press Return. The Maximum Token Rotation Time is set and the `FDDI/1 Config>` prompt is displayed.

Setting the Requested Token Rotation Time

To set the Requested Token Rotation Time (t_req), perform the following steps:

Step	Action
1	At the `FDDI/1 Config>` prompt, enter **set t_req *#-of-milliseconds***, where ***#-of-milliseconds*** must be a value that is greater than the Minimum Token Rotation Time (6 milliseconds) and less than the Maximum Token Rotation Time (8 - 1331 milliseconds). The default is 8 milliseconds. **Note:** The software rounds the specified value to the nearest multiple of 20.48 microseconds. For example, the default value of 8 milliseconds is interpreted by the software as 7.9872 milliseconds.
2	Press Return. The Requested Token Rotation Time is set and the `FDDI/1 Config>` prompt is displayed.

Setting the Valid Transmission Timer

To set the Valid Transmission Time (tvx-timer), perform the following steps:

Step	Action
1	At the `FDDI/1 Config>` prompt, enter **set tvx-timer *#-of-milliseconds***, where ***#-of-milliseconds*** is equal to the maximum number of milliseconds the interface waits for a data frame. The ***#-of-milliseconds*** can be a number from 1 millisecond through 5 milliseconds. The default is 2.5 milliseconds. **Note:** The software rounds the specified value to the nearest multiple of 20.48 microseconds. For example, the default value of 2.5 milliseconds is interpreted by the software as 2.51904 milliseconds.
2	Press Return. The Valid Transmission Time is set and the `FDDI/1 Config>` prompt is displayed.

Configuring the Interface to Purge Bad Frames From the Ring

The GIGAswitch GS2000 FDDI interface is able to detect and remove frame fragments and No Owner Frames (NOFs) from the ring through a function referred to as the Ring Purger. You can turn the Ring Purger on or off using the CLI.

It is generally recommended that you leave the Ring Purger on. The purger uses available bandwidth on the ring to ensure that fragments and No-Owner Frames are removed. Only a very small percentage of available bandwidth may be lost with the purger running if the ring is operating at very high traffic levels. However, when the purger is running, the frame counter observed on any MAC on the ring shows a much larger count than what may be expected. The high number may be the result of including void frames in the total. The value may not, therefore, necessarily reflect a loss of bandwidth.

If these larger frame counts interfere with measurements you wish to make, then the ring purger can be disabled. Note that all nodes capable of being the ring purger must be disabled in order for there to be no ring purger on the ring (ring purging is an elective process). If you attempt to use the frame counter to make utilization measurements, a more accurate method of doing so is available using the MultiChassis Manager feature that provides ring latency and token counts. Refer to Chapter 6 of this document for information about how to monitor the FDDI interface to view the frame count.

To turn the Ring Purger on or off, perform the following steps:

Step	Action
1	At the `FDDI/1 Config>` prompt, enter **set ring-purger *state***, where ***state*** is either **on** or **off**. The default is **off**.
2	Press Return. The Ring Purger is turned on or off, as specified, and the `FDDI/1 Config>` prompt is displayed.

Setting the Interface for Full-Duplex or Half-Duplex Mode

You can set the FDDI interface to function in either full-duplex mode or half-duplex mode. If you set the interface for full-duplex mode, the link will function as a full-duplex circuit only if the device with which auto-negotiation occurs is also enabled for full-duplex mode. If not, half-duplex mode is used.

An interface is typically set for full-duplex mode if it is established as a point-to-point connection to a single device, and for half-duplex mode if connected to a shared medium supporting multiple devices.

Because the auto-negotiation process detects a point-to-point connection before entering full-duplex mode, it is unnecessary to disable it on half-duplex configurations.

To set the FDDI interface for either full-duplex or half-duplex mode, perform the following steps:

Step	Action
1	At the `FDDI/1 Config>` prompt, enter **set full-duplex *state***, where ***state*** is either **on** (for full-duplex mode) or **off** (for half-duplex mode). The default is **on**.
2	Press Return. The interface is set for either full-duplex or half-duplex mode, as specified, and the `FDDI/1 Config>` prompt is displayed.

Resetting All Configuration Parameters to Default Values

You can reset the current interface configuration settings (station type, link error rate alarm, Ring Purger, and so on) to their default values. Refer to the appropriate section in this chapter for information about the default value for a specific parameter, or to Appendix B for a concise list of FDDI interface defaults.

Note

You must restart the GIGAswitch GS2000 module after resetting the configuration parameters for the default values to take effect. Refer to Chapter 10 for information about how to restart the module.

To reset the current FDDI interface configuration parameters to their default values, perform the following steps:

Step	Action
1	At the `FDDI/1 Config>` prompt, enter **clear**.
2	Press Return. The following message is displayed: `For defaults to take effect, restart or reboot is required.`
3	Restart the GIGAswitch GS2000 module according to the instructions provided in Chapter 10.

Displaying Current FDDI Interface Configuration Parameters

You can display specific information about various FDDI interface configuration settings. To display configuration information, perform the following steps:

Step	Action
1	At the `FDDI/1 Config>` prompt, enter **list *configuration***, where ***configuration*** is the command you must enter to display the desired information. Refer to Table 5-2 for a list of commands, and for a description of the type of information that is displayed when you enter the command.
2	Press Return. The desired information and a new `FDDI/1 Config>` prompt is displayed.

Example

```
FDDI/1 Config>list all

Network Interface: 1
STATION TYPE: DAS
Status Report Policy: On
T_REQ: 7.9872ms
TVX: 2.51904ms
T_MAX: 167.77216ms
LER Cutoff, PHY A/M: 10^-8
LER Cutoff, PHY B/S: 10^-8
LER Alarm, PHY A/M: 10^-8
LER Alarm, PHY B/S: 10^-8
Ring Purger: Off
Full Duplex: On
```

Table 5-2: List Command Options and Descriptions for FDDI Configurations

Command	Description
station-type	Lists the station type (DAS or SAC) assigned to the module.
phy	Displays the Link Error Rate cutoff and alarm values for each PHY port on the interface. The link error rate is expressed as a negative exponential value of base 10.
status-report-policy	Displays the state (on or off) of the status report policy.
t_req	Displays the Requested Token Rotation Time, in milliseconds.
tvx-lower-bound	Displays the Valid Transmission Time, in milliseconds.
tmax-lower-bound	Displays the Maximum Token Rotation Time, in milliseconds.
ring-purger	Displays the status (on or off) of the Ring Purger.
full-duplex	Indicates whether the interface is set for full-duplex mode (on) or half-duplex mode (off).
all	Displays information about all of the above commands.

Configuring ATM Physical and Logical Interfaces

The GIGAswitch GS2000 module includes 1 ATM physical interface. The ATM physical interface supports up to 16 logical interfaces, numbered 2 through 17. Each logical interface can be either an ATM Bridge Tunnel, or a LAN Emulation Client (LEC) connected to an Emulated LAN (ELAN). The ATM logical interfaces are directed to the ATM physical interface on the front panel of the module. (Refer to Chapter 1 for information about distinguishing between physical and logical interfaces.)

Configuring the Physical Interface

You can perform the following tasks when configuring an ATM physical interface:

- Set the transmission type (SONET or SDH) and timing.
- Set payload scrambling to help ensure data integrity.
- Initiate a self-test of the ModPHY card.
- Display current physical interface settings.

Accessing the Configuration Prompt

ATM logical interfaces are directed to the ATM physical interface on the front panel of the module. You configure and display parameters for the front panel by accessing different CLI prompts.

To access the configuration prompt for the ATM physical interface on the front panel, perform the following steps:

Step	Action
1	To set parameters or display information about the interface, enter **physical** at the `ATM/n Config>` prompt.
2	Press Return. The `ATM_OC3_Config>` prompt is displayed.

Setting the Transmission Type and Timing

The ATM physical interface can be set to use either the Synchronous Optical Network (SONET) or the Synchronous Digital Hierarchy (SDH) transmission type. SONET is the frame format most commonly used in the United States. SDH is the frame format most commonly used in European countries. The transmission type used by the module must be the same as that used by other devices on an ATM network.

Transmission and receipt of SONET or SDH frames must be synchronized among the ATM interface and devices with which the module communicates. The timing can be based on the system clock of either the module or some other device on the network.

Setting the Transmission Type

To set the transmission type, perform the following steps:

Step	Action
1	To set the transmission type, access the `ATM_OC3_Config>` prompt.
2	Enter **set transmission-type**.
3	Press Return. The following message is displayed: `Transmit type (SONET or SDH):`
4	If you want to use the SONET frame format, enter **sonet**. If you want to use the SDH frame format, enter **sdh**. The factory default is **sonet**.
5	Press Return. The transmission type is set.

Setting Transmission Timing

To set (synchronize) transmission timing, perform the following steps:

Step	Action
1	If you want to set timing for the physical interface, access the `ATM_OC3_Config>` prompt.
2	Enter **set timing**.
3	Press Return. The following message is displayed: `Timing (loop or local (default)):`
4	If you want to synchronize the devices according to the module's clock, enter **local**. If you want to synchronize the devices according to the remote device's clock, enter **loop**. The factory default is **local** for the front panel interface.
5	Press Return. Synchronization is set for the chosen interface.

Enabling and Disabling Payload Scrambling

Payload scrambling is a function used to help ensure data integrity at the level of the SONET or SDH payload envelope. This process is enabled, by default, on the GIGAswitch GS2000 module. If the module is to communicate with a DIGITAL GIGAswitch/FDDI AGL2, you must disable payload scrambling because it is not supported on the GIGAswitch/FDDI AGL2.

To disable or enable payload scrambling, perform the following steps:

Step	Action
1	To set payload scrambling for the physical interface, access the `ATM_OC3_Config>` prompt.
2	Enter **set payload-scramble**.
3	Press Return. The following message is displayed: `Payload scramble (enable or disable):`
4	If you want to disable payload scrambling, enter **disable**. If you want to enable payload scrambling, enter **enable**. The factory default is **enable**.
5	Press Return. Payload scrambling is disabled or enabled for the chosen interface.

Testing the modPHY Card

Loopback testing is used to test the integrity of the ATM modPHY card. If connected to the ATM physical interface on the module's front panel, the PHY LED lights green if the card passes the test. The LED does not light, or lights yellow, if the card fails the test. Refer to Chapter 6 for information about monitoring the ATM physical interface.

Caution

Communication is lost during a loopback test. You should not, therefore, perform a loopback test during critical business hours unless you notify network managers responsible for other nodes. Setting loopback to on (**yes**) automatically reestablishes communication between the GIGAswitch GS2000 module's ATM interface and the network.

To turn the loopback test on or off, perform the following steps:

Step	Action
1	To turn on the loopback test for the physical interface, access the `ATM_OC3_Config>` prompt.
2	Enter **set loopback**.
3	Press Return. The following message is displayed: `Loopback (yes or no):`
4	If you want to turn on the loopback test, enter **yes**. If you want to turn off the loopback test, enter **no**. The factory default is **no**.
5	Press Return. Loopback testing is turned on or off for the chosen interface.

Displaying Current Settings

You can display information about current ATM physical interface configuration settings. To display current configuration settings, perform the following steps:

Step	Action
1	To display current settings for the physical interface, access the `ATM_OC3_Config>` prompt.
2	Enter **list**.
3	Press Return. The desired information is displayed.

Example

```
ATM_OC3_Config>list

payload scramble         :  enable
transmission type        :  sonet
timing                   :  local
loopback                 :  no
```

Configuring a Logical Interface

You can perform the following tasks when configuring an ATM logical interface:

- Enable or disable the interface.
- Configure the interface as an ATM Bridge Tunnel.
- Configure the interface as a LAN Emulation Client (LEC) on an Emulated LAN (ELAN).
- Display the currently selected interface type and state.

Logical Interfaces Established at Startup

Table 5-3 lists the ATM logical interfaces automatically established after installation, and the conditions under which they are active. Each of these default connections can be modified. For example, you can change the default LEC configured on interface 2 to an ATM Bridge Tunnel, if desired.

Table 5-3: ATM Interface Defaults at Startup

Logical Interface Number	Type of Connection Established	Conditions Under Which Connection Is Established
2	ELAN	The GIGAswitch GS2000 module's ATM interface is connected to a DIGITAL GIGAswitch/ATM, or any UNI 3.1-compliant switch.
16	FDDI ATM Bridge Tunnel	The GIGAswitch GS2000 module's ATM interface is connected to a DIGITAL GIGAswitch/FDDI with an AGL2 Card.
17	Ethernet ATM Bridge Tunnel	The GIGAswitch GS2000 module's ATM interface is connected to the ATM interface of a VNswitch 900 series module.

Disabling and Enabling an ATM Logical Interface

You must disable the ATM interface before you reconfigure an ATM Bridge Tunnel or LEC. If you attempt to reconfigure the interface while it is still enabled, CLI and SNMP requests are rejected.

The procedure described in this section provides instructions about how to disable and enable the interface dynamically, through volatile memory from the `ATM/n Config>` prompt. Enabling and disabling an ATM interface through volatile memory does not require that you restart the module to take effect. The setting is effective immediately and does not survive power outages and module restarts. This method of enabling and disabling an interface is most useful when you want to temporarily enable or disable an interface.

Note

You can also enable and disable the ATM interface through volatile memory or NVRAM from the Monitor prompt (Monitor>) and the Config prompt (Config>), respectively. Refer to the Enabling and Disabling an Interface section earlier in this chapter for information about how to do so. However, enabling and disabling the ATM interface from the `ATM/n Config>` prompt allows you to do so without accessing the Monitor prompt or Config prompt, and then returning to `ATM/n Config>`.

Disabling the ATM Interface

To disable the ATM interface through volatile memory, perform the following steps:

Note

You may not be able to disable an interface if the interface is in the process of completing a self-test. If this is the case, one of two messages is displayed. The first indicates self-test is being canceled. The second indicates self-test is in progress and the interface cannot be disabled at this time. If either message is displayed, you can attempt to disable the interface at a later time.

Step	Action
1	At the `ATM/n Config>` prompt, enter **disable-interface**.
2	Press Return. The interface is disabled and the `ATM/n Config>` prompt is displayed.

Enabling the ATM Interface

To enable an interface through volatile memory, perform the following steps:

Step	Action
1	At the `ATM/n Config>` prompt, enter **enable-interface**.
2	Press Return. The interface is enabled and the `ATM/n Config>` prompt is displayed.

Displaying the Logical Interface Type and State

To display the type and state of the currently selected interface, perform the following steps:

Step	Action
1	At the `ATM/n Config>` prompt, enter **list**.
2	Press Return. The report and the `ATM/n Config>` prompt are displayed.

Example

```
ATM/2 Config>list

Interface               : 2 (Bridge Port 2)
Interface Type          : Lec
Lec Status              : INITIAL
Elan Name(Configured)   :
Elan Name(Joined)       : Not available
```

Configuring an ATM Bridge Tunnel Interface

ATM Bridge Tunnels are Permanent Virtual Channel (PVCs) established to provide a simple point-to-point connection between two devices through an ATM network. The link does *not* require those elements (LAN Emulation Server, LAN Emulation Configuration Server, and Broadcast and Unknown Server, for example) otherwise necessary to establish an emulated LAN.

What Type of Tunnel to Configure

You can configure either an Ethernet ATM Bridge Tunnel or an FDDI ATM Bridge Tunnel on each ATM logical interface. The type of bridge tunnel (Ethernet or FDDI) you establish should be that which minimizes the number of points at which Ethernet-to-FDDI translation is required. Table 5-4 provides general guidelines for determining what type of tunnel to configure.

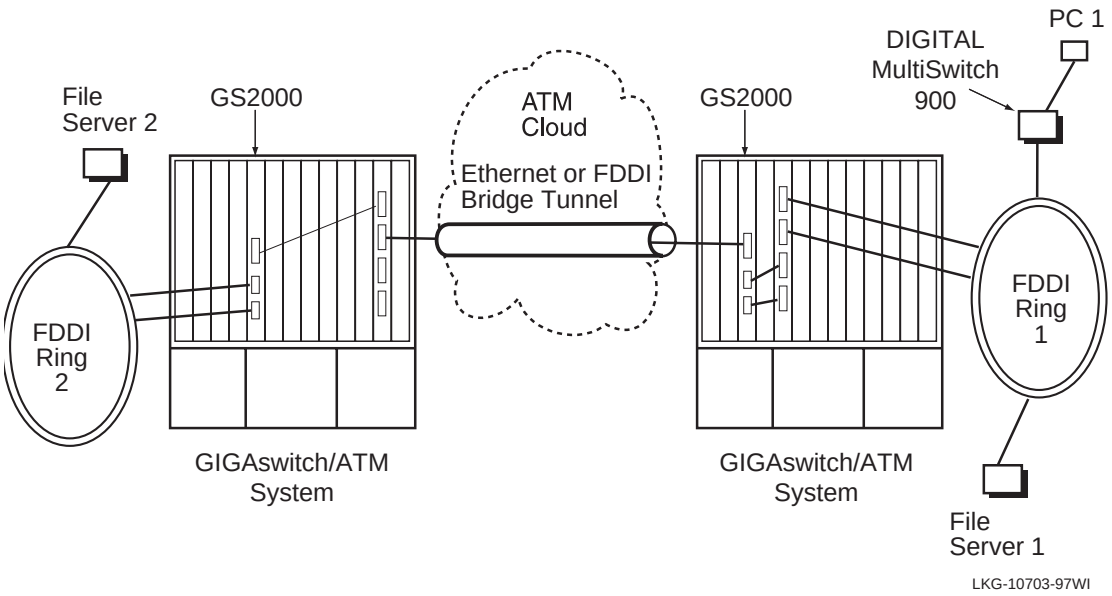
Table 5-4: Guidelines for Determining Bridge Tunnel Type

If. . .	Then. . .
The source and destination devices on either side of an ATM cloud are both on Ethernet LANs	The tunnel should be an Ethernet ATM Bridge Tunnel.
Either the source or destination device is on an FDDI ring, and the other device is on an Ethernet LAN	The tunnel should be an FDDI ATM Bridge Tunnel.
The source and destination devices on either side of an ATM cloud are both on an FDDI ring	The tunnel should be an FDDI ATM Bridge Tunnel.

Using Figure 5-3 as an example, if PC 1 on Ethernet LAN 1 typically requires access to PC 2 on Ethernet LAN 2, the ATM interfaces on GIGAswitch GS2000 modules that connect to the ATM cloud should be configured for an Ethernet ATM Bridge Tunnel.

Again using Figure 5-3 as an example, assume that PC 1 on Ethernet LAN 1 typically requires access to the Corporate Database on FDDI ring 2. In this situation, the ATM interfaces should be configured for an FDDI ATM Bridge Tunnel.

Figure 5-3: ATM Bridge Tunnels



How to Configure an ATM Bridge Tunnel

This section describes how to configure an ATM Bridge Tunnel on the GIGAswitch GS2000 module's ATM interface. Configuring an ATM Bridge Tunnel involves assigning a Virtual Channel Identifier to the Permanent Virtual Channel, and setting the Bridge Tunnel's MAC type.

You must also configure the device on the opposite end of the bridge tunnel. This can be, for example, a VNswitch 900EA, a DIGITAL GIGAswitch/ATM, or another vendor's ATM switch. Refer to the appropriate documentation provided by the manufacturer of that device for configuration instructions.

Each ATM logical interface is automatically set up as either a LAN emulation client (LEC), or a Bridge Tunnel at installation. Refer to Table 5-3 for information about the types of ATM logical interface established at installation, and the conditions under which each is active. If the connection is a LEC, you can change the connection to a Bridge Tunnel.

To change the GIGAswitch GS2000 module's ATM interface from a LEC to an ATM Bridge Tunnel, perform the following steps:

Step	Action
1	At the `ATM/n Config>` prompt, enter **change_interface bridge tunnel**.

2	Press Return. The following message is displayed:
	`Current interface type is LEC.`
	`This command will change interface type to Bridge Tunnel.`
	`Proceed? (Yes/[No]):`

3	Enter **y** if you want to change the LEC to a Bridge Tunnel. Enter **n** if you do not want to change the LEC to a Bridge Tunnel.

4	Press Return. If you entered **y**, the following message is displayed:
	`VPI = 0 in this release`
	`VCI(62-1022):`
	VPI is the Virtual Path Identifier assigned to the Permanent Virtual Channel. The VPI is automatically set at 0. VCI is the Virtual Channel Identifier assigned to the PVC.
	If you entered **n**, the `ATM/n Config>` prompt is displayed.

5	Enter a number from 62 through 1022. This number is the VCI you want to assign to the virtual channel.
6	Press Return. The ATM Bridge Tunnel you specified is configured and the `ATM BT Config>` prompt is displayed. The Bridge Tunnel is assigned a MAC type of Ethernet, by default. Refer to the Modifying the VCI and MAC Type section for information about how to change the MAC type.

Modifying the VCI and MAC Type

You can change the VCI you configured when you first established the Bridge Tunnel. You can also change the MAC type to either an Ethernet ATM Bridge Tunnel or an FDDI ATM Bridge Tunnel. Refer to the What Type of Tunnel to Configure section for information about how to determine the type of Bridge Tunnel you should establish.

To modify the Bridge Tunnel's VCI or MAC type, perform the following steps:

Step	Action
1	At the `ATM/n Config>` prompt, enter **change_interface bridge tunnel**.
2	Press Return. The `ATM BT Config>` prompt is displayed.
3	Enter **set**.

4	Press Return. A message similar to the following is displayed:
	`Configuring ATM bridge tunnel for interface 15`
	`VPI = 0 in this release`
	`VCI(62-1022):`
	VPI is the Virtual Path Identifier assigned to the Permanent Virtual Channel. The VPI is automatically set at 0. VCI is the Virtual Channel Identifier assigned to the PVC.

5	If you want to change the VCI assigned to the PVC, enter a new VCI number from 62 through 1022. If you do not want to change the VCI, reenter the VCI number currently assigned to the PVC.
6	Press Return. The following message is displayed: `MAC Type(Fddi Or Ethernet):`
7	Enter **e** if you want to establish an Ethernet Bridge Tunnel. Enter **f** if you want to establish an FDDI Bridge Tunnel.
8	Press Return. The VCI and MAC type are set as specified, and the `ATM BT Config>` prompt is displayed.

Displaying Current Bridge Tunnel Settings

To display configuration information about the Bridge Tunnel, perform the following steps:

Step	Action
1	At the `ATM/n Config>` prompt, enter **change_interface bridge tunnel**.
2	Press Return. The `ATM BT Config>` prompt is displayed.
3	Enter **list**.
4	Press Return. The report and the `ATM BT Config>` prompt are displayed.

Example

```
ATM/17 Config>list

Network Interface number : 17
Port Type                : Bridge Tunnel
PVC (VPI,VCI)            : 0,68
Mac Type                 : Ethernet
LAN FCS                  : No
Quality of Service       : 3
```

Configuring a LAN Emulation Client Interface

This section describes how to configure an ATM interface serving as a LAN Emulation Client (LEC) on an Emulated LAN (ELAN). You must also configure the ATM device on the opposite end of the ELAN. This second device can be, for example, a VNswitch 900EA, another vendor's ATM switch, and servers or workstations directly attached to the ATM network. Refer to the appropriate documentation provided by the manufacturer of that device for configuration instructions.

You can perform the following tasks when configuring the ATM logical interface as an LEC:

- Assign an ELAN name to the logical interface.
- Set the LEC to identify the LES address automatically or manually.
- Set address resolution parameters.
- Set data frame control parameters.
- Set control frame and Data VCC Timeouts.

- Display current ATM logical interface configuration parameters.

Caution

It is recommended that the only tasks you perform when configuring a logical interface as a LEC are assigning an ELAN to the interface, identifying the LES address, and displaying current configuration settings. It is recommended that you perform other configuration tasks, such as setting maximum frame size or forward delay time, *only* if you fully understand the effect the change will have on the entire network.

Assigning an ELAN Name to the Interface

You can identify the ELAN you want the LEC to join by specifying the name of the ELAN. Typically, the list of valid ELAN names is created by the network administrator on the LECS. If you do not identify the ELAN the interface is to join, the LECS directs the connection to a default ELAN compatible with the requirements of the interface.

To identify the ELAN with which you want the LEC's logical interface to join, perform the following steps:

Step	Action
1	At the `ATM/n Config>` prompt, enter **change lec**.
2	Press Return. The `ATM LEC Config>` prompt is displayed.
3	Enter **elan**.

4	Press Return. The following message is displayed:
	`current elanname :oldname`
	`new elanname :`
	If the ELAN is already assigned a name, the current name is displayed. If the ELAN is not yet assigned a name, the current name field is blank.

5	Enter the (new) name of the ELAN with which you want the interface to establish a connection.
6	Press Return. The specified name is set and the `ATM LEC Config>` prompt is displayed.

Identifying the LES Address

The LECS is, in part, responsible for maintaining identification and location records of ELANs that are members of an ATM network. Typically, more than one LES is configured in an ATM network, and each is responsible for the identification and location of a subset of ELANs on the network. A LEC, attempting to join a particular ELAN, must first determine the address of the LES responsible for the ELAN the LEC is attempting to join.

Identifying which LES is responsible for a target ELAN can be accomplished either automatically or manually. Automatic identification is managed by the LECS based on "look-up" tables previously configured by the network administrator. Automatic identification is the default operational mode. You can choose, however, to disable automatic identification, and to identify the LES manually by specifying the LES ATM address as an LEC configuration parameter. If you choose to provide the LES address manually, the LEC begins the connection process at the Join phase.

Note

Identifying LES addresses is most easily managed on the LAN Emulation Configuration Server. Managing the address tables centrally on the LECS is easier than changing the LES address on each GIGAswitch GS2000 module, especially when the physical configuration of a large network changes.

LEC Connection Phases

This section provides a general description of the process any LEC (including the GIGAswitch GS2000 module) must complete to establish a connection to an ELAN. The process is divided into the five phases described in Table 5-5. Refer to The ATM Forum Technical Committee's *LAN Emulation Over ATM* specification for a detailed discussion about ATM LEC functional parameters.

Table 5-5: ELAN Connection Phases

Phase	Description
LECS Connect	The LEC establishes a connection with the LECS.
Configuration	The LEC obtains the ATM address of a LES. The LEC may also obtain other configuration parameters.
Join	The LEC establishes its connection(s) with the LES, and determines the operating parameters of the ELAN.
Initial Registration	The LEC *may* attempt to register additional LAN destinations according to the registration protocol, through which the LEC identifies the LAN destinations it requires for normal operation.
BUS Connect	The LEC establishes a connection with the BUS.

Automatic Identification of the LES Address

Automatic identification of the LES ATM address occurs during the Configuration phase, described in Table 5-5. During the LECS Connect phase, the GIGAswitch GS2000 module establishes a Configuration Direct Virtual Channel Connection (VCC) with the LECS. This is the connection over which the module requests the LECS to identify the address of the LESs responsible for the target ELANs. The LEC sends a configuration request and the LECS responds with the LES address and other configuration parameters.

Automatic identification of the LES address is the default setting for the GIGAswitch GS2000 module. If, however, you previously configured the module for manual mode and you now want to reset the module to automatic mode, perform the following steps:

Step	Action
1	At the `ATM/n Config>` prompt, enter **change lec**.
2	Press Return. The `ATM LEC Config>` prompt is displayed.
3	Enter **set**.
4	Press Return. The ATM Set prompt (`ATM Set LEC Record>`) is displayed.

Step	Action
5	Enter **config_mode**.
6	Press Return. The following message is displayed: `Config Mode(automatic(default) or manual):`
7	Enter **automatic**.
8	Press Return. The module is set to identify the LES address automatically through the LECS, and the `ATM Set LEC Record>` prompt is displayed.

Manual Identification of the LES Address

You can configure the module so that you provide the address of the LES responsible for the target ELAN. The GIGAswitch GS2000 module uses this address during the Join phase (Table 5-5) to establish a Control Direct Virtual Channel Connection (VCC) with the LES. This is the connection over which the module determines the operating parameters of the ELAN.

To identify the LES address manually, perform the following steps:

Step	Action
1	At the `ATM/`*`n`* `Config>` prompt, enter **change lec**.
2	Press Return. The `ATM LEC Config>` prompt is displayed.
3	Enter **set**.
4	Press Return. The ATM Set prompt (`ATM Set LEC Record>`) is displayed.
5	Enter **config_mode**.
6	Press Return. The following message is displayed: `Config Mode(automatic(default) or manual):`
7	Enter **manual**.
8	Press Return. The ATM Set prompt (`ATM Set LEC Record>`) is displayed.
9	Enter **les_atm_addr**.
10	Press Return. An address format template and the following message are displayed: `Les Atm address:`

Step	Action
11	Enter the ATM address of the LES responsible for the ELAN to which the interface is to connect. The ATM address is a 40-character alphanumeric string divided into three segments by periods (.). The first segment is a 26-character prefix. The second is the End Station Identifier (ESI) that is equivalent to the MAC address. The third segment is a 2 character selector byte. **Example:** 3999990000000008002bb5f380.0000f84de70e.00 The address must be entered using the hexadecimal value, according to the format indicated by the address format template. Each two-digit hexadecimal value must be separated by a space. The periods (.) shown in the above example must not be entered. **Example:** 39 99 99 00 00 00 00 08 00 2b b5 f3 80 00 00 f8 4d e7 0e 00
12	Press Return. The module is configured to access the LES identified by the specified address, and the `ATM Set LEC Record>` prompt is displayed.

Setting Address Resolution Parameters

Address resolution is the process by which a LEC associates the MAC address of a LAN destination with the ATM address of another LEC, or the BUS. This process is managed by the LAN Emulation Address Resolution Protocol (LE_ARP), which generates LE_ARP Requests for address information.

You can configure the following parameters that are related to address resolution:

- Expected ARP Response Time
- LE_ARP Request Retries
- Aging the LE_ARP cache

Setting the Expected ARP Response Time

ARP response time is the maximum amount of time a transmitting LEC expects an LE_ARP response to occur after an LE_ARP request is sent. If the length of time it takes for the transmitting LEC to receive a response equals or exceeds the expected time, the LEC initiates a retry.

To set the Expected ARP Response Time, perform the following steps:

Step	Action
1	At the `ATM/`*`n`* `Config>` prompt, enter **change lec**.
2	Press Return. The `ATM LEC Config>` prompt is displayed.

Step	Action
3	Enter **set**.
4	Press Return. The ATM Set prompt (`ATM Set LEC Record>`) is displayed.
5	Enter **arp_response_time**.
6	Press Return. The following message is displayed: `Arp Response Time #seconds(default = 1):`
7	Enter the number of seconds within which the transmitting LEC expects to receive an LE_ARP response after it sends an LE_ARP request. The range of acceptable values for this parameter is 1 to 30 seconds. The default is 1 second.
8	Press Return. The Expected ARP Response time is set and the `ATM Set LEC Record>` prompt is displayed.

Setting the Number of LE_ARP Request Retries

If a GIGAswitch GS2000 module's LEC interface sends an LE_ARP Request, and a response is not received within the Expected ARP Response Time, the LEC resends the unanswered LE_ARP Request, up to a specified number of retries. You can set the number of times the interface attempts to resend the LE_ARP Request by performing the following steps:

Step	Action
1	At the `ATM/`*`n`* `Config>` prompt, enter **change lec**.
2	Press Return. The `ATM LEC Config>` prompt is displayed.
3	Enter **set**.
4	Press Return. The ATM Set prompt (`ATM Set LEC Record>`) is displayed.
5	Enter **max_retry_count**.
6	Press Return. The following message is displayed: `Max Retry Count #(default = 1):`
7	Enter the number of seconds within which the transmitting LEC expects to receive an LE_ARP response after it sends an LE_ARP request. The range of acceptable values is 0 (zero) to 2. The default is 1.

Step	Action
8	Press Return. The Retry Count is set and the `ATM Set LEC Record>` prompt is displayed.

Aging the LE_ARP Cache

LEC clients each maintain a table of entries that establishes a relationship between destination MAC addresses and the ATM address to which data frames for the MAC address is sent. Each entry in the table is based on address information included in LE_ARP Responses.

When the LEC receives a frame for transmission, and the destination MAC address is resident in the LE_ARP cache, the client can forward the frame based on the ATM address mapping in the table. This eliminates the need to repeatedly generate an LE_ARP request to determine the destination address. However, the MAC address may move due to a cabling change or a change in the spanning tree by a downstream bridge. This results in invalid mapping of MAC addresses to ATM addresses. To accommodate such changes, entries in the LE_ARP cache are maintained for a limited period of time, thereby forcing generation of new LE_ARP Requests and verification of MAC address-to-ATM address mappings.

Each entry in the cache is retained for a period of time equal to either the Aging Time or Forward Delay Time. Aging time is used to age entries in the cache under normal operation. Forward delay is used to age entries in the LE_ARP cache when a topology change is in progress. Refer to The ATM Forum Technical Committee's *LAN Emulation Over ATM* specification for a detailed discussion about the conditions under which the Aging Time and Forward Delay Time are used.

To set Aging Time for entries in the LE_ARP cache, perform the following steps:

Step	Action
1	At the `ATM/`*`n`* `Config>` prompt, enter **change lec**.
2	Press Return. The `ATM LEC Config>` prompt is displayed.
3	Enter **set**.
4	Press Return. The ATM Set prompt (`ATM Set LEC Record>`) is displayed.
5	Enter **aging_time**.
6	Press Return. The following message is displayed: `Aging Time #seconds(default = 300):`

Step	Action
7	Enter the number of seconds each entry in the LE_ARP cache is retained. The range of acceptable values is 10 to 300 seconds. The default is 300 seconds.
8	Press Return. The Aging Time is set and the `ATM Set LEC Record>` prompt is displayed.

To set Forward Delay Time for entries in the LE_ARP cache, perform the following steps:

Step	Action
1	At the `ATM/n Config>` prompt, enter **change lec**.
2	Press Return. The `ATM LEC Config>` prompt is displayed.
3	Enter **set**.
4	Press Return. The ATM Set prompt (`ATM Set LEC Record>`) is displayed.
5	Enter **forward_delay_time**.
6	Press Return. The following message is displayed: `Forward Delay Time #seconds(default = 15):`
7	Enter the number of seconds each entry in the LE_ARP cache is retained. The range of acceptable values is 4 to 30 seconds. The default is 15 seconds.
8	Press Return. The Forward Delay Time is set and the `ATM Set LEC Record>` prompt is displayed.

Setting the Maximum Unknown Frame Count

The Broadcast and Unknown Server (BUS) manages all broadcast and multicast traffic, and all initial unicast data associated with a MAC address that is unknown by the LEC. An unknown frame is a unicast frame with an unknown destination MAC address. You can set the maximum number of unknown frames that a LEC can send to the BUS within a given period of time.

Setting the Maximum Number of Unknown Frames

To set the maximum number of unknown frames sent to the BUS, perform the following steps:

Step	Action
1	At the `ATM/n Config>` prompt, enter **change lec**.
2	Press Return. The `ATM LEC Config>` prompt is displayed.
3	Enter **set**.
4	Press Return. The ATM Set prompt (`ATM Set LEC Record>`) is displayed.
5	Enter **max_unknown_frames_count**.
6	Press Return. The following message is displayed: `Maximum Unknown Frames Count #(default = 1):`
7	Enter the maximum number of frames sent within the time specified in the Setting Unknown Frame Time section. The range of acceptable values is 1 to 10 frames. The default is 1 frame.
8	Press Return. The Maximum Unknown Frame Count is configured as specified, and the `ATM Set LEC Record>` prompt is displayed.

Setting Unknown Frame Time

To set the time period within which the maximum number of unknown frames is not to be exceeded, perform the following steps:

Step	Action
1	At the `ATM/n Config>` prompt, enter **change lec**.
2	Press Return. The `ATM LEC Config>` prompt is displayed.
3	Enter **set**.
4	Press Return. The ATM Set prompt (`ATM Set LEC Record>`) is displayed.
5	Enter **max_unknown_frames_time**.
6	Press Return. The following message is displayed: `Max Unknown Frame Time #seconds(default = 1):`

Step	Action
7	Enter the maximum number of seconds within which the maximum number of unknown frames is not to be exceeded. The range of acceptable values is 1 to 60 seconds. The default is 1 second.
8	Press Return. The Unknown Frame Time is configured as specified, and the `ATM Set LEC Record>` prompt is displayed.

Setting Control Frame and Data VCC Timeouts

You can set the maximum amount of time a LEC waits for a response after sending a request. If this value is exceeded, the LEC issues another request.

You can also set the maximum amount of time a Data Direct VCC is allowed to be inactive (no data frame traffic is transmitted or received). If the Data Direct VCC timeout value is exceeded, the GIGAswitch GS2000 module's LEC interface releases the VCC.

Setting the Control Frame Timeout

To set the Control Frame Timeout, perform the following steps:

Step	Action
1	At the `ATM/`*`n`* `Config>` prompt, enter **change lec**.
2	Press Return. The `ATM LEC Config>` prompt is displayed.
3	Enter **set**.
4	Press Return. The ATM Set prompt (`ATM Set LEC Record>`) is displayed.
5	Enter **control_timeout**.
6	Press Return. The following message is displayed: `Control timeout #seconds(default=120):`
7	Enter the maximum number of seconds request and response control frame interactions are to occur. The range of acceptable values is 10 to 300 seconds. The default is 120 seconds.
8	Press Return. The Control Timeout value is configured as specified, and the `ATM Set LEC Record>` prompt is displayed.

Setting the VCC Timeout Value

To set the VCC Timeout, perform the following steps:

Step	Action
1	At the `ATM/n Config>` prompt, enter **change lec**.
2	Press Return. The `ATM LEC Config>` prompt is displayed.
3	Enter **set**.
4	Press Return. The ATM Set prompt (`ATM Set LEC Record>`) is displayed.
5	Enter **vcc_timeout**.
6	Press Return. The following message is displayed: `Vcc Timeout Period #minutes(default = 20):`
7	Enter the amount of time after which an inactive Data Direct SVC should be closed. The default is 20 minutes.
8	Press Return. The VCC Timeout value is configured as specified, and the `ATM Set LEC Record>` prompt is displayed.

Setting the Maximum Frame Size

The Maximum Frame Size specifies the maximum data frame size the LEC can send on a Multicast Send VCC, or receive on the Multicast Send VCC or the Multicast Forward VCC. This parameter also specifies the maximum frame size for all LEC Data Direct VCCs.

ELAN services require that the maximum frame size is the same for all LECs belonging to a specific ELAN. All LECs that are members of an ELAN participate in a negotiation process to determine the maximum frame size used on the ELAN. The value set on the LEC should not exceed the Maximum Frame Size set on the LES. You can set the Maximum Frame Size to either 1516 octets, or 4544 octets. The default GIGAswitch GS2000 module's LEC Maximum Frame Size is 1516 octets. The value you enter is the size requested in the configuration message. The actual value used may be smaller, depending on the results of the negotiation process.

To set the Maximum Frame Size, perform the following steps:

Step	Action
1	At the `ATM/n Config>` prompt, enter **change lec**.
2	Press Return. The `ATM LEC Config>` prompt is displayed.
3	Enter **set**.
4	Press Return. The ATM Set prompt (`ATM Set LEC Record>`) is displayed.
5	Enter **max_frame_size**.
6	Press Return. The following message is displayed: `Max Frame size #(1516(default) or 4544):`
7	Enter the maximum frame size you want to set. The values you can enter are 1516 or 4544. The default is 1516 octets.

8	Press Return. If you are changing the frame size to a greater value than was previously set, the following message and the `ATM Set LEC Record>` prompt are displayed:
	`Warning: New frame size is larger than current size.`
	`Restart VNswitch to use new size.`
	If are changing the frame size to a smaller value than was previously set, the Maximum Frame Size is configured as specified, and the `ATM Set LEC Record>` prompt is displayed.

9	If you are changing the frame size to a greater value than was previously set, restart the module according to the instructions provided in Chapter 10.

Setting the Flush Timeout

LECs can transmit unicast frames to the same destination LAN address through either the BUS or a data direct VCC at different times. To avoid the possibility that frames are sent out of order, because of the dual paths, a procedure known as the Flush Message Protocol is used. The flush protocol requires that the LEC transmit an LE_Flush_Request on the previously used path, before switching to the second path. An LE_Flush_Response must be returned to the sender by the destination client. When the LEC that originated the flush request receives the response, the old path is clear of data and the originating LEC begins using the new path.

You can set the maximum amount of time that the LEC waits to receive an LE_Flush_Response after it sends a request. If this period of time is exceeded, the originating LEC begins using the new path. To set the Flush Timeout value, perform the following steps:

Step	Action
1	At the `ATM/n Config>` prompt, enter **change lec**.
2	Press Return. The `ATM LEC Config>` prompt is displayed.
3	Enter **set**.
4	Press Return. The ATM Set prompt (`ATM Set LEC Record>`) is displayed.
5	Enter **flush_timeout**.
6	Press Return. The following message is displayed: `Flush Timeout #seconds(default = 4):`
7	Enter the maximum number of seconds the LEC waits to receive an LE_Flush_Response after it sends a request. The range of acceptable values is 1 to 4 seconds. The default is 4 seconds.
8	Press Return. The Flush Timeout value is configured as specified, and the `ATM Set LEC Record>` prompt is displayed.

Setting Path Switching Delay

You can set the period of time after which a LEC assumes a data frame it transmits is either delivered to its destination, or discarded. Flush Timeout is ignored if the Path Switching Delay value is lower than the Flush Timeout.

To set the Path Switching Delay, perform the following steps:

Step	Action
1	At the `ATM/n Config>` prompt, enter **change lec**.
2	Press Return. The `ATM LEC Config>` prompt is displayed.
3	Enter **set**.
4	Press Return. The ATM Set prompt (`ATM Set LEC Record>`) is displayed.
5	Enter **path_switching_delay**.

Step	Action
6	Press Return. The following message is displayed: `Path Switch Delay #seconds(default = 6):`
7	Enter the number of seconds after which an LEC assumes a data frame it transmits is either delivered to its destination, or discarded. The range of acceptable values is 1 to 8 seconds. The default is 6 seconds.
8	Press Return. The Path Switching Delay value is configured as specified, and the `ATM Set LEC Record>` prompt is displayed.

Displaying Current ATM LEC Configuration Parameters

You can display specific information about various ATM LEC configuration settings. To display configuration information, perform the following steps:

Step	Action
1	At the `ATM/n Config>` prompt, enter **change lec**.
2	Press Return. The `ATM LEC Config>` prompt is displayed.
1	Enter **list *command***, where ***command*** is the command you must enter to display the desired information. Refer to Table 5-6 for a list of commands, and for a description of the type of information that is displayed when you enter the command.
2	Press Return. The desired information and a new `ATM LEC Config>` prompt is displayed.

Example

```
ATM LEC Config>list all

Interface                       : 2 (Bridge Port 2)
Config Mode                     : Auto
Mac Type                        : Ethernet
Max Frame size                  : 1516
ELan Name                       :
Control timeout(seconds)        : 120
Max Unknown Frames Count        : 1
Max Unknown Frame Time(seconds) : 1
Vcc Timeout Period(seconds)     : 1200
Max Retry Count                 : 1
Aging Time(seconds)             : 300
Forward Delay Time(seconds)     : 15
Arp Response Time(seconds)      : 1
Flush Timeout(seconds)          : 4
Path Switch Delay(seconds)      : 6
Lec Mac Address                 : 00-00-F8-4E-56-0E
Les Atm address:
          39999900000000000F84EEE80.0000F84EEE91.00
```

Table 5-6: List Command Options and Descriptions for ATM Logical Configurations

Command	Description
config_mode	Lists whether identification of the LES address is set to automatic or manual mode.
mac_type	Lists the frame type used by the ATM LEC. The frame type is always Ethernet.
max_frame_size	Displays the maximum frame size requested for the LEC on this interface.
elan_name	Lists the name of the ELAN with which the LEC is associated.
control_timeout	Displays the timeout value of LECS and LES requests.
max_unknown_frames_count	Displays the maximum number of unknown frames that an LEC can send to the BUS within the time period specified by the unknown-frame-time-max parameter.
max_unknown_frames_time	Displays the time period within which the maximum number of unknown frames is not to be exceeded.
vcc_timeout	Lists the maximum amount of time a Data Direct VCC is inactive (no data frame traffic is transmitted or received) before the VCC is released.
max_retry_count	Displays the number of times the LEC attempts to resend an LE_ARP Request when the Expected LE_ARP Response Time is exceeded.
aging-time	Lists the aging time value used to limit the amount of time entries in the LE_ARP cache are retained.
forward_delay_time	Lists the forward delay value used to limit the amount of time entries in the LE_ARP cache are retained.
arp_response_time	Displays the maximum amount of time, in seconds, a LEC waits before retrying a LE_ARP Request.

Command	Description
flush_timeout	Displays the maximum amount of time that the LEC waits to receive an LE_Flush_Response before starting to use the new channel.
path_switching_delay	Displays the period of time after which an LEC assumes a data frame it transmits is either delivered to its destination, or discarded. Flush Timeout is ignored if the Path Switching Delay value is lower than the Flush Timeout.
lec_mac_addr	Displays the local unicast MAC addresses assigned to the LEC interface.
les_atm_addr	Lists whether identification of the LES address is set to automatic mode or manual mode. Automatic identification is managed by the LECS based on “look-up” tables previously configured by the network administrator. Manual mode enables you to specify the LES ATM address as an LEC configuration parameter.
all	Displays information associated with all of the above commands.

Configuring the Address Resolution Protocol

When a network device sends an IP packet, the transmitting device must first determine the MAC address associated with the IP address in the packet. The Address Resolution Protocol (ARP) is responsible for determining the MAC-to-IP address mapping. ARP does so by broadcasting an ARP Request that includes the IP address of the destination. The destination node then responds to the request by providing its MAC address to the original node that requested the information. The original node retains the mapped addresses in an ARP cache for later use. This MAC-to-IP address learning process is typically handled automatically by ARP. Under certain conditions, however, you may need to map an IP address to its associated MAC address manually. You may need to do so, for example, if ARP is not running on the destination node.

You can perform the following tasks when configuring ARP:

- Add and change ARP cache entries manually.
- Delete a manually entered ARP entry.
- Manage the time that learned entries are retained.
- Display information about the current configuration.

Adding and Changing ARP Cache Entries Manually

On a GIGAswitch GS2000 module, manually entered ARP cache entries are configured on a per interface basis. A separate ARP cache is, therefore, retained for each interface. You cannot change a learned entry.

To manually map an IP address to a MAC address for an interface, or to change an existing manual entry, perform the following steps:

Step	Action
1	At the Config prompt, enter **arp**. **Example:** `Config>`**arp**
2	Press Return. The ARP configuration prompt (`ARP config>`) is displayed.
3	If you want to add a new ARP entry, enter **add entry**. If you want to change an existing ARP entry, enter **change entry**.
4	Press Return. The following message is displayed: `Interface Number [0]?`

Step	Action
5	Enter the number of the logical interface for which you want to create or change an IP-to-MAC address entry.
6	Press Return. The following message is displayed: `IP Address [0.0.0.0]?`
7	Enter the IP address of the device for which you want to create or change an entry.
8	Press Return. The following message is displayed: `Mac Address []?`
9	Enter the MAC address of the device for which you want to create or change an entry. The address must be entered using the format 08002bAABBCC. Hyphens (-) and colons (:) are not allowed.
10	Press Return. The IP-to-MAC address entry is created or modified as specified, and the `ARP config>` prompt is displayed.
11	Restart the module if you want the new configuration settings to take effect.

Deleting a Manually Entered ARP Entry

You can delete ARP cache entries that were previously entered manually. You cannot delete learned entries. Learned entries are automatically aged out of the cache.

To delete an existing IP-to-MAC address ARP entry that was previously added manually, perform the following steps:

Step	Action
1	At the Config prompt, enter **arp**. **Example:** `Config>`**arp**
2	Press Return. The ARP configuration prompt (`ARP config>`) is displayed.
3	Enter **delete entry**.
4	Press Return. The following message is displayed: `Interface Number [0]?`
5	Enter the number of the logical interface for which you want to delete an IP-to-MAC address entry.

Step	Action
6	Press Return. The following message is displayed: `IP Address [0.0.0.0]?`
7	Enter the IP address of the device for which you want to delete an IP-to-MAC address entry.
8	Press Return. The IP-to-MAC address entry is deleted, and the ARP `config>` prompt is displayed.
9	Restart the module if you want the new configuration settings to take effect.

Managing the Time That Learned Entries Are Retained

As long as an IP-to-MAC address entry is in the ARP cache, the module can transmit data directly to their associated device without rebroadcasting ARP requests. This helps maintain network performance by reducing the need to repeatedly broadcast ARP requests for active communication between two devices.

The module retains learned ARP cache entries for a set period of time managed by a Refresh Timer and an Auto-Refresh function. The Refresh Timer specifies the amount of time a learned entry is retained before the module attempts to reverify the presence of the device. The verification process is referred to as Auto-Refresh. Auto-Refresh is the process that attempts to verify that the device associated with a learned ARP entry still exists. The Refresh Timer and Auto-Refresh function do not affect ARP cache entries that are entered manually.

Setting the Refresh Timer

The Refresh Timer specifies the amount of time a learned entry is retained before the module attempts to verify the presence of the device. The default is 20 minutes. If the entry is no longer valid, the entry is deleted from the cache and the module must relearn the mapping the next time it attempts to transmit data to the same IP address. If, before the Refresh Time expires, the module detects verification of an entry through an ARP Request sent by another device, the entry is retained and the Refresh Timer is restarted. Similarly, if the Refresh Time is about to expire, the module attempts to verify the entry by sending its own ARP Request. If the entry is still valid, the entry is retained and the Refresh Timer is restarted.

You can change the Refresh Time to affect the length of time each learned entry in the cache is retained. To set the Refresh Timer, perform the following steps:

Step	Action
1	At the Config prompt, enter **arp**. **Example:** `Config>`**arp**
2	Press Return. The ARP configuration prompt (`ARP config>`) is displayed.
3	Enter **set refresh-timer**.
4	Press Return. The following message is displayed: `timeout (in minutes) [20]?` The factory default is 20 minutes. If the factory default was modified, the default is the most recent setting.
5	Enter the number of minutes after which you want ARP to attempt to verify the ARP entry is still valid. The number must be a whole number in the range of **1** to **65535** minutes. A value of zero (0) disables the refresh timer.
6	Press Return. The Refresh Timer is set as specified, and the `ARP config>` prompt is displayed.
7	Restart the module if you want the new configuration settings to take effect.

Enabling and Disabling Auto-Refresh

Auto-Refresh is the process that attempts to verify that a device still exists when its learned entry in the ARP cache exceeds the Refresh Timer. You can enable and disable Auto-Refresh. When enabled, Auto-Refresh initiates verification shortly before the Refresh Time is exceeded. When disabled, the verification process does not occur and the learned ARP entry is deleted if no active communication is otherwise initiated between the devices before the Refresh Time is exceeded. The factory default is disabled. If the factory default was modified, the default is the most recent setting.

To enable or disable Auto-Refresh, perform the following steps:

Step	Action
1	At the Config prompt, enter **arp**. **Example:** `Config>arp`
2	Press Return. The ARP configuration prompt (`ARP config>`) is displayed.
3	If you want to disable Auto-Refresh, enter **disable auto-refresh**. If you want to enable Auto-Refresh, enter **enable auto-refresh**.
4	Press Return. Auto-Refresh is disabled or enabled as specified.
5	Restart the module if you want the new configuration settings to take effect.

Displaying Information About the Current Configuration

To display information about the current ARP configuration, perform the following steps:

Step	Action
1	At the Config prompt, enter **arp**. **Example:** `Config>arp`
2	Press Return. The ARP configuration prompt (`ARP config>`) is displayed.
3	Enter **list** ***option***, where ***option*** is the command you must enter to display the desired information. Refer to Table 5-7 for a list of commands and for a description of the information that is displayed when you enter the command.
4	Press Return. The desired information and a new `ARP config>` prompt is displayed.

Example

```
ARP config>list all

ARP configuration:
Refresh timeout: 8 minutes
Auto refresh: enabled
Mac address translation configuration
Ifc #   Prot #  Protocol -> Mac address
 1       0      16.20.48.79 -> 112233445566
 1       0      16.20.48.68 -> 112233445566
 2       0      16.20.48.89 -> 223344556677
```

Table 5-7: List Command Options and Descriptions for ARP Configurations

Command	Description
entry	The following information is listed for each ARP cache entry added manually: • The number of the interface with which the entry is associated • The IP address and MAC address for the entry
config	The following information is listed about the length or time ARP is configured to retain entries added manually: • The Refresh Timer value in minutes • Whether Auto-Refresh is enabled or disabled
all	All the information described for both the **entry** and **config** options are displayed.

Chapter 6

Monitoring Network Interfaces

Overview

Introduction

This chapter provides information about how to monitor a DIGITAL GIGAswitch GS2000 line card (GS2000) module's FDDI and ATM network interfaces.

In This Chapter

The following topics are covered in this chapter:

Displaying the Interface Number and Type

You can display the number assigned to a logical interface and the interface type (FDDI or ATM).

To list a GIGAswitch GS2000 module's logical interface numbers and types, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **list all**.
2	Press Return. A report that includes general information about the module is displayed, including the number associated with each type of interface.

Example

The following is an example of the information displayed for an FDDI module. The report is divided into three sections. The first section includes module identification information and the console baud rate. The interface number is displayed in the third section of the report. The first two sections include general information about the module and supported protocols. Refer to Table 6-1 for a description of the third section of the report that includes the interface number.

```
Monitor>list all

GIGAswitch GS2000, 1 ATM 1 FDDI,HW=04f1E1,RO=V1.5.5,#1083,SW=V2.0
Hostname: [not configured]
Console baud rate: 0

Num Name    Protocol
 3  ARP     Address Resolution
11  SNMP    Simple Network Management Protocol
23  BRIDGE  Adaptive Source Routing Transparent Enhanced Bridge
24  HST     TCP/IP Host Services

Num Name    Feature
 5  RMON    Remote Monitoring

18 Interfaces:
Ifc Name       MAC/Data-Link         Hardware                      State
 0  Vnbus/0    VNbus-encapsulation   VNbus                         Not present
 1  FDDI/1     FDDI/IEEE 802.2       FDDI                          Up
 2  ALEC/2     ATM LAN Emulation C   ATM                           Testing
 3  ALEC/3     ATM LAN Emulation C   ATM                           Testing
 4  ALEC/4     ATM LAN Emulation C   ATM                           Testing
 5  ALEC/5     ATM LAN Emulation C   ATM                           Testing
 6  ALEC/6     ATM LAN Emulation C   ATM                           Testing
 7  ALEC/7     ATM LAN Emulation C   ATM                           Testing
 8  ALEC/8     ATM LAN Emulation C   ATM                           Testing
 9  ALEC/9     ATM LAN Emulation C   ATM                           Testing
10  ALEC/10    ATM LAN Emulation C   ATM                           Testing
11  ALEC/11    ATM LAN Emulation C   ATM                           Testing
12  ALEC/12    ATM LAN Emulation C   ATM                           Testing
13  ALEC/13    ATM LAN Emulation C   ATM                           Testing
14  ALEC/14    ATM LAN Emulation C   ATM                           Testing
15  ALEC/15    ATM LAN Emulation C   ATM                           Testing
16  AFBT/16    ATM F Bridge Tunnel   ATM                           Testing
17  AEBT/17    ATM E Bridge Tunnel   ATM                           Down
```

Table 6-1: Description of the Interface Information Displayed

Information Displayed	Description
Ifc	Physical and logical interface number.
Name	Interface type (FDDI, ATM LEC, ATM FDDI Bridge Tunnel, and so on), followed by a number indicating the instance within this type. Instance numbering starts at zero.
MAC/Data Link	Type of MAC/data link configured for the interface.
Hardware	Interface hardware type.
State	Current state of the interface. The following states are possible: • `Up` — The interface is connected and operational. • `Down` — The interface is not operational and failed self-test. • `Disabled` — The interface is either temporarily or permanently disabled. • `Testing` — The interface is in the process of completing a self-test. • `Not present` — Power-up (restart) diagnostics detected a fault on the interface.

Monitoring an FDDI Interface

This section provides information about how to monitor the FDDI interface. Monitoring includes the ability to display specific information about operational states, activity counters, and various interface configuration settings.

To monitor the interface, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **interface statistics**, followed by the number of the interface you want to monitor. The number is 1 for an FDDI interface.
2	Press Return. Information about operational states, activity counters, and various interface configuration settings is displayed.

Example

The following is an example of the information displayed. Refer to Table 6-2 for a description of the information.

```
Monitor>interface statistics 1

                      Self-Test     Self-Test      Maintenance
Ifc Ifc' Name        Passed         Failed         Failed
 1   1   FDDI/1              1             1               0

  FDDI/IEEE 802.2 MAC/data-link on FDDI interface

UNA: 0000F8000000 -> MLA: 08002BB4FE8E -> DNA: 0000F8000000
Policy: reject A-A B-B M-M                            Ring Inits: 4
Bypass: False           Purger State: purgerOff       FDX State: fdxIdle

Station: Das          ECM: In           CFM: thru          RMT: Ring_Op

Interface 1 A/M:  (PHY A, active)
   LEM Rejects: 0             LCT Fail Ct: 0             LEM Ct  : 0
   Alarm      : 10^-8         Cutoff     : 10^-8         Estimate: 10^-15
Interface 1 B/S:  (PHY B, active)
   LEM Rejects: 0             LCT Fail Ct: 0             LEM Ct  : 0
   Alarm      : 10^-8         Cutoff     : 10^-8         Estimate: 10^-15

T_Neg : 7.9872ms      TVX : 2.51904ms      T_Max : 167.77216ms
T_Req : 7.9872ms      T_Notify : 10s      Ring Latency : 0.13ms
Beacon Rcv: 0       Beacon Xmt: 0       Trace Rcv: 0       Trace Xmt: 0
Frame Ct: 10517            Frame Errors: 0               Frames Lost: 0

Bad CRC Xmt: 0
```

Table 6-2: Description of the Monitoring Information Displayed for FDDI

Information Displayed	Description
Ifc	Physical and logical interface number.
Ifc’	Not applicable on GIGAswitch GS2000 module.
Name	Interface type (FDDI, ATM LEC, ATM FDDI Bridge Tunnel, and so on), followed by a number indicating the instance within this type. Instance numbering starts at zero.
CSR	This field is not active for the FDDI interface.
Vec	This field is not active for the FDDI interface.
Self-Test Passed	Number of times the interface passed self-test since it was last restarted.

Information Displayed	Description
Self-Test Failed	Number of times the interface failed diagnostic self-test since it was last restarted.
Maintenance Failed	This field is not active for the FDDI interface.
UNA:	Address of the upstream neighbor, displayed in canonical format.
MLA:	Module MAC address of the FDDI interface, displayed in canonical format.
DNA:	Address of the downstream neighbor, displayed in canonical format.
Policy:	Shows the PHY port type connection combinations not allowed (rejected) on the interface's PHY ports. For example, `reject A-A B-B M-M`, indicates a link between PHY A port on one station and PHY A port on a second station is not allowed. PHY B port-to-PHY B port and PHY M port-to-PHY M port are also not allowed.
Bypass:	A value or `True` indicates an optical bypass relay (OBR) is present. `False` indicates an OBR is not present.
Purger State:	Indicates the state of the Ring Purger. Possible states include: Purger Off, Candidate, Nonpurger, and Purger. Refer to Chapter 5 for information about how to set the Ring Purger.
FDX State:	Indicates whether full-duplex mode is active or idle on the FDDI interface. Possible states include: fdx Idle, fdx Operation, fdx Request, and fdx Confirm. A value of fdx Operation indicates the interface is set to full-duplex mode and a full-duplex circuit was established following auto-negotiation. A value of fdx Idle indicates the interface is either set to half-duplex mode, or set to full-duplex mode but a half-duplex circuit was established following auto-negotiation. The fdx Request and fdx Confirm states are transitional states. Refer to Chapter 5 for information about how to set the interface for full-duplex or half-duplex mode.

Information Displayed	Description
Station:	Displays the station type to which the interface is set. Possible values include DAS, SAC, or SAS. Refer to Chapter 5 for information about how to set the Station Type.
ECM:	Displays the FDDI Entity Connection Management (ECM) state. ECM controls and manages the optical bypass. Possible states include: In, Out, Trace, Leave, Path-Test, Insert, Deinsert, and Check.
CFM:	Displays the FDDI Configuration Management State (CFM) state. Possible states include: Isolated, Local-a, Local-b, Local-ab, Local-s, Wrap-a, Wrap-b, Wrap-ab, Wrap-s, C-wrap-a, C-wrap-b, C-wrap-s, and Thru.
RMT:	Identifies the Ring Management (RMT) software monitoring the state of the ring. Possible values include: Isolated, Non-Op, Ring-Op, Non-Op-Dup, Ring-Op-Dup, Directed, and Trace.
Interface 1 A/M:	Indicates the state of the PHY port. Possible states include Disabled, Connecting, Stand By, and Active.
LEM Rejects:	Displays the number of times the Link Error Monitor detects a link was rejected.
LCT Fail Ct:	Displays the number of times the link confidence test failed since the last restart.
LEM Ct:	Displays the total number of link error events that occurred since the last restart.
Alarm:	Displays the currently configured Set PHY LER-Alarm value. Refer to Chapter 5 for information about how to set the Link Error Rate Alarm.
Cutoff:	Displays the currently configured Set PHY LER-Cutoff value. Refer to Chapter 5 for information about how to set the Link Error Rate Cutoff.

Information Displayed	Description
Estimate:	Displays the estimated bit error rate based on link monitoring.
T_Neg:	Displays the token rotation time.
TVX:	Displays the Valid Transmission Timer setting. This value is the maximum amount of time the interface waits to receive a *valid* data frame. Refer to Chapter 5 for information about how to set the Valid Transmission Timer.
T_Max:	Displays the Maximum Token Rotation Time (tmax-lower-bound). Refer to Chapter 5 for information about how to set this value.
T_Req:	Displays the Requested Token Rotation Time (t-req). Refer to Chapter 5 for information about how to set this value.
T_Notify:	Displays how often the interface generates Neighbor Information Frames (NIF) to neighbor nodes. This parameter is not user-configurable.
Ring Latency:	Amount of time it takes for data to make one rotation around the ring.
Beacon Rcv:	Displays the total number of times the interface received its own beacon frames and those of other stations since the last restart.
Beacon Xmt:	Displays the number of times the interface entered the Beacon Transmit state since the last restart.
Trace Rcv:	Displays the number of trace frames received.
Trace Xmt:	Displays the number of trace frames transmitted.

Information Displayed	Description
Frame Ct:	Displays the total number of frames passed on the ring since the last restart. **Note:** Disable the Ring Purger on all devices on the ring to get the most accurate ring utilization frame count. If the Ring Purger is on, void frames transmitted by the MAC are also counted, artificially increasing the frame count.
Frame Errors:	Displays the total number of Cyclic Redundancy Check (CRC) errors that occur on the ring since the last restart.
Frames Lost:	Displays the total number of frames lost on the ring since the last restart.

Monitoring an ATM Interface

This section provides information about how to display the results of interface maintenance and self-tests, and the MAC data link type associated with the interface. This section also provides information about how to monitor both an ATM physical interface and an ATM logical interface. Monitoring includes the ability to display specific information about operational states, activity counters, and various interface configuration settings.

Displaying Interface Test Results and MAC Type

To display interface test results and MAC type, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **interface statistics**, followed by the number of the desired interface. The range of possible ATM interface numbers is 2 through 17.
2	Press Return. The test report and MAC type are displayed.

Example

```
Monitor>interface statistics 14

                        Self-Test  Self-Test  Maintenance
Ifc Ifc' Name           Passed     Failed       Failed
14  14   ALEC/14             0            1              0
  ATM LAN Emulation C MAC/data-link on ATM interface
```

Monitoring the Physical Interface

To monitor a physical interface, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **interface** and the number of the interface you want to monitor. The range of possible ATM interface numbers is 2 through 17.
2	Press Return. The `ATM/`*n*`>` prompt is displayed.
3	If you want to monitor the physical interface, enter **physical**.
4	Press Return. The `ATM_OC3>` prompt is displayed.

Step	Action
5	Enter **list *option***, where ***option*** is the command you must enter to display the desired information. Refer to Table 6-3 for a list of commands.
6	Press Return. Information about the selected option and the ATM_OC3> prompt is displayed.

Example

ATM_OC3>**list mib-statistics current**

```
sect status              : 0x01
sect ess                 : 426
sect sess                : 426
sect sefs                : 0
sect cvs                 : 426
line status              : 0x01
line ess                 : 0
line sess                : 0
line cvs                 : 0
line uass                : 426
path width               : sonet path sts3
path status              : 0x08
path ess                 : 0
path sess                : 0
path cvs                 : 0
path uass                : 426
oocd                     : 4911
lcd_alarm                : no alarm
```

Table 6-3: ATM Physical Interface Command Options

Command Option	Description
modpmd-errors	Lists status and counters of the physical medium.
atom3-errors	Lists status and counters of the ATM SAR function.
status	Provides detailed status information on ATM links.
medium	Provides information about the physical medium.
mib-statistics *mib-option*, where ***mib-option*** is one of the command options described in the ATM Physical Interface MIB Statistics section.	Provides MIB statistics for the physical interface.

ATM Physical Interface MIB Statistics

The ATM physical interface maintains a variety of activity counters. Each counter records the total number of occurences of each activity per 15-minute period. Each 15-minute period is referred to as an interval. The module maintains a record of counts for the last 96 intervals which is equivalent to 24 hours. You can display counters for the current interval, for all 96 intervals (the last 24 hours), or for a selected interval.

Table 6-4: ATM Physical Interface MIB-Statistics Command Options and Descriptions

Command	Description
current	Displays counter information for the current interval (15-minute period).
total	Displays counter information for the last 24 hours (all 96 15-minute intervals).
interval	After you press Return, the following prompt is displayed: `1..96:` Enter a number from 1 through 96, where the number specifies the interval for which you want counter information displayed.

Monitoring a Logical Interface

To monitor a logical interface, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **interface** and the number of the interface you want to monitor. The range of possible ATM interface numbers is 2 through 17.
2	Press Return. The `ATM/`*n*`>` prompt is displayed.
3	Enter **list** ***option***, where ***option*** is the command you must enter to display the desired information. Refer to Table 6-5 for a list of commands, and for a description of the type of information that is displayed when you enter the command.
4	Press Return. Information about the selected option and the `ATM/`*n*`>` prompt are displayed.

Example

The following is an example of the information displayed when you enter the **all** command option for interface 2, when the interface is configured as a LAN Emulation Client (LEC):

ATM/2>**list all**

```
Interface               : 2 (Bridge Port 2)
Lec Status              : INITIAL
Elan Name(Configured)   :
Elan Name(Joined)       : Not available
Atm address             : 399999000000000000F84EEE80.0000F848890E.00

LE Arp Request Sent                  : 91256
LE Arp Request Received              : 31544
LE Arp Response Sent                 : 0
LE Arp Response Received             : 4

LEC Control Frames Sent              : 131703
LEC Control Frames Received          : 73049
LEC Illegal Control Frames Received  : 0

Ifc VP VCI   Type        S/PVC                ATM Address
2  0    5 Signaling     PVC
2  0   16 ILMI          PVC
```

If the interface is configured as an ATM bridge tunnel, the **list all** command would display information such as the following:

ATM/2>**list all**

```
Interface               : 2 (Bridge Port 2)
Bridge Tunnel Status    : up
Ifc VP VCI   Type        S/PVC                ATM Address
2   0    5 Signaling     PVC
2   0   16 ILMI          PVC
17  0   62 BT Ethernet   PVC
2   0 1000 BT Ethernet   PVC
3   0 1001 BT Ethernet   PVC
4   0 1002 BT Ethernet   PVC
```

Table 6-5: ATM Logical Interface Command Options

Command Option	Description
atm_address	ATM address for this logical port
le_arp_counters	Counters for LE ARP requests (responses sent and transmitted on this LEC port)
lec_counters	LEC port counters
lec_status	LEC port status

Command Option	Description
tunnel_state	State (up or down) of the Ethernet or FDDI bridge tunnel (applies only when configured as an ATM bridge tunnel)
vc	All virtual circuits on this interface (applies only when configured as an ATM bridge tunnel)
all	(Applies only when configured as an ATM bridge tunnel.)

Monitoring Packet Statistics and Error Counts

You can monitor the following information about one or more interfaces:

- Packet buffers
- Error counts
- Input and output queues
- Packet statistics

Displaying Packet Buffer Data

You can display a report that displays packet buffer data for one or all interfaces. The buffer size for each interface is built dynamically and is different for each type of interface. Global system buffers are of one size and are equal to the maximum buffer size of all interface buffers.

Note

The information provided by the packet buffer report reflects activity occurring on the module's management processor only. It does not include data about buffers in the module's forwarding subsystem.

To display the report, perform the following steps:

Step	Action
1	If you want to view packet buffer data for all interfaces, enter **buffer** at the Monitor prompt (`Monitor>`). If you want to view packet buffer data for a selected interface, enter **buffer** ***interface#*** at the Monitor prompt (`Monitor>`), where ***interface#*** is the number of the interface for which you want to display packet buffer data.
2	Press Return. The packet buffer report is displayed, and the Monitor prompt is displayed.

Example

The following is an example of the information displayed for a single (FDDI) interface. If you chose to display data for all interfaces, a similar report is displayed, containing the same information for each interface. Refer to Table 6-6 for a description of the information.

```
Monitor>buffer 1

                Input Buffers        Buffer sizes                    Bytes
Ifc Name        Req Alloc Low Curr   Hdr  Wrap  Data Trail Total    Alloc
1  FDDI/1        16   16    4   16    28    42  4478     4  4552    72832
```

Table 6-6: Description of the Buffer Information Displayed

Information Displayed	Description
Ifc	Physical and logical interface number.
Name	Interface type (FDDI, ATM LEC, ATM FDDI Bridge Tunnel, and so on), followed by a number indicating the instance within this type. Instance numbering starts at zero.
Input Buffers Req	Number of buffers requested.
Input Buffers Alloc	Number of buffers allocated.
Input Buffers Low	Low water mark (for flow control).
Input Buffers Curr	Current number of buffers on this interface. The value is 0 if the interface is down. The packet is eligible for flow control if the value of `Curr` is below `Low` when a packet is received. Refer to the Input and Output Queues section for conditional information.
Buffer Sizes Hdr	Sum of the maximum hardware, MAC, and data link headers.
Buffer Sizes Wrap	Allowance given for MAC, LLC, or network layer headers due to protocol wrapping.
Buffer Sizes Data	Maximum data link layer packet size.
Buffer Sizes Trail	Sum of the largest MAC and hardware trailers.
Buffer Sizes Total	Overall size of each packet buffer.
Buffer Sizes Bytes Alloc	Amount of buffer memory for the interface. This value is determined by multiplying the values of `Alloc X Total`.

Packet Error Statistics

You can display a report that displays packet error statistics for one or all interfaces. To display the report, perform the following steps:

Step	Action
1	If you want to view error statistics for all interfaces, enter **error** at the Monitor prompt (`Monitor>`). If you want to view error statistics for a selected interface, enter **error** ***interface#*** at the Monitor prompt (Monitor>), where ***interface#*** is the number of the interface for which you want to display error statistics.
2	Press Return. The error statistics report is displayed, and the Monitor prompt is displayed.

Example

The following is an example of the information displayed for a single (FDDI) interface. If you chose to display data for all interfaces, a similar report is displayed, containing the same information for each interface. Refer to Table 6-7 for a description of the information.

```
Monitor>error 1

                    Input       Input      Input      Input     Output     Output
Ifc Name          Discards      Errors  Unk Proto  Flow Drop   Discards     Errors
 1  FDDI/1               0           0         18          0          0          0
```

Table 6-7: Description of the Packet Error Information Displayed

Information Displayed	Description
Ifc	Physical and logical interface number.
Name	Interface type (FDDI, ATM LEC, ATM FDDI Bridge Tunnel, and so on), followed by a number indicating the instance within this type. Instance numbering starts at zero.
Input Discards	Number of packets received unsuccessfully.
Input Errors	Number of packets that were defective at the data link.
Input Unk Proto	Number of packets received for an unknown protocol.
Input Flow Drop	Number of packets received that are flow controlled on input.
Output Discards	Number of packets the module chose to discard rather than transmit due to flow control.
Output Errors	Number of output errors including, for example, attempts to send data over a network that is down or that went down during transmission.

Note

The sum of the Output Discards is not the same as Input Flow Drops over all networks. Output Discards may indicate locally originated packets.

Input and Output Queues

You can display a report that displays information about the length of input and output queues for one or all interfaces.

Note

The information provided by the input and output queue report reflects activity occurring on the module's management processor only. It does not include data about queues in the module's forwarding subsystem.

To display the input and output queue report, perform the following steps:

Step	Action
1	If you want to view input and output queues for all interfaces, enter **queue** at the Monitor prompt (`Monitor>`). If you want to view input and output queues for a selected interface, enter **queue** ***interface#*** at the Monitor prompt (`Monitor>`), where ***interface#*** is the number of the interface for which you want to display queues.
2	Press Return. The queue report is displayed, and the Monitor prompt is displayed.

Example

The following is an example of the information displayed for a single (FDDI) interface. If you chose to display data for all interfaces, a similar report is displayed, containing the same information for each interface. Refer to Table 6-8 for a description of the information.

```
Monitor>queue 1

                Input Queue     Output Queue
Ifc Name       Alloc Low Curr    Fair Curr
 1  FDDI/1        16   4   16       8    0
```

Table 6-8: Description of the Input and Output Queue Information Displayed

Information Displayed	Description
Ifc	Physical and logical interface number.
Name	Interface type (FDDI, ATM LEC, ATM FDDI Bridge Tunnel, and so on), followed by a number indicating the instance within this type. Instance numbering starts at zero.
Input Queue Alloc	Number of buffers allocated to the interface.
Input Queue Low	Low water mark for flow control on this interface.
Input Queue Curr	Current number of buffers on this interface. The value is 0 if the interface is disabled or down.
Output Queue Fair	Fair level for the length of the output queue on the interface.
Output Queue Curr	Number of packets currently waiting to be transmitted on the interface. For locally originated packets, the eligibility discard depends on the global low water mark value you can monitor by displaying the module's memory as described in Chapter 4.

Flow Control and Dropped Buffers

The module attempts to keep at least the Low value packets available for receiving over an interface. If a packet is received and the value of `Curr` is less than `Low`, then the packet is subject to flow control. If a buffer subject to flow control is to be queued on the interface and the `Curr` value is greater than `Fair`, the buffer is dropped instead of queued. The dropped buffer is displayed in the `Output Discards` column of the packet error statistics report. (Refer to the Packet Error Statistics section.) It also generates ELS event GW.036 or GW.057.

Interpreting Current Buffer Values During Packet Forwarding

Due to the scheduling algorithms of the module, the dynamic values of `Curr` (especially `Input Queue Curr`) may not be fully representative of typical values. The Monitor code runs when the input queues are drained. Therefore, `Input Queue Curr` is nonzero when those packets are waiting on slow transmit queues.

Note

The information provided by the input and output queue report reflects activity occurring on the module's management processor only. It does not include data about queues in the module's forwarding subsystem.

Packet Statistics

You can display a report that displays packet information for one or all interfaces. To display the report, perform the following steps:

Step	Action
1	If you want to view packet statistics for all interfaces, enter **statistics** at the Monitor prompt (`Monitor>`). If you want to view packet statistics for a selected interface, enter **statistics** ***interface#*** at the Monitor prompt (`Monitor>`), where ***interface#*** is the number of the interface for which you want to display packet statistics.
2	Press Return. The queue report is displayed, and the Monitor prompt is displayed.

Example

The following is an example of the information displayed for a single (FDDI) interface. If you chose to display data for all interfaces, a similar report is displayed, containing the same information for each interface. Refer to Table 6-9 for a description of the information.

```
Monitor>statistics 1

                  Unicast      Multicast       Unicast      Multicast
Ifc Name          Pkts Rcv      Pkts Rcv    Pkts Trans    Pkts Trans
 1  FDDI/1            2793           518          2739          3311
```

Table 6-9: Description of the Packet Statistics Displayed

Information Displayed	Description
Ifc	Physical and logical interface number.
Name	Interface type (FDDI, ATM LEC, ATM FDDI Bridge Tunnel, and so on), followed by a number indicating the instance within this type. Instance numbering starts at zero.
Unicast Pkts Rcv	Number of nonmulticast, nonbroadcast, specifically addressed packets at the MAC layer.
Multicast Pkts Rcv	Number of multicast or broadcast packets received.
Unicast Pkts Trans	Number of nonmulticast, nonbroadcast, specifically addressed packets transmitted.
Multicast Pkts Trans	Number of multicast or broadcast packets transmitted.

Displaying Interface Test Results

You can display a report that includes the results of interface maintenance tests and self-tests for all interfaces. Refer to the Testing an Interface section for additional information about interface tests.

To display interface test results for all interfaces, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **interface statistics**.
2	Press Return. The test report is displayed.

Example

```
Monitor> interface statistics

                        Self-Test     Self-Test      Maintenance
Ifc Ifc' Name              Passed        Failed           Failed
 0   0   VNbus/0                0             0                0
 1   1   FDDI/1                 1             1                0
 2   2   ALEC/2                 0             1                0
 3   3   ALEC/3                 0             1                0
 4   4   ALEC/4                 0             1                0
 5   5   ALEC/5                 0             1                0
 6   6   ALEC/6                 0             1                0
 7   7   ALEC/7                 0             1                0
 8   8   ALEC/8                 0             1                0
 9   9   ALEC/9                 0             1                0
10  10   ALEC/10                0             1                0
11  11   ALEC/11                0             1                0
12  12   ALEC/12                0             1                0
13  13   ALEC/13                0             1                0
14  14   ALEC/14                0             1                0
15  15   ALEC/15                0             1                0
16  16   AFBT/16                0             1                0
17  17   AEBT/17                4            52                0
```

Clearing Interface Counters

You can clear (reset to zero) error, packet, and other counters associated with a specific interface, or all interfaces. You may find the ability to do so useful if you want to track recent changes in one or more counters. The counters cleared are those discussed in the Monitoring an FDDI Interface, Monitoring an ATM Interface, and Monitoring Packet Statistics and Error Counts sections. For a complete list of interface and bridge port countes, see Appendix C.

To clear interface counters, perform the following steps:

Step	Action
1	Access the Monitor prompt (`Monitor>`).
2	If you want to clear counters for all interfaces on the module, enter **clear**. If you want to clear counters for a specific interface on the module, enter **clear *interface#***, where ***interface#*** is the number of the interface for which you want to clear counters.
3	Press Return. The following message is displayed: `Clear network statistics? (Yes or [No]):`
4	Enter **y** if you want to clear the interface counters. Enter **n** if you do not want to clear the interface counters.
5	Press Return. The counters are cleared or not cleared as specified, and the Monitor prompt is displayed.

Testing an Interface

FDDI and ATM interfaces perform a self-test when they are first powered up. With the exception of ATM, these interfaces periodically perform maintenance tests while they are up. Self-tests typically provide a more thorough verification process than maintenance tests. ATM interfaces perform self-tests only during power up and do not perform maintenance tests. Doing so would disable all ATM logical interfaces, not just the interface you specify.

To test a physical interface, use the **enable interface *n*** and **disable interface *n*** commands at the Config> prompt as explained in the Enabling and Disabling an Interface section of Chapter 5.

Monitoring the Address Resolution Protocol

This section provides information about how to monitor the Address Resolution Protocol (ARP). Monitoring includes the ability to perform the following tasks:

- List learned and manual entries in the ARP cache.
- List the interfaces registered with ARP.
- List the protocols with addresses registered with ARP.
- Display ARP operational statistics, including such information as input packet overflows.
- Delete (clear) all learned entries from the ARP cache.

To monitor the interface, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **arp**.
2	Press Return. The ARP> prompt is displayed.
3	Enter one of the command options shown in Table 6-10 to display the desired information.
4	Press Return. The desired information and the ARP> prompt is displayed.

Table 6-10: ARP Monitor Command Options

Command Option	Description
clear ***interface***, where ***interface*** is the number of the TCP/IP Host Services logical interface. (Refer to Chapter 1 for a description of the Host Services logical interface.) To determine the correct interface number, first use the **hardware** command, below. The interface number you enter is the number adjacent to the TCP/IP Host Services logical interface name BDG/0.	Deletes all learned and manually entered entries from the ARP cache associated with the specified interface. This command option can be used to force the deletion of bad transactions.

Command Option	Description
dump ***interface*** [***protocol***], where ***interface*** is the number of the TCP/IP Host Services logical interface. (Refer to Chapter 1 for a description of the Host Services logical interface.) To determine the correct interface number, first use the **hardware** command, below. The interface number you enter is the number adjacent to the TCP/IP Host Services logical interface name BDG/0. The ***protocol*** parameter specifies the short name or number of the protocol for which you want to display information. Use the **protocol** option to determine the protocol's name or number. The protocol name and number are optional if ARP is in use by only one protocol on the specified interface.	Displays the ARP cache for the specified interface/protocol combination. If more than one protocol is on the interface, the protocol number must also be entered. This displays the address-to-protocol mappings.
hardware	Displays the interfaces registered with ARP. The interface is identified by number and type. The command option also displays the interface's hardware address space (AS) and local hardware address.
protocol	Displays the protocols for each interface that have addresses registered with ARP. The information displayed includes the interface number and type, the protocol name, the protocol address space (AS) in hexadecimal, and the associated local protocol address.

Command Option	Description
statistics	Displays the number of ARP input packet overflows by interface, and the following ARP cache information for each protocol per interface: `Max` — All time maximum length hash chain. `Cur` — Current maximum length hash chain. `Cnt` — Number of currently active entries. `Alloc` — Number of entries created. `Refresh:Tot` — Number of refresh requests sent for the network interface and protocol. `Failure` — Number of Auto-Refresh attempt failures due to unavailability of internal resources. This count is not related to whether or not an entry was refreshed. `TMOs: Refresh` — Number of entries deleted due to a timeout of the Refresh Timer.

Monitoring ICMP Counters

Internet Control Message Protocol (ICMP) is a part of IP that handles error and control messages, including an echo request/reply function to test whether a destination is reachable and responding. ICMP provides error, status and administrative messages that are incorporated into the data field of an IP packet. To display the list of ICMP counters, perform the following steps:

Step	Action
1	At the `IP>` prompt, enter: **icmp-counters**
2	Press Return. A list of ICMP counters are displayed.

Example

```
IP> icmp-counters

ICMP counters                     Receive       Transmit
Total number of messages               15             17
Number of errors                        0              0
Destination Unreachable                 0              0
Time Exceeded                           0              2
Parameter Problem                       0              0
Source Quench                           0              0
Redirect                                0              0
Echo request                           13              0
Echo reply                              0             13
Timestamp request                       1              0
Timestamp reply                         0              1
Address Mask request                    1              0
Address Mask reply                      0              1
```

Field	Description
`Total number of messages`	Total number of ICMP messages sent and received
`Number of errors`	Generic errors, such as buffer allocation errors, detected by the router.
`Destination Unreachable`	Used by the router or the destination host and is invoked if a router encounters problems reaching the destination network specified in the IP destination address. Also, the destination host can invoke this if an identified higher-level protocol is not available on the host or if a specified port is not available.
`Time Exceeded`	Initiated by the router when the time-to-live value becomes zero or if a timer expires during reassembly of a fragmented datagram
`Parameter Problem`	Initiated by a host or the router if it encounters problems processing any part of an IP header
`Source Quench`	Flow and congestion control that is used if the router has insufficient buffer space for queuing incoming datagrams
`Redirect`	Invoked by the router and sent to the source host and is used to provide routing management information
`Echo request`	A PING message sent to any IP address to determine the state of the internet or a network segment.
`Echo reply`	A PING message sent by a host in response to an echo request.
`Timestamp request`	This is used by the router and hosts to determine the delay incurred when delivering packets through a network
`Timestamp reply`	Timestamp values sent by a host in response to a timestamp request.
`Address Mask request`	Used by a host to obtain a subnet mask used on the host's network. The requesting host can send the request directly to a router or broadcast it.
`Address Mask reply`	A reply from an address mask agent host or any authoritative originator of the address mask on the network containing the network's subnet mask.

Chapter 7

Configuring the Transparent Bridge

Overview

Introduction

This chapter provides information about how to configure the DIGITAL GIGAswitch GS2000 line card module transparent bridge and how to display information about the current configuration. The parameters you configure, as described in this chapter, are stored in nonvolatile RAM (NVRAM). Information stored in NVRAM is retained in memory even if power to the module is interrupted or the module is reset.

In This Chapter

The following topics are covered in this chapter:

Accessing and Exiting the Bridge Configuration Prompt

You must access the bridge configuration prompt to configure and display network parameters. The prompt is accessed from the Config prompt (`Config>`).

Accessing the Bridge Configuration Prompt

To access the Bridge configuration prompt, perform the following steps:

Step	Action
1	At the Config prompt, enter **bridge**. The default protocol selection is **bridge**. **Example:** `Config>` **bridge**
2	Press Return. The Bridge configuration prompt (`BRIDGE config>`) is displayed.

Exiting the Bridge Configuration Prompt

You exit the Bridge config prompt to return to the Config prompt.

Example

To return to the Config prompt (`Config>`) from the `BRIDGE config>` prompt, enter **exit** and then press Return.

Setting and Enabling Module-Wide Rate Limiting

This section describes how to configure rate limiting on a module-wide basis. To configure module-wide rate limiting, perform the following tasks:

Task	Description
1	Set the maximum number of packets per second (pps).
2	Enable or disable rate limiting.

Rate limiting is used to minimize the effects of broadcast storms. A broadcast storm is typically caused when a host system responds to multicast packets that are circulating continuously on the network, or when it tries to respond to another system that never replies. The generation of such traffic at an uncontrolled rate can severely affect the available bandwidth on a network, perhaps making communications impossible.

You can limit broadcast storms to that segment of the network from which the packets are generated. You do so by setting the maximum number of multicast packets per second (pps) that the module is to forward. The rate (pps) you set is applied only if rate limiting is enabled. If the maximum number of packets per second is reached, the module forwards packets at the specified maximum rate, thereby limiting the effect of the broadcast storm on the other side of the module. Module-wide rate limiting is disabled by default.

Setting Maximum Frames Per Second

You can set the maximum number of frames per second either independent of enabling rate limiting, or while enabling rate limiting. To set the maximum number of frames per second independent of enabling rate limiting, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **set rate-limit**.
2	Press Return. The following message is displayed: `Rate Limit Value (frames/sec) [400]?`
3	Enter the maximum number of packets per second the module is to forward destined for a particular MAC address, or that are of a particular protocol type. The default is 400 frames per second.
4	Press Return. The maximum number of frames per second is set and the `BRIDGE config>` prompt is displayed.

Enabling and Disabling Rate Limiting

You enable and disable rate limiting on both a module-wide basis and on a per-filter (MAC address or protocol) basis. This section describes how to enable and disable module-wide rate limiting. Refer to the Creating and Modifying a Permanent Address Filter section for information about how to set rate limiting for multicast address filters. Refer to the Creating and Modifying Protocol Filters section for information about how to set rate limiting for protocol filters.

If rate limiting is disabled on the module, it is disabled for all address and protocol filters, even if rate limiting for the individual filter is enabled. If rate limiting is enabled on the module, it is enabled for a specific filter only if rate limiting is also enabled for the filter. Disabled is the default for module-wide rate limiting.

Enabling Module-Wide Rate Limiting

To enable module-wide rate limiting, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **enable rate-limit**.
2	Press Return. The following message is displayed: `Rate limit value [400]?`
3	Enter the maximum number of packets per second the module is to forward destined for a particular MAC address, or that are of a particular protocol type. The factory default is 400 frames per second. If the factory default was modified, the default is the most recent setting.
4	Press Return. Rate limiting is enabled and the specified rate is applied on a module-wide basis. The `BRIDGE config>` prompt is again displayed.

Disabling Module-Wide Rate Limiting

To disable module-wide rate limiting, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **disable rate-limit**.
2	Press Return. Rate limiting is disabled on a module-wide basis.

Configuring Permanent Address Filters

This section discusses how to add, modify, and delete MAC address filters. The process of filtering network traffic is used to reduce the amount of unnecessary traffic over specific segments of a network, thereby maximizing network capacity and performance. It can also be used to restrict the distribution of sensitive information to specific locations. You can configure the module to selectively filter or forward packets it receives, based on their MAC addresses and protocol types.

MAC address filters are stored in NVRAM as permanent entries. (Refer to Chapter 1 for information about NVRAM.) Permanent address entries are retained in memory even if power to the module is interrupted or the switch is reset. Permanent entries are not affected by address Aging Time, and can exist concurrently with dynamic entries having the same address. (Refer to Chapter 8 for information about configuring a MAC address as a static entry.)

You configure a filter by specifying a set of ports that are allowed for a given MAC address. The address can be an individual, multicast, or broadcast address. If a packet has a source or destination MAC address that is listed in the filter, the packet is allowed on the specified set of ports. If the address is not listed in the filter, the packet is dropped (filtered).

Source Address Filtering

A packet received on an input port is dropped (filtered) if the source address is listed in a filter and the input port is not one of the allowed ports. In addition, the source address is not learned.

If the input port is one of the allowed ports, the packet is a candidate for forwarding, based on the behavior of destination address filtering and protocol filtering. (Refer to the Configuring Protocol Filters section for information about protocol filtering.)

Destination Address Filtering

A packet about to be placed on an output port is forwarded if the destination address is listed in a filter and the output port is one of the allowed ports. If the address was not previously learned, the packet is flooded to the subset of the allowed ports that are in the forwarding state.

Creating and Modifying a Permanent Address Filter

To create or modify a MAC address filter, you must perform the following tasks:

Task	Description
1	Identify the address to be filtered, and the ports on which the address is allowed.
2	Enable or disable multicast rate limiting (multicast addresses only).

Identifying the Address and Allowed Ports

The addresses you specify when creating a filter are added to the module's permanent database (NVRAM). To identify the allowed ports for an address, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **set address**. You can, alternatively, enter **set address *mac_address***, where ***mac_address*** is the 12-digit MAC address for which you want to create or modify a filter on the module. If you enter the command using this syntax, go to step 4.
2	Press Return. The following message is displayed: `Address (in 12-digit hex) []?`
3	Enter the 12-digit MAC address for which you want to create or modify a filter. You can enter the address with or without hyphens separating the octets. For example, you can enter **11-22-33-44-55-66** or **112233445566**.
4	Press Return. The following message is displayed: `Enter allowed ports ("None" or "All") []?` If you are modifying the forwarding ports for an existing address, the previously configured ports are the default.

Step	Action
5	Enter a list of the bridge ports to which you want the packet with the specified MAC address forwarded. (The packet is filtered from those ports not entered.) Enter **None** if you want the packet filtered from all ports. Enter **all** if you want the packet allowed on all ports. You can list the forwarding ports individually by separating each with a comma (for example, **0,1,2,3,4,5**) or you can enter a range of ports by separating the first and last port numbers in the range with a hyphen (for example, **0-5**). You can also combine a list of individual entries with a range of entries (for example, **0-4,6,7**). Spaces are not permitted between port numbers and the comma or hyphen.

6	Press Return.
	If the address is a unicast address, the address is set and the `BRIDGE config>` prompt is displayed.
	If the address is a multicast address, the following message is displayed:
	`Enable Multicast Rate Limiting (Yes or No)? [No]:`
	Refer to the Enabling and Disabling Multicast Rate Limiting section.
	If any of the specified ports do not exist, the address is set for forwarding on the port but the port setting has no effect. A message similar to the following is displayed:
	`Warning, ports 9, 10 do not exist`

Enabling and Disabling Multicast Rate Limiting

Multicast rate limiting is used to minimize the effects of multicast storms. You can restrict multicast storms, consisting of packets that have a specific destination MAC address, to that segment of the network from which the packets are generated. You do so by setting the maximum number of those packets the module is to forward per second, and by enabling rate limiting.

Rate limiting is enabled on both a per-address basis and a module-wide basis. This section provides instructions about how to enable or disable rate limiting on a per MAC address basis. Refer to the Setting and Enabling Module-Wide Rate Limiting section for information about setting the maximum number of packets per second and enabling or disabling rate limiting on a module-wide basis.

To enable or disable multicast rate limiting for the address specified in the Identifying the Address and Allowed Ports section, perform the following steps:

Step	Action
1	Enter **Yes** to enable Multicast Rate Limiting. Enter **No** to disable Multicast Rate Limiting. **No** is the default unless it was previously enabled for the address.
2	Press Return. The selected filter is applied to the module and rate limiting is enabled or disabled, as specified.

Deleting Permanent Address Filters

This section describes how to delete MAC address filters that you, or another switch administrator, previously entered manually. (Refer to the Creating and Modifying a Permanent Address Filter section.) You can delete address filters one at a time, or you can delete all MAC address filters previously added to the module's permanent database (NVRAM). Deleting an address filter removes the address from the forwarding database as well as its associated multicast rate limiting status.

Note

Registered unicast and reserved addresses cannot be deleted.

Deleting a Single Permanent Address Filter

To delete one MAC address, its filter, and its associated rate limiting status, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **delete address**. You can, alternatively, enter **delete address *mac-address***, where ***mac-address*** is the 12-digit MAC address you want to delete. If you enter the command using this syntax, go to step 4.
2	Press Return. The following message is displayed: `Address (in 12-digit hex) []?`
3	Enter the 12-digit MAC address you want to delete. You can enter the address with or without hyphens separating the octets. For example, you can enter **11-22-33-44-55-66** or **112233445566**.

Step	Action
4	Press Return. The specified address is deleted. If you entered an address that does not exist, the following message is displayed: `No entry found for this address`

Deleting All Permanent Address Filters

To delete all MAC addresses and associated filters and rate limiting status, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **delete address all**.
2	Press Return. All MAC addresses are deleted.

Configuring Protocol Filters

Protocol filtering enables you to configure a module so that it selectively filters traffic based on the data's MAC frame format. The module supports protocol filtering for the following frame types:

- Ethernet-II (IEEE 802.3)
- IEEE 802.3 Subnetwork Access Protocol (SNAP)
- IEEE 802.3 Destination Service Access Point (DSAP)

Each frame type can conform to one of a number of different protocols. Common protocols are listed in Table 7-1 through Table 7-3. When you create a protocol filter, you can configure the module to receive or forward frames on one or more selected bridge ports, based on the frame's protocol. For example, you can configure one or more ports on the module so that Ethernet frames, conforming to the AppleTalk Phase 1 protocol, are received or forwarded only on those ports.

A received packet is dropped (filtered) if there is a filter for the protocol and the input port is not one of the allowed ports. Also, the packet can only be output on a port that is one of the allowed ports.

You can also configure the module to receive or forward *all* frames of a particular type from one or more bridge ports, using protocols not already filtered as described above. You do so by configuring a default protocol filter. For example, if you configure the module so that Ethernet frames conforming to the AppleTalk Phase 1 protocol are discarded, you can then use a default filter to discard (or receive/forward) all Ethernet frames of any other protocol type such as IP, ARP, DECnet, and so on. Refer to the Creating and Modifying Default Protocol Filters section for information about how to create a default protocol filter.

Note

GIGAswitch GS2000 firmware allows you to configure protocol filters based on both the encapsulation and the protocol type. That is, to configure a protocol filter for a given set of ports, the user chooses the encapsulation, the protocol type, and the list of the ports to which the filter applies.

When configuring protocol filters, keep the following in mind. Forwarding of a packet from a LAN segment with one type of encapsulation to another LAN segment with a different encapsulation type requires translation. The translation of the packet takes place after the filter-forwarding decision is made. Therefore, if an Ethernet IP packet is forwarded to the FDDI port, an Ethernet IP filter needs to be set for the FDDI port for filtering to occur, even though the transmitted packet has a SNAP encapsulation.

To prevent an error in the protocol filter configuration for a given set of ports, the best approach is to set protocol filters for all encapsulation types of the protocol to be filtered on each set of ports. This, typically, can be done without any side effects. If this approach interferes with other considerations, base the configuration on filter encapsulation and choose with caution.

Creating and Modifying Protocol Filters

To create or modify a protocol filter, perform the following tasks:

Task	Description
1	Identify the specific protocol to be filtered and the allowed ports on which frames of the specified protocol type can be received and forwarded.
2	Enable or disable protocol rate limiting.

Identifying the Protocol and Allowed Ports

To specify the protocol to be filtered and the allowed ports on which the frames are received or forwarded, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **set protocol-filter**.
2	Press Return. The following message is displayed: `Protocol type [DSAP]?`
3	Enter one of the following types of frames for which you want to specify a protocol: • **ether** (Ethernet-II) • **snap** • **dsap** DSAP is the default.

Step	Action

4	Press Return.
	If you entered **ether**, the following message is displayed:
	`Protocol Type in hex (5DD-FFFF) [0800]?`
	If you entered **snap**, the following message is displayed:
	`Address (in 10-digit hex) [00-00-00-08-00]?`
	If you entered **dsap**, the following message is displayed:
	`Protocol Type in hex (0-FF) [1]?`

5	Enter the hexadecimal value associated with the protocol you want to filter from receiving ports. Refer to Table 7-1 for the hexadecimal value of common Ethernet protocols you can filter. Refer to Table 7-2 for the hexadecimal value of common SNAP protocols you can filter. Refer to Table 7-3 for the hexadecimal value of common DSAP protocols you can filter.
6	Press Return. The following message is displayed: `Enter allowed ports ("None" or "All") [0-254]?` The default is all ports if you are creating a new filter. The previously configured ports are the default if you are modifying an existing protocol filter.
7	Enter a list of the bridge ports on which you want frames to be received or forwarded based on the specified protocol. (The frames are filtered from those ports not entered.) Enter **None** if you want the frames filtered from all ports. Enter **all** if you want the frames allowed on all ports. You can list the ports individually by separating each with a comma (for example, **0,1,2,3,4,5**) or you can enter a range of ports by separating the first and last port numbers in the range with a hyphen (for example, **0-5**). You can also combine a list of individual entries with a range of entries (for example, **0-4,6,7**). Spaces are not permitted between port numbers and the comma or hyphen.

Step	Action

8	Press Return. The following message is displayed:
	`Enable Multicast Rate Limiting (Yes or No)? [Yes]:`
	The default is **No** if you are creating a new filter. The default is the previously configured setting if you are modifying an existing filter.
	Refer to the Enabling and Disabling Multicast Rate Limiting section.
	If the specified ports do not exist, the frame is set for forwarding on the port but is not operational until the port is added. A message similar to the following is displayed in addition to the rate limiting prompt:
	`Warning, ports 9, 10 do not exist`

Table 7-1: Hexadecimal Values for Common Ethernet-II (IEEE 802.3) Protocols

Protocol	Hexadecimal Value
IP	0800
ARP	0806
CHAOS	0804
DECnet MOP Dump/Load	6000
DECnet MOP Remote Console	6002
DECnet	6003
DEC LAT	6004
DEC LAVC	6007
XNS	0600
Maintenance Packet Type	7030
Apollo Domain	8019 (Ethernet)
Novell NetWare IPX	8137 (Ethernet)
AppleTalk Phase 1	809B
Apple ARP Phase 1	80F3
Loopback assistance	9000

Table 7-2: Hexadecimal Values for Common SNAP OUI/IP Protocols

Protocol	Ten-Digit Hexadecimal Value
AppleTalk Phase 2	08-00-07-80-9B
Apple ARP Phase 2	00-00-00-80-F3
Proprietary AppleTalk Phase 1 for FDDI	00-00-93-00-02
Proprietary AppleTalk ARP Phase 1 for FDDI	00-00-93-00-03

Table 7-3: Hexadecimal Values for Common DSAP Protocols

Protocol	Hexadecimal Value
Banyan SAP	BC (used for only 802.5)
Novell IPX SAP	E0 (used for only 802.5)
NetBIOS SAP	F0
ISO Connectionless Internet	FE

Enabling and Disabling Multicast Rate Limiting

Multicast rate limiting is used to minimize the effects of broadcast storms. You can limit broadcast storms, consisting of frames of a particular protocol type, to that segment of the network from which the frames are generated. You do so by setting the maximum number of those frames the module is to receive per second, and by enabling rate limiting.

Rate limiting is enabled on both a protocol basis and a module-wide basis. This section provides instructions about how to enable or disable rate limiting on a protocol basis. Refer to the Setting and Enabling Module-Wide Rate Limiting section for information about setting the maximum number of packets per second (pps) and enabling or disabling rate limiting on a module-wide basis.

To enable or disable rate limiting for the protocol specified in the Identifying the Protocol and Allowed Ports section, perform the following steps:

Step	Action
1	Enter **Yes** to enable Multicast Rate Limiting. Enter **No** to disable Multicast Rate Limiting. **No** is the default.
2	Press Return. The selected filter is applied to the module and rate limiting is enabled or disabled, as specified.

Deleting Protocol Filters

You can delete previously configured protocol filters from the module. You can delete filters one at a time by protocol type, or you can delete all protocol filters by frame type or protocol type.

Deleting a protocol filter may increase the amount of traffic over specific segments of a network and may, therefore, reduce network capacity and performance.

Deleting a Single Filter by Protocol Type

To delete a single filter by protocol type, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **delete protocol-filter**.
2	Press Return. The following message is displayed: `Protocol type [DSAP]?`
3	Enter one of the following types of frames for which you want to delete a protocol filter: • **ether** (Ethernet-II) • **snap** • **dsap** DSAP is the default.

Step	Action

4	Press Return.
	If you entered **ether**, the following message is displayed:
	`Protocol Type in hex (5DD-FFFF or ALL) [800]?`
	If you entered **snap**, the following message is displayed:
	`Address (in 10-digit hex or ALL) [00-00-00-08-00]?`
	If you entered **dsap**, the following message is displayed:
	`Protocol Type in hex (0-FF or ALL) [1]?`

5	Enter the hexadecimal value associated with the filter you want to delete. Refer to Table 7-1 for the hexadecimal value of common Ethernet protocols you can filter. Refer to Table 7-2 for the hexadecimal value of common SNAP protocols you can filter. Refer to Table 7-3 for the hexadecimal value of common DSAP protocols you can filter.
6	Press Return. The protocol filter is deleted and the `BRIDGE config>` prompt is displayed.

Deleting All Protocol Filters of a Particular Frame Type

To delete all protocol filters associated with a particular frame type, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **delete protocol-filter**.
2	Press Return. The following message is displayed: `Protocol type [DSAP]?` The default is DSAP, ETHER, or SAP if the respective filters of that protocol are present.
3	Enter one of the following frame types for which you want to delete all associated protocol filters: • **ether** (Ethernet-II) • **snap** • **dsap** The default is DSAP.

Step	Action

4	Press Return.
	If you entered **ether**, the following message is displayed:
	`Protocol Type in hex (5DD-FFFF or ALL) [800]?`
	If you entered **snap**, the following message is displayed:
	`Address (in 10-digit hex or ALL) [00-00-00-08-00]?`
	If you entered **dsap**, the following message is displayed:
	`Protocol Type in hex (0-FF or ALL) [1]?`

5	Enter a protocol type or enter **all** and go to step 6.
6	Press Return. A message similar to the following is displayed: `Modify default protocol filters for DSAP (Yes or No)? [Yes]:`
7	If you want to modify the default protocol filters associated with all the protocol filters you are about to delete, enter **Yes**. If you do not want to modify the default protocol filters associated with all the protocol filters you are about to delete, enter **No**.
8	Press Return. If you entered **Yes**, go to step 9. If you entered **No**, go to step 11.
9	The following message is displayed: `Allowed port numbers ("None" or "All") [0-254]?` The previously configured ports are the default if you are modifying an existing default protocol filter.
10	Enter a list of the bridge output ports from which you want frames forwarded based on the specified protocol. (The frames are filtered from those ports not entered.) Enter **None** if you want the frames filtered from all ports. Enter **all** if you want the frames forwarded on all ports. You can list the forwarding ports individually by separating each with a comma (for example, **0,1,2,3,4,5**) or you can enter a range of ports by separating the first and last port numbers in the range with a hyphen (for example, **0-5**). You can also combine a list of individual entries with a range of entries (for example, **0-4,6,7**). Spaces are not permitted between port numbers and the comma or hyphen.
11	Press Return. All filters associated with the specified frame type are modified and the Bridge config prompt is displayed.

Deleting All Protocol Filters For All Frame Types

To delete all protocol filters associated with all frame types, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **delete protocol-filter all**.
2	Press Return. The following message is displayed: `Modify default protocol filters for DSAP (Yes or No)? [Yes]:`
3	If you want to modify the default protocol filters associated with all the DSAP (Ether or SNAP) protocol filters you are about to delete, enter **Yes**. If you do not want to modify the default protocol filters associated with all the DSAP (Ether or SNAP) protocol filters you are about to delete, enter **No**.
4	Press Return. If you entered **Yes**, go to step 5. If you entered **No**, go to step 7.
5	The following message is displayed: `Allowed port numbers ("None" or "All") [0-254]?` The previously configured ports are the default if you are modifying an existing default protocol filter.
6	Enter a list of the bridge output ports from which you want frames forwarded based on the specified protocol. (The frames are filtered from those ports not entered.) Enter **None** if you want the frames filtered from all ports. Enter **all** if you want the frames forwarded on all ports. You can list the forwarding ports individually by separating each with a comma (for example, **0,1,2,3,4,5**) or you can enter a range of ports by separating the first and last port numbers in the range with a hyphen (for example, **0-5**). You can also combine a list of individual entries with a range of entries (for example, **0-4,6,7**). Spaces are not permitted between port numbers and the comma or hyphen.

Step	Action
7	Press Return. When you have modified all the protocol filters for a given frame type, you can modify protocol filters for the next frame type (dsap, ether, or snap). A message similar to the following is displayed: `Modify default protocol filters for ETHER (Yes or No)? [Yes]:` If you want to modify additional protocol filters, enter **yes** and go to step 3. If there are no additional default protocol filters to modify, go to step 8.
8	All protocol filters associated with all frame types are deleted and the Bridge config prompt is displayed.

Creating and Modifying Default Protocol Filters

Default protocol filters forward (or discard) all frames of a particular type (Ethernet, SNAP, or DSAP) from one or more bridge ports. They act on only those frames that conform to protocols not already specified as described in the Identifying the Protocol and Allowed Ports section.

To create or modify a default protocol filter, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **set default-protocol-filter**.
2	Press Return. The following message is displayed: `Protocol type [DSAP]?`
3	Enter one of the following types of frames for which you want to specify a default protocol: • **ether** (Ethernet-II) • **snap** • **dsap** DSAP is the default.
4	Press Return. `Allowed port numbers ("None" or "All") [0-254]?` The default is all ports if you are creating a new filter. The previously configured ports are the default if you are modifying an existing filter.

Step	Action
5	Enter a list of the bridge output ports from which you want frames forwarded based on the specified protocol. (The frames are filtered from those ports not entered.) Enter **None** if you want the frames filtered from all ports. Enter **all** if you want the frames forwarded on all ports. You can list the forwarding ports individually by separating each with a comma (for example, **0,1,2,3,4,5**) or you can enter a range of ports by separating the first and last port numbers in the range with a hyphen (for example, **0-5**). You can also combine a list of individual entries with a range of entries (for example, **0-4,6,7**). Spaces are not permitted between port numbers and the comma or hyphen.
6	Press Return. The default protocol filter is created or modified and the `BRIDGE config>` prompt is displayed.

Example

You can configure a module so that Ethernet frames conforming to the AppleTalk Phase 1 protocol are forwarded. You do so by creating a discrete protocol filter. Refer to the Creating and Modifying Protocol Filters section for information about how to do so. You can then use a default filter to discard all other Ethernet frames of any other protocol type such as IP, ARP, DECnet, and so on. Refer to Table 7-1 for a list of common Ethernet protocol types that can be filtered in this way.

Deleting Default Protocol Filters

You can delete previously configured default protocol filters from the module. When you delete a default protocol filter, all protocols associated with the specified frame type are then forwarded on all ports.

Deleting a default protocol filter may increase the amount of traffic over specific segments of a network and may, therefore, reduce network capacity and performance.

To delete a default protocol filter, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **delete default-protocol-filter**.
2	Press Return. The following message is displayed: `Protocol type [DSAP]?`
3	Enter one of the following frame types for which you want to delete all default protocol filters: • **ether** (Ethernet-II) • **snap** • **dsap** DSAP is the default.
4	Press Return. The default protocol filter is deleted and the Bridge config prompt is displayed.

Configuring the Spanning Tree Protocol

The Spanning Tree Protocol (STP) is used to detect and break circular traffic patterns, or loops. Loops can cause exponential traffic replication resulting in severe network congestion. The module implements the IEEE 802.1D Spanning Tree Protocol. The module does not interoperate with DEC LANbridge 100 STP.

STP eliminates loops by selecting one of the redundant bridges as the primary or root bridge, and maintaining secondary bridges as backups. The root bridge is selected, in part, based on a priority value you can assign to each bridge. STP then selects a root port on each secondary bridge. The root port is selected based on the relative priority of each port, and which port provides access to the root bridge at the least cost. The bridge then enables all root ports for forwarding, and disables other ports to prevent loops.

The Spanning Tree Protocol algorithm runs automatically for each VSD you create. Therefore, multiple spanning trees are supported on the bridge. The STP parameters you set, as described in this section, affect all instances of STP. You cannot configure different values for each instance of STP. Refer to Chapter 9 for information about Virtual LANs (VLANs).

You can enable and disable STP on a port. You can also set certain parameters that influence selection of the root bridge, the root port, and the frequency with which changes in network topology are detected. These options are discussed in the following sections.

Note

The concepts presented in this section are simplified for the purpose of providing a general introduction. Refer to the *DIGITAL VNswitch 900 Series Technical Overview* for a more detailed discussion of STP concepts.

Influencing Selection of the Root Bridge

The root bridge is selected based on a value that is the combination of a bridge's address and a number you can assign that is the bridge's priority. A lower number for bridge priority makes it likely that the bridge is selected as the root.

To set the bridge's priority, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **set bridge priority**.
2	Press Return. The following message is displayed: `Bridge-Priority [32768]?`
3	Enter a number from 0 to 65535 for the bridge priority. The lower the number, the more likely the bridge is selected as the root. The factory default bridge priority is 32768. If the factory default was modified, the default is the most recent setting.
4	Press Return. The number entered is set as the bridge's priority and the `BRIDGE config>` prompt is displayed.

Influencing Selection of the Root Port

The root port on a bridge is selected based on which port provides access to the root bridge at the lowest Path Cost and the relative Priority of each port.

You can choose either to set the Path Cost for a port manually through the CLI or allow STP to do so automatically. If the spanning tree sets the Path Cost, the value it assigns is based on the line speed associated with the port. The higher the line speed, the lower the assigned cost. However, you can override this value by manually entering a value that weights the Path Cost in favor of a particular port. The lower a port's Path Cost, the more likely it is to be selected as the root port. You may want to set a high Path Cost for a port if, for example, the LAN to which the port is connected has a low bandwidth.

Setting port priorities also affects which port is selected as the bridge's root port when a bridge has two ports connected in a loop. The port having the lowest assigned number is more likely to be selected as the root port. For example, if port 3 is assigned a Priority of 1, and port 6 is assigned a Priority of 2, port 3 is likely to be selected as the root port by STP. If more than one port has the same Priority, the port that has the lowest port number is used.

To set the Path Cost and Priority for one or more ports on a module, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **set stp port**.
2	Press Return. The following message is displayed: `Port Number [0]?`
3	Enter the number of the port for which you want to set Path Cost and Priority. The default is port 0.
4	Press Return. The following message is displayed: `Port Path-cost (0 for default) [0]?`
5	If you want STP to calculate the Path Cost for the port, enter the default value of `0`. If you want to enter your own value, enter a number from 1 through 65535. The lower the value entered, the more likely the port will be selected as the root port.
6	Press Return. The following message is displayed: `Port Priority [128]?`
7	Enter a number from 0 through 255. The lower the number entered, the more likely the port will be selected as the root port.
8	Press Return. The port's Path Cost and Priority are set and the `BRIDGE config>` prompt is displayed.

Detecting Changes in Network Topology

All bridges periodically transmit Hello Messages (Configuration Bridge Protocol Data Units — BPDUs) on their subset of designated ports. These messages, which include such information as the Path Cost of the port from which the message is transmitted, are initially used to determine the network topology and set up a spanning tree. When the spanning tree is established, Hello Messages are then used to detect changes in network topology by comparing the latest BPDU received on a port with the best BPDU previously received. (The best BPDU is, in part, based on Path Cost.) If a change in topology is detected, STP recomputes the spanning tree.

You can fine-tune the ability of STP to detect changes in topology by performing the following tasks:

- Adjusting the frequency with which bridges transmit Hello Messages
- Fine-tuning the ability to detect a failed bridge or link
- Avoiding loops

Caution

It is recommended that you alter the STP default settings associated with these tasks *only* if you fully understand the effect the change will have on the bridge network.

Adjusting Hello Message Frequency

You can configure the frequency, in seconds, with which bridges transmit Hello Messages to check for changes in network topology. The parameter used to configure this value is called the Bridge Hello Time. The greater the frequency (the lower the number of seconds), the sooner changes in topology are detected. The lower the frequency (the greater the number of seconds), the lower the overhead associated with detecting changes.

Refer to the Setting Bridge Hello Time, Bridge Max Age, and Bridge Forward Delay section for information about how to configure the Bridge Hello Time.

Detecting a Failed Bridge or Link

You can also fine-tune STP's ability to detect a change in topology that is the result of a failed bridge or link. This is accomplished by setting or modifying the Bridge Max Age. If the time since a bridge last received a Hello Message on a port exceeds the Bridge Max Age setting, perhaps the result of a failed link, the bridge recalculates the root, path cost, and root port.

Note

Although you can configure each bridge in a spanning tree with a different value for Bridge Max Age, the value configured on the root bridge is used by all bridges in the spanning tree. The values configured on non-root bridges are used only if a non-root bridge subsequently becomes root.

The lower the Bridge Max Age value, the earlier a failed bridge or link may be detected. However, if the Bridge Max Age time is exceeded due to a normal drop in network activity and not because of a link or bridge failure, the result may be failure to compute a correct spanning tree. This may cause forwarding loops and severe network congestion.

Refer to the Setting Bridge Hello Time, Bridge Max Age, and Bridge Forward Delay section for information about how to configure the Bridge Max Age.

Loop Avoidance

The Bridge Forward Delay parameter is used to prevent temporary forwarding loops between bridges. If a temporary forwarding loop occurs, it can cause severe network congestion. The Bridge Forward Delay must be at least twice the maximum amount of time it takes for data to traverse the network.

Refer to the Setting Bridge Hello Time, Bridge Max Age, and Bridge Forward Delay section for information about how to configure the Bridge Forward Delay.

Setting Bridge Hello Time, Bridge Max Age, and Bridge Forward Delay

There is a functional relationship among Bridge Hello Time, Bridge Max Age, and Bridge Forward Delay. That relationship requires that the values set for the three parameters conform to the following algorithm:

(2) X (Bridge Forward Delay – 1 second) $\geq$ Bridge Max Age

and

Bridge Max Age $\geq$ (2) X (Bridge Hello Time + 1 second

To set or modify Bridge Hello Time, Bridge Max Age, and Bridge Forward Delay, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **set stp bridge**.
2	Press Return. The following message is displayed: `Bridge-Max-Age [20]?`
3	Enter a value for the maximum amount of time a bridge port waits to receive a Hello Message before the bridge recalculates the root, path cost, and root port. The value can be from 6 through 40. The default is 20.
4	Press Return. The following message is displayed: `Bridge-Hello-Time [2]?`

Step	Action
5	Enter the frequency with which you want the bridge port to transmit Hello Messages. The value can be from 1 through 10 seconds. The default is 2 seconds.
6	Press Return. The following message is displayed: `Bridge-Forward-Delay [15]?`
7	Enter the number of seconds you want a bridge to wait before allowing disabled bridge ports to transition to the forwarding state. The value can be from 4 through 30 seconds. The default is 15 seconds.
8	Press Return. The values you entered are set and the `BRIDGE config>` prompt is displayed. If the entered parameters do not conform to the algorithm described at the beginning of the Setting Bridge Hello Time, Bridge Max Age, and Bridge Forward Delay section, an error message is displayed.

Enabling and Disabling STP

You can disable and reenable STP on a specific port, if the port currently exists. STP is automatically enabled (the default) on all bridge ports at installation.

Caution

DIGITAL recommends you keep STP enabled on all ports. Disabling STP may result in loops and severe network congestion.

Disabling STP

To disable STP on a specific port, perform the following steps. Disabling STP on a port causes the port to transition to the forwarding state immediately.

Step	Action
1	At the `BRIDGE config>` prompt, enter **disable stp**.
2	Press Return. The following message is displayed: `Port Number [0]?`
3	Enter the number of the bridge port for which you want to disable STP.

Step	Action
4	Press Return. STP is disabled on the specified port and the `BRIDGE config>` prompt is displayed.

Enabling STP

To enable STP on a specific port, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **enable stp**.
2	Press Return. The following message is displayed: `Port Number [0]?`
3	Enter the number of the bridge port for which you want to enable STP.
4	Press Return. STP is enabled on the specified port and the `BRIDGE config>` prompt is displayed.

Forwarding Using Only Manually Created Address Filters

You can configure the module to forward frames using only manually created address filters. Doing so allows you to strictly control traffic through selected ports and can provide an additional level of security to the desired subnetworks.

For example, you may want to operate a port securely so that only one system is allowed to source and sink traffic on that port. To do so, you enable manual mode on the port. You then create an address filter entry (permanent or static) for that system's MAC address, specifying only that port in the filter's allowed port map. In addition, if you want multicast or broadcast frames to be forwarded to that port, you must create an address filter for each such address, specifiying at least that port in the allowed port map.

You configure the use of only manually created filters by enabling manual mode on selected ports. When manual mode is enabled, the port's forwarding table that contains learned addresses is purged, and new addresses are not learned. However, you can still configure new MAC address filters manually. (Refer to the Configuring Permanent Address Filters section for information about creating address filters manually.) The addresses and locations of other network devices are relearned if manual mode is later disabled.

Enabling Manual Mode

To enable manual mode, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **enable manual-mode**.
2	Press Return. The following message is displayed: `Port Number [0]?` The value displayed for port number is based on the ports that are currently enabled.
3	Enter the number of the port on which you want to enable manual mode (disable bridge learning).
4	Press Return. Manual mode is enabled on the specified port and the `BRIDGE config>` prompt is displayed.
5	Repeat steps 1 through 4 for each port on which you want to enable manual mode.

Disabling Manual Mode

To disable manual mode (enable bridge learning), perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **disable manual-mode**.
2	Press Return. The following message is displayed: `Port numbers [0-254]?` The value displayed for port number is based on the ports that are currently enabled or disabled. For example, because you do not need to disable ports that are already disabled, the enable command displays only the ports that are enabled.
3	Enter the number of the port for which you want to disable manual mode (enable bridge learning).
4	Press Return. Manual mode is disabled on the specified port and the `BRIDGE config>` prompt is displayed.
5	Repeat steps 1 through 4 for each port on which you want to disable manual mode.

Enabling and Disabling a Bridge Port

You can enable or disable selected bridge ports, if the ports are already added. You may want to disable a bridge port to help isolate network problems, for example. Disabling a port turns off bridging services on the port but does not disable its associated logical interface. Although a disabled port does not forward frames, it continues to receive certain STP packets. All bridge ports are enabled (the default) at startup.

Enabling a Port

To enable a bridge port, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **enable port**.
2	Press Return. The following message is displayed: `Port Number [0]?`
3	Enter the number of the bridge port you want to enable.
4	Press Return. The selected port is enabled and the `BRIDGE config>` prompt is displayed.

Disabling a Port

To disable a bridge port, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **disable port**.
2	Press Return. The following message is displayed: `Port Number [0]?`
3	Enter the number of the bridge port you want to disable.
4	Press Return. The selected port is disabled and the `BRIDGE config>` prompt is displayed.

Bridging Ethernet and FDDI Networks

When bridging an Ethernet LAN to an FDDI backbone, frames must be repackaged to resolve differences in frame formats between the two networks. GIGAswitch GS2000 line cards repackage the frames automatically using standard encapsulation and translation. They also implement IP fragmentation automatically. However, you may need to enable or disable IPX translation on a bridge if the bridge is to handle datagrams transmitted by network nodes using IPX protocols.

IP Fragmentation

IP fragmentation is used to "cut up" (fragment) large data packets into frame sizes that can be handled by Ethernet or Fast Ethernet LAN segments, or an Ethernet ATM Emulated LAN or Bridge Tunnel. This may occur, for example, if IP datagrams traverse multiple LAN segments to reach their destination. If the first LAN segment the datagram enters is an FDDI or ATM segment, larger IP datagrams are accommodated by FDDI and ATM frames. If subsequent hops include an Ethernet or Fast Ethernet LAN segment, however, the FDDI or ATM frames may then be too large for the smaller Ethernet frames. IP fragmentation is used to resolve this incompatibility. Destination devices reassemble the fragmented packets when the packets are received. You cannot disable IP fragmentation.

Condition Under Which Packets Are Discarded

IP packets cannot be fragmented if their Don't Fragment Bit (DF Bit) is set. If a packet's DF Bit is set, the packet is discarded and an ICMP message is sent notifying the source node of the condition.

Note

An ICMP message is sent only if an IP address has been configured.

Enabling and Disabling IPX Translation

Internetwork Packet Exchange (IPX) is a peer-to-peer networking protocol for Novell NetWare. You may need to enable IPX translation on a module under the following circumstances:

- Some nodes on your network are set to generate and receive IPX datagrams in Raw Ethernet frame format
- Some nodes in the same NetWare network number as above are directly connected to an FDDI LAN

Translation is necessary under the above conditions because the FDDI-attached NetWare node cannot recognize raw frames, while the Ethernet-attached nodes are configured to recognize only raw frames. For all these nodes to communicate, the modules can be configured to translate between raw format (on the Ethernet LAN) and SNAP format (on the FDDI LAN).

Note

IPX translation incurs extra overhead when forwarding frames. If possible, reconfigure the Ethernet-attached nodes in this scenario to use SNAP encapsulation so that IPX translation is not needed. Note also that if all the nodes in the network number use raw encapsulation, then IPX translation is not needed because Raw frames can be sent over the FDDI network.

Translation Rules

To determine whether IPX translation should be enabled or disabled on a module, you must understand the translation rules listed in Table 7-4. The examples in the table refer to Figure 7-1.

Table 7-4: IPX Translation Rules

If. . .	And. . .	Then. . .
The module receives a Raw Ethernet frame from an Ethernet LAN (switch 1)	IPX translation is *enabled* on the module	The Raw Ethernet frames are translated and are output to the FDDI backbone as SNAP frames.
The module receives a Raw Ethernet frame from an Ethernet LAN (switch 1)	IPX translation is *disabled* on the module	The Raw Ethernet frames are *not* translated and are output to the FDDI backbone as Raw Ethernet frames.
The module receives a SNAP frame from an FDDI backbone (switch 2)	IPX translation is *enabled* on the module	The SNAP frames are translated and are output to the Ethernet LAN (LAN B) as Raw Ethernet frames.
The module receives a SNAP frame from an FDDI backbone (switch 2)	IPX translation is *disabled* on the module	The SNAP frames are *not* translated to the Raw Ethernet frame type and are output to the Ethernet LAN (LAN B) as SNAP frames.

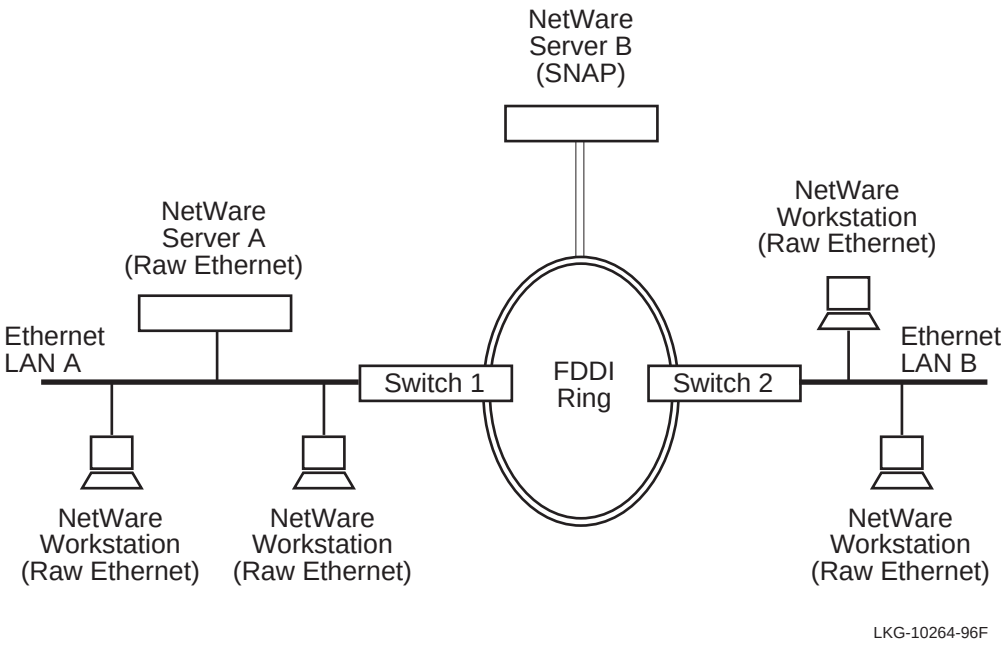
Examples

The following examples show how you can use the translation rules to accommodate several network configurations. Figure 7-1 is used to illustrate the examples.

- NetWare server A on LAN A must exchange data with the Novell workstations on LAN B. Because the nodes on both LAN A and B generate and receive only Raw Ethernet frames, IPX translation does not need to be enabled on either switch 1 or switch 2.
- NetWare server B, directly connected to the FDDI backbone, must exchange data with the Novell workstations on LAN B. Because the server is set to handle SNAP frames, it can place data on the backbone without modification. However, in order for the workstations on LAN B to receive the SNAP frames, the frames must be translated back to Raw Ethernet format by switch 2. IPX translation must, therefore, be enabled on switch 2.

  Conversely, in order for the workstations on LAN B to place their Raw Ethernet frames on the FDDI backbone, switch 2 must have IPX translation enabled. The module can then translate the frames between raw format and SNAP format.

Figure 7-1: Modules Requiring IPX Translation



NetWare Ethernet Frame Type Options

The NetWare operating system can be set to encapsulate IPX datagrams into one of several Ethernet frame types, two of which are Raw Ethernet and SNAP. What frame type you can set on the NetWare node varies, depending on the type of network to which the node is connected:

If. . .	Then. . .
The NetWare node is directly connected to an Ethernet LAN	The NetWare operating system can be configured to encapsulate IPX datagrams into any one of the following four Ethernet frame types: • Ethernet-II • Raw Ethernet • Subnetwork Access Protocol (SNAP) • Destination Service Access Point (DSAP)

If. . .	Then. . .
The NetWare node is directly connected to an FDDI backbone	The NetWare operating system can be configured to encapsulate IPX datagrams into any one of the following two Ethernet frame types: • Subnetwork Access Protocol (SNAP) • Destination Service Access Point (DSAP)

Note

DIGITAL recommends that IPX network nodes, connected directly to Ethernet LANs, use the Ethernet-II frame format for full connectivity of IPX stations across Ethernet networks and FDDI bridged networks. If Ethernet-II is used by all IPX network nodes connected to an Ethernet LAN, IPX translation does not need to be enabled on any module.

Enabling IPX Translation

To enable IPX translation, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **enable ipx-translation**.
2	Press Return. IPX translation is enabled on the module.

Disabling IPX Translation

To disable IPX translation, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **disable ipx-translation**.
2	Press Return. IPX translation is disabled on the module.

Auto-Testing of Ports Inactive for Extended Periods

A failure can sometimes cause a port to loose the ability to receive frames although it can still transmit frames. STP is unable to detect this condition. Such a failure can result in a forwarding loop and severe network congestion.

You can set the maximum amount of time a port operates without receiving a frame, although it may be transmitting frames. This setting, referred to as the No Frame Interval, is expressed in seconds and is applied to all ports on a module. If this time is exceeded, the module tests the port for correct operation. If the self-test determines a problem exists, the port and STP are disabled. (Refer to the Displaying Current Bridge Configuration Parameters section for information about displaying a change in port and STP status. Refer to Chapter 5 for information about displaying a change in the status of the logical interface.) All three conditions are logged to the Event Logging System. If no problem is found during the self-test, the No Frame Interval clock is restarted.

To set or modify the No Frame Interval, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **set no-frame-interval [*interval in seconds*]**, where ***interval in seconds*** is the maximum number of seconds the port is to remain inactive (no frames are received by, or transmitted from, the port).
2	Enter the maximum number of seconds (from **0** to **1000**) the port is to remain inactive before a test is run. The default is **300** seconds.
3	Press Return. The No Frame Interval you entered is set for all ports on the module.

Setting the Time That Unused Addresses Are Retained

A port's forwarding database stores Dynamic (learned) MAC addresses for a predetermined period of time, referred to as the Aging Time. If the module does not receive a datagram from the device associated with that address within the period specified by the Aging Time, the address is "unlearned" by the port. If the module subsequently receives data with that destination address, the data is forwarded through all ports, except the one on which it was received. This process is referred to as "flooding."

You can set or modify the Aging Time for all ports on a module. To do so, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **set age**.
2	Press Return. The following message is displayed: `Seconds [300] ?`
3	Enter the Aging Time in seconds (from 10 through 1,000,000). The default is 300 seconds.
4	Press Return. The Aging Time is set.

Displaying Current Bridge Configuration Parameters

You can display specific information about various bridge configuration settings. To display configuration information, perform the following steps:

Step	Action
1	At the `BRIDGE config>` prompt, enter **list *configuration***, where ***configuration*** is the command you must enter to display the desired information. Refer to Table 7-5 for a list of commands and for a description of the information that is displayed when you enter the command.
2	Press Return. The desired information and a new `BRIDGE config>` prompt is displayed.

Example

BRIDGE config>**list bridge**

```
                      Transparent Bridge Configuration

Bridge:                Enabled              Bridge Behaviour:  STB
Rate Limiting:         Disabled             Rate Limit value:  400
Raw 802.3 IPX Trans:   Disabled             No Frame Interval: 300

                         Bridge Database Information

Ageing Time:           300                 Entries in Perm Database: 0
Number of Rehashes:    0

                       Spanning Tree Protocol Information

Bridge Priority:       32768/0x8000

                                Port Information

Number of ports: 18

Port   Interface   State      Behaviour    STP        Manual Mode
   0   0           Enabled    STB Only     Enabled    Disabled
   1   1           Enabled    STB Only     Enabled    Disabled
   2   2           Enabled    STB Only     Enabled    Disabled
   3   3           Enabled    STB Only     Enabled    Disabled
   4   4           Enabled    STB Only     Enabled    Disabled
   5   5           Enabled    STB Only     Enabled    Disabled
   6   6           Enabled    STB Only     Enabled    Disabled
   7   7           Enabled    STB Only     Enabled    Disabled
   8   8           Enabled    STB Only     Enabled    Disabled
   9   9           Enabled    STB Only     Enabled    Disabled
  10   10          Enabled    STB Only     Enabled    Disabled
  11   11          Enabled    STB Only     Enabled    Disabled
  12   12          Enabled    STB Only     Enabled    Disabled
  13   13          Enabled    STB Only     Enabled    Disabled
  14   14          Enabled    STB Only     Enabled    Disabled
  15   15          Enabled    STB Only     Enabled    Disabled
  16   16          Enabled    STB Only     Enabled    Disabled
  17   17          Enabled    STB Only     Enabled    Disabled
```

Table 7-5: List Command Options and Descriptions

Command	Description
address	The following information is listed for any permanent or static address you specify: • Whether Rate Limiting is enabled for a specific MAC address • The address type (permanent, static, dynamic, and so on) for the MAC address • The allowed (forwarding) ports for the address
bridge	The following information is listed about the transparent bridge: • Bridge state (enabled or disabled) • Bridge behavior (Spanning Tree Bridge only) • Rate limiting state and value • IPX translation state • No Frame Interval • Ageing Time • Number of entries in permanent database • Number of rehashes (the number of times the module's programmable randomizer function was reprogrammed to more efficiently access the address and protocol databases used by the lookup engine) • Bridge priority and STP standard • Number of ports, and a list of port numbers and their associated interface numbers • Port states and whether STP and Manual Mode is enabled on each port
default-protocol-filter	A list of default protocol filters in use and a list of their forwarding ports

Command	Description
port	The following information is listed for the port you specify: • ID and state of the port • Whether STP is enabled • Type of functionality supported by the port (Transparent Bridging only) • Whether Manual Mode is enabled • The number of the logical interface associated with the port, and its type (Ethernet, FDDI, and so on) • Path Cost of the port
protocol-filter	The following information is listed about protocol filters: • List of protocol filter classes in use • List of protocol filter classes in use, including type • Whether Rate Limiting is enabled • The ports on which the protocol is forwarded
range	The following information is listed for each address within the range of permanent or static MAC addresses you specify: • Whether Rate Limiting is enabled • The address type (permanent, static, dynamic, and so on) for the range of MAC addresses • The allowed ports for the addresses
stp	The following information is listed about STP: • STP's Bridge Max Age time • STP's Bridge Hello Time • STP's Bridge Forward Delay

Duplicate MAC Addresses on Separate VSDs

In most networks, the same MAC address is not expected to appear as a Source Address (SA) on more than one VLAN Secure Domain (VSD). Exceptions do exist, for example:

- A DECnet router can be attached to multiple VSDs to perform routing between those VSDs. DECnet routers force a phase IV-style derived MAC address on all the router's interfaces. This MAC address then appears as a duplicate on each VSD where the router has an interface.
- Sun systems with multiple interfaces use the same MAC address on all interfaces. However, you can configure these systems to use a unique MAC address on each interface.
- Any address can appear transiently as a duplicate if the address moves from one VSD to another.

The GIGAswitch GS2000 module learns the duplicate address on the port in the VSD where the address first appears. When you manually configure the duplicate MAC addresses, the GIGAswitch GS2000 module then properly forwards packets with the duplicate address as a DA on the VSD where it was learned and floods such packets on all other VSDs. Additionally, you can avoid the flooding behavior by configuring each duplicate MAC as a static or permanent address and setting its permitted ports to the ports on which that MAC address is reachable.

Configuring Duplicate MAC Addresses

Permanent Duplicate MAC Addresses

You configure permanent duplicate MAC addresses from the `BRIDGE config>` prompt. To set a permanent duplicate MAC address, perform the following tasks:

Step	Action
1	At the `BRIDGE config>` prompt, enter **set duplicated-address *address*** where ***address*** is the 12-digit MAC address. You can enter the address with or without hyphens separating the octets. For example, you can enter 11-22-33-44-55-66 or 112233445566.
2	Press Return. The following message is displayed: `Enter allowed ports, "None", or "All" []?`
3	Enter the ports on which this address is reachable.

Static Duplicate MAC Addresses

You configure a static duplicate MAC address from the `BRIDGE>` prompt. To set a static duplicate MAC address, perform the following tasks:

Step	Action
1	At the `BRIDGE>` prompt, enter **set duplicate-address *address*** where ***address*** is the 12-digit MAC address. You can enter the address with or without hyphens separating the octets. For example, you can enter 11-22-33-44-55-66 or 112233445566.
2	Press Return. The following message is displayed: `Enter allowed ports, "None", or "All" []?`
3	Enter the ports on which this address is reachable.

Displaying Duplicate MAC Addresses

To display all duplicate MAC addresses, perform the following tasks:

Step	Action
1	At the BRIDGE> prompt, enter **list database duplicate**
2	Press Return. The duplicate MAC address is displayed.

Example

```
BRIDGE>list database duplicate

                                  Last
                Multi    Rate                      Seen     Learned   Allowed
MAC Address Cast*  Limit Entry Type   Port   Port   Port(s)

08-00-09-00-4A-E8  N/A   Stat Dupl                 All
```

Deleting A Duplicate MAC Address

Permanent Duplicate MAC Addresses

To delete a permanent duplicate MAC address, perform the following tasks:

Step	Action
1	At the BRIDGE config> prompt, enter **delete address** ***address*** where ***address*** is the 12-digit MAC address. You can enter the address with or without hyphens separating the octets. For example, you can enter 11-22-33-44-55-66 or 112233445566.
2	Press Return. The duplicate MAC address is deleted.

Static Duplicate MAC Addresses

To delete a static duplicate MAC address, perform the following steps:

Step	Action
1	At the BRIDGE > prompt, enter **delete** ***address*** where ***address*** is the 12-digit MAC address. You can enter the address with or without hyphens separating the octets. For example, you can enter 11-22-33-44-55-66 or 112233445566.
2	Press Return. The duplicate MAC address is deleted.

Chapter 8

Monitoring the Transparent Bridge

Overview

Introduction

This chapter provides information about how to monitor the DIGITAL GIGAswitch GS2000 line card transparent bridge and how to configure static addresses. Monitoring includes the ability to display specific information about operational states, activity counters, and various bridge configuration settings. Static addresses you configure are stored in volatile RAM and are lost when the module is powered down or restarted. The addresses, therefore, must be relearned when power is again applied to the module.

In This Chapter

The following topics are covered in this chapter:

Accessing and Exiting the Bridge Monitor Prompt

You must access the Bridge monitor prompt to monitor bridge parameters and to configure static MAC addresses. The prompt is accessed from the Monitor prompt (`Monitor>`).

Accessing the Bridge Monitor Prompt

To access the Bridge monitor prompt, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **bridge**. **Example:** `Monitor>`**bridge**
2	Press Return. The Bridge monitor prompt (`BRIDGE>`) is displayed.

Exiting the Bridge Monitor Prompt

You exit the Bridge monitor prompt to return to the Monitor prompt.

Example

To return to the Monitor prompt (`Monitor>`) from the `BRIDGE>` prompt, enter **exit** and then press Return.

Monitoring the Bridge

You can monitor the bridge by displaying such information as operational states, activity counters, and various configuration settings associated with the following bridge software components:

- General bridging operation
- Bridge ports
- MAC address database
- Protocol filters
- Spanning Tree Protocol

General Bridging Operation

You can display the following types of information about the bridge:

- Operational states and port profile
- Aging parameters

To display a profile of the bridge's ports, aging parameters, and information about the operational state of various bridge functions such as IP fragmentation and rate limiting, perform the following steps:

Step	Action
1	At the `BRIDGE>` prompt, enter **list bridge**.
2	Press Return. The desired information and a new `BRIDGE>` prompt is displayed.

Example

This example lists the port's MAC address as MAC Address and the maximum frame size as Maximum PDU.

```
BRIDGE>list bridge
```

```
Bridge state:               Enabled
Multicast Rate Limiting:    Disabled (400 pps)
No Frame Interval:          300 seconds
Raw 802.3 IPX Trans:        Disabled
Bridge type:                STB
Ageing time:                300 seconds
Number of rehashes:         0
Number of static entries:   0
Number of dynamic entries:  0
Number of ports:            18

                 Operational                          Maximum
Port  Interface      State      MAC Address            PDU        Flags
   0  VNbus/0         Down       00-00-F8-63-08-01                 MD
   1  FDDI/1            Up       00-00-F8-63-08-02       4491      MD
   2  ALEC/2          Down       00-00-F8-63-08-03                 MD
   3  ALEC/3          Down       00-00-F8-63-08-04                 MD
   4  ALEC/4          Down       00-00-F8-63-08-05                 MD
   5  ALEC/5          Down       00-00-F8-63-08-06                 MD
   6  ALEC/6          Down       00-00-F8-63-08-07                 MD
   7  ALEC/7          Down       00-00-F8-63-08-08                 MD
   8  ALEC/8          Down       00-00-F8-63-08-09                 MD
   9  ALEC/9          Down       00-00-F8-63-08-0A                 MD
  10  ALEC/10         Down       00-00-F8-63-08-0B                 MD
  11  ALEC/11         Down       00-00-F8-63-08-0C                 MD
  12  ALEC/12         Down       00-00-F8-63-08-0D                 MD
  13  ALEC/13         Down       00-00-F8-63-08-0E                 MD
  14  ALEC/14         Down       00-00-F8-63-08-0F                 MD
  15  ALEC/15         Down       00-00-F8-63-08-10                 MD
  16  AFBT/16         Down       00-00-F8-63-08-11                 MD
  17  AEBT/17         Down       00-00-F8-63-08-12       1516      MD

Flags:  ME = Manual Mode Enabled, MD = Manual Mode Disabled
```

Port Activity Counters

To display information about port activity, perform the following steps:

Step	Action
1	At the BRIDGE> prompt, enter **list counters** ***ports***, where ***ports*** is the option you must enter to display the desired information. Refer to Table 8-1 for a list of options and for descriptions of the information that is displayed when you enter the option.
2	Press Return. The desired information and a new BRIDGE> prompt is displayed.

Table 8-1: List Counters Command Options and Descriptions

Command Option	Description
all-ports	Lists port activity counters for all ports.
port ***port-number***	Lists port activity counters for a specific port, where ***port-number*** is the number of the port for which you want to display information.
summary	Displays the sum of activity across all ports for each counter.

Example

```
BRIDGE>list counters summary

Port restarts:                                2
Total frames received by interfaces:      38412
IP frames fragmented:                         0
IP frames not fragmented:                     0
Frames submitted to bridging:             38412
Frames with unknown dest address:          1121
Frames causing learning transactions:        10
Dropped, source address filtering:            0
Dropped, dest address filtering:          32952
Dropped, protocol filtering:                  0
Dropped, address rate limiting:               0
Dropped, protocol rate limiting:              0
Dropped, no buffer available:                 0
Dropped, input queue overflow:                0
Dropped, source or dest port blocked:         0
Dropped, terminating queue overflow:          0
Dropped, fragmentation queue overflow:        0
Dropped, translate flood queue overflow:      0
Dropped, translation failure:                 0
Frames sent by bridging:                    228
Dropped, transmit queue overflow:             0
Dropped, transmit error:                      0
Dropped, too big to send on port:             0
```

Bridge Ports

You can display the following information for one or all bridge ports:

- Port ID
- Whether STP and Manual Mode are enabled
- Name and number of the interface associated with the port
- State of the port

If the port is a member of multiple VLAN Secure Domains (VSDs), the state of each VSD is listed, followed by the number and name of the VSD.

To display information about one or all bridge ports, perform the following steps:

Step	Action
1	At the BRIDGE> prompt, enter **list port** ***port-number***, where ***port-number*** is either the number of the port for which you want to display information or **all** for information about all ports.
2	Press Return. The desired information and a new BRIDGE> prompt is displayed.

Example

This example shows the types of information displayed for any port, other than the VNbus port.

```
BRIDGE>list port 1

Port Id (dec)    : 128: 1, (hex): 80-01
STP Participation: Enabled
Manual Mode      : Disabled
Assoc Interface  : 1 (FDDI/1)
Port State       : Forwarding
```

MAC Address Database

You can display the following information for each MAC address in the filtering database:

- Whether Rate Limiting is enabled for an address
- Whether the address is a multicast address (an asterisk indicates it is a multicast address)
- Address entry type (dynamic, reserved, registered, and so on)
- Last port on which the address was seen (dynamic, unicast static, and unicast permanent addresses only)
- Port on which the address was learned (dynamic, unicast static, and unicast permanent addresses only)
- Ports on which the address is allowed (permanent and static addresses only)

You can display this information selectively for addresses of a particular entry type (permanent, static, registered, and so on), for a range of addresses, or on a per-port basis.

To display information about selected portions of the database, perform the following steps:

Step	Action
1	At the `BRIDGE>` prompt, enter **list database** ***selected-information***, where ***selected-information*** is the option you must enter to display the desired information. Refer to Table 8-2 for a list of options and for descriptions of the type of information that is displayed when you enter the option.
2	Press Return. The desired information and a new `BRIDGE>` prompt is displayed.

Table 8-2: List Database Command Options and Descriptions

Command Option	Description
all	Lists information for all addresses associated with all ports.
dynamic	Lists information for all dynamic entries in the database.
local	Lists information for all registered entries in the database.
permanent	Lists information for all permanent entries in the database.
port	Lists information for all addresses associated with the specified port.
range	Lists information for all addresses within a specified range.
static	Lists information for all static entries in the database.

Example

BRIDGE>**list database local**

```
                                        Last
            Multi   Rate                Seen  Learned  Allowed
MAC Address  Cast*  Limit     Entry Type  Port  Port     Port(s)
00-00-F8-48-84-00   N/A       Registered                All
00-00-F8-48-84-02   N/A       Registered                1
00-00-F8-48-84-03   N/A       Registered                2
00-00-F8-48-84-04   N/A       Registered                3
00-00-F8-48-84-05   N/A       Registered                4
00-00-F8-48-84-06   N/A       Registered                5
00-00-F8-48-84-07   N/A       Registered                6
00-00-F8-48-84-08   N/A       Registered                7
00-00-F8-48-84-09   N/A       Registered                8
00-00-F8-48-84-0A   N/A       Registered                9
00-00-F8-48-84-0B   N/A       Registered                10
00-00-F8-48-84-0C   N/A       Registered                11
00-00-F8-48-84-0D   N/A       Registered                12
00-00-F8-48-84-0E   N/A       Registered                13
00-00-F8-48-84-0F   N/A       Registered                14
00-00-F8-48-84-10   N/A       Registered                15
00-00-F8-48-84-11   N/A       Registered                16
00-00-F8-48-84-12   N/A       Registered                17
01-00-5E-00-00-01*  Disabled  Registered                All
FF-FF-FF-FF-FF-FF*  Disabled  Registered                All
```

Protocol Filters

You can display the types of protocol filters and the default protocol filter applied to one or more ports. Protocol filtering is supported for the following frame types:

- Ethernet-II
- Subnetwork Access Protocol (SNAP)
- Destination Service Access Point (DSAP)

Displaying Protocol Filters

To display the protocol filters applied to one or more ports, perform the following steps:

Step	Action
1	At the BRIDGE> prompt, enter **list protocol-filter** ***frame-type***, where ***frame-type*** is the option you must enter to display the desired information. Refer to Table 8-3 for a list of options and for descriptions of the information that is displayed when you enter the command.

Step	Action
2	Press Return. The desired information and a new `BRIDGE>` prompt is displayed.

Table 8-3: List Protocol Filter Command Options and Descriptions

Command Option	Description
all	Lists all the protocol filters in use, and the ports on which the protocols are filtered. The filters are listed by frame type (Ethernet-II, SNAP, and SNAP) and hexadecimal value. Refer to Table 8-4, Table 8-5, and Table 8-6 for a list of hexadecimal values for common protocols.
ethertype ***protocol hexadecimal value***	Lists the ports on which the specified protocol is filtered, where ***protocol hexadecimal value*** is the hexadecimal value of the protocol in which you are interested. Refer to Table 8-4 for a list of hexadecimal values for common Ethernet-II protocols. Enter **0**, the default, to display all Ethernet-II protocols that are filtered.
dsap ***protocol hexadecimal value***	Lists the ports on which the specified protocol is filtered, where ***protocol hexadecimal value*** is the hexadecimal value of the protocol in which you are interested. Refer to Table 8-5 for a list of hexadecimal values for common DSAP (also referred to as SAP) protocols. Enter **100**, the default, to display all SAP (DSAP) protocols that are filtered.
snap ***protocol hexadecimal value***	Lists the ports on which the specified protocol is filtered, where ***protocol hexadecimal value*** is the 10-digit hexadecimal value of the protocol in which you are interested. Refer to Table 8-6 for a list of hexadecimal values for common SNAP protocols. Enter **00-00-00-00-00**, the default, to display all SNAP protocols that are filtered.

Example

```
BRIDGE>list protocol-filter all

Destination SAP        Rate Limit          Port(s)
01                     Disabled            2-3
Ethernet type          Rate Limit          Port(s)
0800                   Enabled             4-8
No SNAP filters configured
```

Table 8-4: Hexadecimal Values for Common Ethernet-II Protocols

Protocol	Hexadecimal Value
IP	0800
ARP	0806
CHAOS	0804
DECnet MOP Dump/Load	6000
DECnet MOP Remote Console	6002
DECnet	6003
DEC LAT	6004
DEC LAVC	6007
XNS	0600
Maintenance Packet Type	7030
Apollo Domain	8019 (Ethernet)
Novell NetWare IPX	8137 (Ethernet)
AppleTalk Phase 1	809B
AppleTalk ARP Phase 1	80F3
Loopback assistance	9000

Table 8-5: Hexadecimal Values for Common DSAP Protocols

Protocol	Hexadecimal Value
Banyan SAP	BC (used for only 802.5)
Novell IPX SAP	E0 (used for only 802.5)
NetBIOS SAP	F0
ISO Connectionless Internet	FE

Table 8-6: Hexadecimal Values for Common SNAP OUI/IP Protocols

Protocol	Ten-Digit Hexadecimal Value
AppleTalk Phase 2	08-00-07-80-9B
AppleTalk ARP Phase 2	00-00-00-80-F3
Proprietary AppleTalk Phase 1 for FDDI	00-00-93-00-02
Proprietary AppleTalk ARP Phase 1 for FDDI	00-00-93-00-03

Displaying Default Protocol Filters

You can also display default protocol filters used to filter *all* frames of a particular type from one or more output bridge ports, using protocols not already filtered as described above. For example, the module can be configured so that Ethernet frames conforming to the AppleTalk Phase 1 protocol are discarded, while a default filter is used to discard all Ethernet frames of any other protocol type such as IP, ARP, DECnet, and so on.

To display the default protocol filters applied to one or more ports, perform the following steps:

Step	Action
1	At the `BRIDGE>` prompt, enter **list default-protocol-filter**.
2	Press Return. The desired information and a new `BRIDGE>` prompt is displayed.

Example

```
BRIDGE>list default protocol-filter
Protocol        Allowed Ports

DSAP            0-254

ETHER           0-254

SNAP            0-254
```

Spanning Tree Protocol

You can display the following information about STP:

- Configuration parameters such as the Bridge Hello Time, port Priorities and Costs, the number of VSDs on a port, and whether STP is enabled on a port
- Activity data such as the number of times the network topology has changed and the number of BPDUs sent and received
- Whether STP is active on a given port
- Information about the designated root and designated bridge for each port

To display information about the Spanning Tree Protocol, perform the following steps:

Step	Action
1	At the BRIDGE> prompt, enter **list stp** ***option***, where ***option*** is the option you must enter to display the desired information. Refer to Table 8-7 for a list of options and for descriptions of the type of information that is displayed when you enter the option.
2	Press Return. The desired information and a new BRIDGE> prompt is displayed.

Example

BRIDGE>**list stp counters 1**

```
VSD  1  DEFAULT
Time since topology change (seconds):         6400
Topology changes:                                1
BPDUs received:                                  5
BPDUs sent:                                   3233

Port  Interface      BPDUs received  BPDU input overflow  Forward transitions
   0  VNbus/0                   0                    0                    0
   1  FDDI/1                    0                    0                    1
   2  ALEC/2                    0                    0                    0
   3  ALEC/3                    0                    0                    0
   4  ALEC/4                    0                    0                    0
   5  ALEC/5                    0                    0                    0
   6  ALEC/6                    0                    0                    0
   7  ALEC/7                    0                    0                    0
   8  ALEC/8                    0                    0                    0
   9  ALEC/9                    0                    0                    0
  10  ALEC/10                   0                    0                    0
  11  ALEC/11                   0                    0                    0
  12  ALEC/12                   0                    0                    0
  13  ALEC/13                   0                    0                    0
  14  ALEC/14                   0                    0                    0
  15  ALEC/15                   0                    0                    0
  16  AFBT/16                   0                    0                    0
  17  AEBT/17                   5                    0                    0
```

Table 8-7: List STP Command Options and Descriptions

Command Option	Description
configuration	Lists the following STP parameters configured on the module: • Bridge Maximum Age • Bridge Hello Time • Bridge Forward Delay • Hold Time (This value is fixed at one second and is not configurable, as required by IEEE standard 802.1D.) • Interface type and number, Priority, Cost, Administrative State, and number of VSDs on each port
counters ***vsd#-or-name***	Lists the following information about STP activity, where ***vsd#-or-name*** is the number or name of the VSD for which you want the information displayed. If no number or name is specified, information for all VSDs is displayed. • Time, in seconds, since the current topology change within the VSD was detected. This value is zero when there is no topology change in effect. • Number of changes in network topology within the VSD since the VSD was created • Number of BPDUs received and sent by the VSD • Number of BPDUs received, BPDU input overflow, and forward transitions for each port in the VSD

Command Option	Description
state ***vsd#-or-name***	Lists the following information about STP activity, where ***vsd#-or-name*** is the number or name of the VSD for which you want the information displayed. If no number or name is specified, information for all VSDs is displayed. • ID (a combination of the bridge priority and address) for the instance of STP in the VSD • ID (a combination of the bridge priority and address) of the root bridge in the VSD's spanning tree • Path Cost of the root port in the VSD's spanning tree • Which port is the root port on the VSD's spanning tree • Current Bridge Max Age, Hello Time, and Forward delay dictated by the root bridge and used by all bridges in the VSD's spanning tree • Whether the VSD's spanning tree has detected (True or False) a topology change • Whether the root bridge has confirmed (True or False) a topology change in the VSD's spanning tree • State (Forwarding, Blocking, Listening, Learning, or Down) of each port in the VSD
tree ***vsd#-or-name***	Lists the following information for each port in the VSD's spanning tree, where ***vsd#-or-name*** is the number or name of the VSD for which you want the information displayed. If no number or name is specified, information for all VSDs is displayed. • Associated interface number • Designated root • Designated cost • Designated bridge • Designated port

Configuring a MAC Address As a Static Entry

This section discusses how to add MAC address filters as static entries. This section also describes how to modify and delete static entries. Because static addresses are stored in volatile RAM and are lost when the module is powered down or restarted, you may find the ability to add static entries to be most useful when trying to isolate network problems. (Refer to Chapter 1 for information about volatile RAM.) Static entries are not affected by address Aging Time. (Refer to Chapter 7 for information about address aging.)

The process of filtering network traffic is used to reduce the amount of unnecessary traffic over specific segments of a network, thereby maximizing network capacity and performance. It can also be used to restrict the distribution of sensitive information to specific locations. You can configure the module to selectively filter or forward packets it receives, based on their MAC addresses and protocol types.

You configure a filter by specifying a set of ports that are allowed for a given MAC address. The address can be an individual, multicast, or broadcast address. If a packet has a source or destination MAC address that is listed in the filter, the packet is allowed on the specified set of ports. If the address is not listed in the filter, the packet is dropped (filtered).

Source Address Filtering

A packet received on an input port is dropped (filtered) if the source address is listed in a filter and the input port is not one of the allowed ports. In addition, the source address is not learned.

If the input port is one of the allowed ports, the packet is a candidate for forwarding, based on the behavior of destination address filtering and protocol filtering. (Refer to Chapter 5 for information about protocol filtering.)

Destination Address Filtering

A packet about to be placed on an output port is forwarded if the destination address is listed in a filter and the output port is one of the allowed ports. If the address was not previously learned, the packet is flooded to the subset of the allowed ports that are in the forwarding state.

Creating and Modifying a Static MAC Address Filter

To create or modify a static MAC address filter, perform the following tasks:

Task	Description
1	Identify the address to be filtered and the ports on which the address is allowed.
2	Enable or disable multicast rate limiting.

Identifying the Address and Allowed Ports

The addresses you specify when creating a filter are added to the module's static database (volatile RAM). To identify the allowed ports for an address, perform the following steps:

Step	Action
1	At the `BRIDGE>` prompt, enter **set static-address**. You can, alternatively, enter **set static-address *mac_address***, where ***mac_address*** is the 12-digit MAC address for which you want to create or modify a filter on the module. If you enter the command using this syntax, and go to step 4.
2	Press Return. The following message is displayed: `Address (in 12-digit hex) []?`
3	Enter the 12-digit MAC address for which you want to create or modify a static filter. You can enter the address with or without hyphens separating the octets. For example, you can enter **11-22-33-44-55-66** or **112233445566**.
4	Press Return. The following message is displayed: `Enter allowed ports ("None", or "All") []?` If you are modifying the forwarding ports for an existing address, the previously configured ports are the default.

Step	Action
5	Enter a list of the bridge ports to which you want the packet with the specified MAC address forwarded. (The packet is filtered from those ports not entered.) Enter **None** if you want the packet filtered from all ports. Enter **all** if you want the packet allowed on all ports. You can list the forwarding ports individually by separating each with a comma (for example, **0,1,2,3,4,5**) or you can enter a range of ports by separating the first and last port numbers in the range with a hyphen (for example, **0-5**). You can also combine a list of individual entries with a range of entries (for example, **0-4,6,7**). Spaces are not permitted between port numbers and the comma or hyphen.

6	Press Return.
	If the address is a unicast address, the address is set and the `BRIDGE>` prompt is displayed.
	If the address is a multicast address, the following message is displayed:
	`Enable Multicast Rate Limiting (Yes or No)? [No]:`
	Refer to the Enabling and Disabling Multicast Rate Limiting section.
	If the specified ports do not exist, the address is set for forwarding on the port but the port setting has no effect. A message similar to the following is displayed in addition to the Bridge config or rate limiting prompts, whichever is appropriate:
	`Warning, ports 9, 10 do not exist`

Enabling and Disabling Multicast Rate Limiting

Multicast rate limiting is used to minimize the effects of multicast storms. You can restrict multicast storms, consisting of packets that have a specific destination MAC address, to that segment of the network from which the packets are generated. You do so by setting the maximum number of those packets the module is to forward per second, and by enabling rate limiting.

Rate limiting is enabled on both a per-address basis and a module-wide basis. This section provides instructions about how to enable or disable rate limiting on a per static MAC address basis. Refer to Chapter 7 for information about setting the maximum number of packets per second and enabling or disabling rate limiting on a module-wide basis.

To enable or disable multicast rate limiting for the static address specified in the Identifying the Address and Allowed Ports section, perform the following steps:

Step	Action
1	Enter **Yes** to enable Multicast Rate Limiting. Enter **No** to disable Multicast Rate Limiting. **No** is the default unless it was previously enabled for the address.
2	Press Return. The selected filter is applied to the module and rate limiting is enabled or disabled, as specified.

Deleting Static MAC Address Filters

This section describes how to delete static MAC addresses that you, or another switch administrator, previously entered manually. (Refer to the Creating and Modifying a Static MAC Address Filter section.) Deleting an address filter removes the address from the forwarding database as well as its associated multicast rate limiting status.

Note

Permanent, registered, and reserved addresses cannot be deleted.

To delete a static MAC address, its filter, and its associated rate limiting records, perform the following steps:

Step	Action
1	At the `BRIDGE>` prompt, enter **delete mac_address**. You can, alternatively, enter **delete *address***, where ***address*** is the 12-digit MAC address you want to delete. If you enter the command using this syntax, and go to step 4.
2	Press Return. The following message is displayed: `Address (in 12-digit hex) []?`
3	Enter the 12-digit MAC address you want to delete.
4	Press Return. The specified address is deleted. If you entered an address that does not exist, the following message is displayed: `No entry found for this address.`

Chapter 9

Configuring Virtual LANs

Overview

Introduction

A VLAN is a group of bridge ports logically linked to define a LAN on one or more switches. This network configuration scheme enables you to configure a set of devices so they logically appear to be on the same LAN segment, although they may be physically on different segments. You can create a maximum of 32 VLANs per DIGITAL GIGAswitch GS2000 line card.

Assume, for example, that two of five members in a bank's loan department are located in different areas of a building. Further, the two individuals are using terminals that are physically connected to an ATM emulated LAN, while the other three workers' terminals are physically connected to a segment in an Ethernet LAN. You can configure the module software so that all five terminals are logically on the same LAN, thereby minimizing traffic from the loan department over those segments of the network outside the loan department's VLAN. The five terminals can be physically connected to either the same module or to two or more modules on the same or different switches. If any individual is later assigned to another department, the module software can be dynamically reconfigured so the user's terminal is no longer associated with the loan department's VLAN, but is associated with a different VLAN, if desired.

In This Chapter

The following topics are covered in this chapter:

VLAN Secure Domains

A VLAN Secure Domain (VSD) is a logical set of one or more VLANs that operates with one spanning tree. The resulting configuration is a set of distinct bridge ports isolated from other ports on the same module by blocking all unicast and multicast traffic between VSDs. The GIGAswitch GS2000 line cards presently support one VLAN per VSD, but the VSD concept provides for expanded support of multiple VLANs within a single VSD.

Default VSD

All bridge ports on a module are, by default, members of a default VSD. The default VSD is numbered VSD 1 and is assigned the name "DEFAULT." The number and name cannot be changed.

When more than one module is resident in a switch, all ports on all modules are, by default, members of the same (default) VSD. Ports that are members of the default VSD operate as a traditional bridge without VLANs. When you create a new VSD as described in the Creating VSDs section, the ports you assign as members of the new VSD are removed from the default VSD. Conversely, when a VSD is deleted, all ports that were members of the VSD automatically become members of the default VSD.

Spanning Tree Protocol Support

The Spanning Tree Protocol (STP) algorithm runs automatically for each VSD you create. Therefore, multiple spanning trees are supported on the bridge. STP inhibits loops in redundant bridges by assigning a redundant bridge as a backup.

Accessing and Exiting the VSD Configuration Prompt

You must access the VSD configuration prompt to create and manage VSDs and to display configuration information about VSDs.

Accessing the VSD Configuration Prompt

To access the VSD configuration prompt, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **vlans**.
2	Press Return. The `VSD Config>` prompt is displayed.

Exiting the VSD Configuration Prompt

You exit the VSD prompt to return to the Bridge configuration prompt. For example, to return to the Bridge configuration prompt (`Bridge Config>`) from the `VSD Config>` prompt, enter **exit** and then press Return.

Creating VSDs

How you create a VSD varies, depending on which of the following port groupings is planned:

- The VSD is composed of a port group located on a single module.
- The VSD includes ATM Emulated LANs or Bridge Tunnels.

You use the **create vsd** command to create a VSD, followed by one or more of the command options shown in Table 9-1.

Table 9-1: Create VSD Command Options

Command Option	Description
ports ***port-list***	The ***port-list*** is a list of the bridge ports you want to assign to the VSD. You can list the ports individually by separating each with a comma (for example, **1,2,3,4,5**) or you can enter a range of ports by separating the first and last port numbers in the range with a hyphen (for example, **1-5**). You can also combine a list of individual entries with a range of entries (for example, **1-4,6,7**). Spaces are not permitted between port numbers and the comma or hyphen. Assigning a port-list is optional.
name ***name***	The ***name*** is the name you want to assign to the VSD (**Math_dept**, for example). A name can be composed of up to 32 ASCII-printable characters, except a question mark (?), must not include spaces, and must contain at least one alphabetic character. The name assigned must be unique. You cannot create another VSD on the same module using the same name. Assigning a name to a VSD is optional.

VSDs Within a Single Module

You create a VSD within a single module by identifying those ports that are members of the VSD. The module then assigns a number to each VSD you create. The default VSD always retains the VSD number of 1, even if all ports are reassigned to newly created VSDs. You can also, optionally, assign a name to the VSD. Assigning a name (for example, **Math_dept**) to the VSD provides a way of more easily recognizing functional groupings of ports, rather than simply using the system-assigned VSD number.

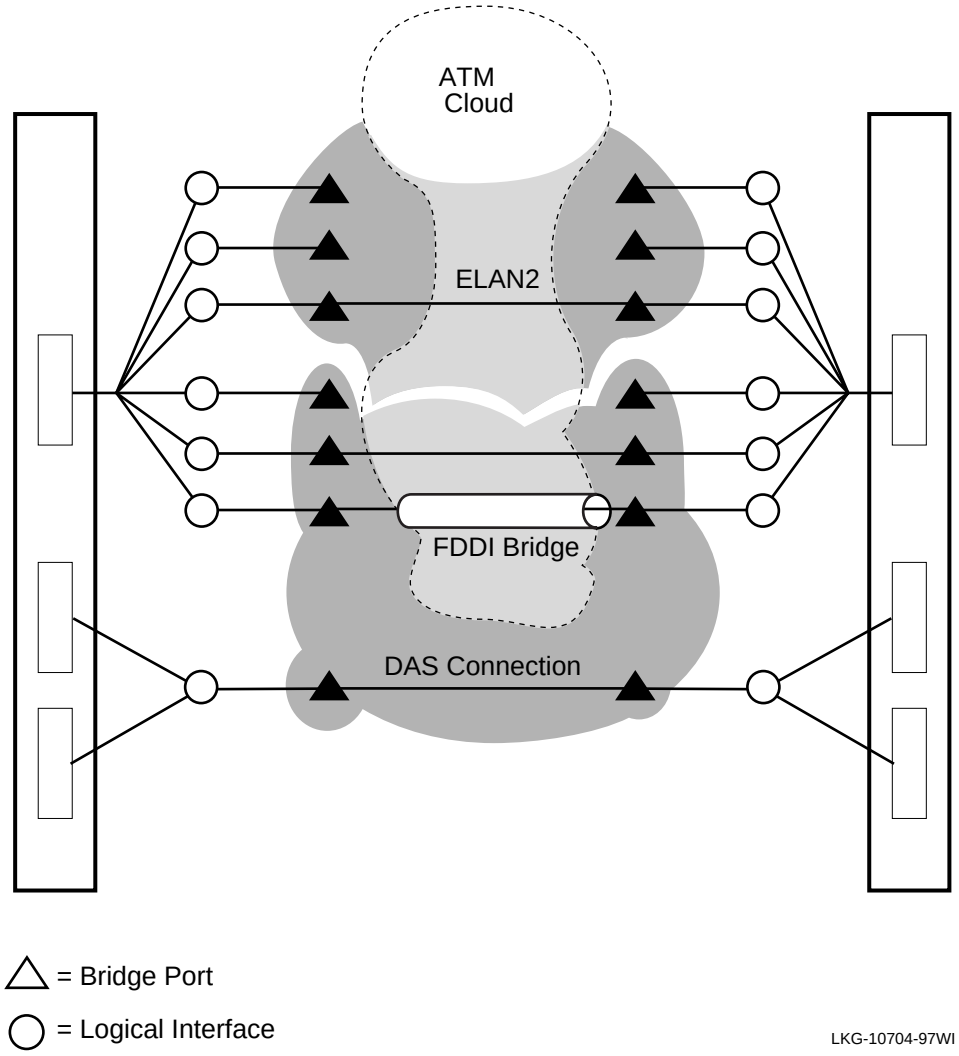
To create a VSD within a single module, perform the following steps:

Step	Action
1	Access the VSD configuration (`VSD Config>`) prompt. (Refer to the Accessing the VSD Configuration Prompt section for instructions.)
2	If you want to create a VSD without assigning it a name, enter **create vsd ports** ***port-list***. If you want to create a VSD and assign it a name, enter **create vsd ports** ***port-list*** **name** ***name***. Refer to Table 9-1 for a description of the options you can enter.
3	Press Return. The VSD you configured is created, including any name you assigned. A message is displayed showing the number assigned by the module to the VSD. You can view the list of assigned VSD numbers at any time. Refer to the Displaying Information About VSDs section for instructions about how to do so.

VSDs Across ATM Emulated LANs and Bridge Tunnels

You can configure VSDs across ATM ports located on different modules in different switches. You do so by providing a logical connection from the bridge port associated with an ATM LEC interface or ATM bridge tunnel that is a member of one module's VSD, to the bridge port associated with an ATM LEC interface or ATM bridge tunnel that is a member of a second module's VSD.

Figure 9-1: ATM ELAN and Bridge Tunnel VSDs



To create a VSD across ATM ports located on different modules in different switches, you must first configure either an ATM LEC logical interface or an ATM bridge tunnel logical interface. (Refer to Chapter 5 for information about how to do so.) You then create a VSD according to the instructions in the VSDs Within a Single Module section earlier in this chapter, including the LEC bridge port number or bridge tunnel port number that is to be included in the VSD.

Assume, for example, that two modules are resident on different GIGAswitch systems. An ELAN is configured from ATM LEC interface number 16 (port 16) on one module to ATM LEC interface number 4 (port 4) on the second module. (Refer to Chapter 5 for information about configuring ATM LEC and bridge tunnel logical interfaces.) The first module includes VSD 3 named **Math_dept**. The second module includes VSD 2, also named **Math_dept**. To make VSD 3 (**Math_dept**) on the first module and VSD 2 (**Math_dept**) on the second module members of the same VSD, ATM LEC port number 16 is added to VSD 3 on the first module, and ATM LEC port number 4 is added to VSD 2 on the second module.

Reserving VSDs

You reserve a VLAN Secure Domain by creating a VSD without assigning it ports. You may want to do so if, for example, certain work groups or portions of the network are not ready to go on line, while others are. You can later specify what ports are members of the VSD when the work group or network segments are ready.

To reserve a VLAN Secure Domain, create a VSD according to the instructions in this section, but do not use the **ports** ***port-list*** option to assign ports. The VSD you configure is created, including any name you assigned. A message is displayed showing the number assigned by the module to the VSD.

You can view a list of assigned VSD numbers and names at any time, and can later assign ports to the VSD. Refer to the Displaying Information About VSDs section for instructions about how to view VSD numbers and names. Refer to the Modifying VSDs section for instructions about how to add ports to reserved VSDs.

Modifying VSDs

You can modify a VSD's name or list of assigned ports. You may want to change assigned ports if, for example:

- Nodes logically associated with one VSD are moved and require new port assignments
- Some members of a work group or department associated with one VSD are moved and should be reassigned to another VSD

To modify a VSD's name or list of ports, perform the following steps:

Step	Action
1	Access the VSD configuration (`VSD Config>`) prompt. (Refer to the Accessing and Exiting the VSD Configuration Prompt section for instructions.)
2	If you want to modify a VSD's name, enter: **modify vsd *number* name *new-name***
	If you want to modify the ports assigned to a VSD, enter: **modify vsd *number* ports *new-port-list***
	If you want to modify the VSD using more than one command option (for example the name and port list), enter: **modify vsd *number* name *new-name* ports *new-port-list***
	Refer to Table 9-2 for a description of the options you can enter.
3	Press Return. The VSD is modified according to the changes you entered. You can view the list of assigned VSD numbers at any time. Refer to the Displaying Information About VSDs section for instructions about how to do so.

Table 9-2: Modify VSD Command Options

Command Option	Description
ports *new-port-list*	The ***new-port-list*** is the new list of bridge ports you want to assign to the VSD. You can list the ports individually by separating each with a comma (for example, **1,2,3,4,5**) or you can enter a range of ports by separating the first and last port numbers in the range with a hyphen (for example, **1-5**). You can also combine a list of individual entries with a range of entries (for example, **1-4,6,7**). Spaces are not permitted between port numbers and the comma or hyphen.
name *new-name*	The ***new-name*** is the new name you want to assign to the VSD (changing **Math_dept** to **Advanced_Math_dept**, for example). A name can be composed of up to 32 ASCII-printable characters, except a question mark (?), must not include spaces, and must contain at least one alphabetic character. The name assigned must be unique. You cannot create another VSD on the same module using the same name. Assigning a name to a VSD is optional.

Deleting VSDs

You can delete VSDs one at a time, or you can delete all VSDs on a particular module at the same time. When a VSD is deleted, all ports that were members of the VSD automatically become members of the default VSD. You cannot delete the default VSD.

To delete one or all VSDs, perform the following steps:

Step	Action
1	Access the VSD configuration (`VSD Config>`) prompt. (Refer to the Accessing and Exiting the VSD Configuration Prompt section for instructions.)
2	If you want to delete a single VSD, enter **delete vsd *number*** or **delete vsd *name***, where ***number*** is the number of the VSD you want to delete and ***name*** is the name of the VSD you want to delete. (Refer to the Displaying Information About VSDs section for instructions about how to list the numbers and names assigned to existing VSDs. If you want to delete all VSDs on the module, enter **delete all**.
3	Press Return. The VSDs you entered are deleted and the ports that are members of the deleted VSD become members of the default VSD.

Displaying Information About VSDs

You can display the following configuration information for either a specific VSD or for all VSDs:

- VSD number
- VSD name
- List of ports that are members of a VSD on a single module
- Warning messages

To display VSD configuration information, perform the following steps:

Step	Action
1	Access the VSD configuration (`VSD Config>`) prompt. (Refer to the Accessing and Exiting the VSD Configuration Prompt section for instructions.)
2	If you want to display information about a single VSD, enter **list vsd** ***number*** or **list vsd** ***name***, where ***number*** is the number of the VSD for which you want to display information and ***name*** is the name of the VSD for which you want to display information. If you want to display information about all VSDs on the module, enter **list all**.
3	Press Return. Information about the specified VSDs is displayed.

Examples

```
VSD Config>list all

VSD Name    Ports                                  VNbus Tag
  1  DEFAULT 1-17                                        65

TCP/IP-Host Services offered on VSD 1, DEFAULT.
Module not in Hub -- VNbus tags not used!
```

```
VSD>list vsd 3

VSD Number:     3
VSD Name:       Math-Dept
VNbus Tag:      98

 Port    Assoc Interface #/Name
  1          1/FDDI/1
  2          2/ATMLEC/2
```

Warning Messages

The following warning messages are also displayed under certain conditions when you use the **list** command:

Warning Message	Description
TCP/IP-Host's affiliated VSD has no ports	This message is displayed when the VSD associated with TCP/IP Host Services currently has no ports in it. When the VSD associated with IP Host has no ports in it, there is no remote access to TCP/IP Host Services. Refer to the Assigning a GIGAswitch GS2000 Module IP End Node to a VSD section for additional information about the relationship between VSDs and TCP/IP Host Services. Refer to the Creating VSDs section for information about how to add ports to an existing VSD.
Module not in Hub -- VNbus tags not used	This message is displayed when the module is installed in a GIGAswitch system. The message is a reminder that VNbus tags are not used in a GIGAswitch system and that the values in the VNbus column can be ignored.

Assigning a GIGAswitch GS2000 Module IP End Node to a VSD

GIGAswitch GS2000 line card (GS2000) modules can serve as IP end nodes in a network. As an IP end node, a module supports several IP protocols including, for example, Telnet, SNMP, TFTP, and Ping. Telnet and SNMP provide two vehicles for remotely managing modules. TFTP is used to backup and restore module configurations and to load new software images. Ping is used to diagnose network problems. Refer to Chapter 12 for information about using Telnet and SNMP. Refer to Chapter 10 for information about backing up and restoring module configurations.

When the module serves as an IP end node, you must perform the following tasks before any of these IP protocols (Telnet, SNMP, and so on) can be used:

- Assign an IP address and subnet mask to the module
- Select the VSD on which you want a module IP end node to reside

Assume, for example, each of three VSDs represents a different IP subnet. You must select the VSD on which the IP end node is to reside. If you select VSD 1, then you must assign an IP address and subnet mask to the IP end node that is valid for VSD 1's subnet. IP nodes directly attached to VSD 1's subnet can initiate an ARP request for, and connect to, the module directly. IP nodes connected to other subnets (VSD 2, for example) must connect to the module through a router.

You do not need to assign an IP address to the module or assign the address to a VSD if you do not want to use any of the IP end node protocols' features (remote management, network backup and restoration, and so on).

Restrictions

Assigning an IP host to a VSD affects only in-band management (IP packets received over FDDI or ATM network interfaces). IP packets received through the OBM port of a DIGITAL MultiSwitch 900 or a DEChub ONE are not affected. Packets received through an OBM port are not subject to VSD or bridge filtering.

Assigning an IP Address and Subnet Mask

Refer to Chapter 12 for information about how to assign the module's TCP/IP host address.

Selecting the VSD on Which the Host Resides

To associate an IP Host address with a specific VSD, perform the following steps:

CAUTION

You should assign the module's IP host address and associate the host address with a particular VSD one after the other. If you change the IP address or the address-to-VSD association without also changing the other and then restart the module, you may lose inband connectivity to the module. This may occur because the IP host address and the VSD's subnet do not match. If you encounter this problem, you may be able to correct the mismatch only by using a local console (inband management), or by resetting the module to factory defaults.

Step	Action
1	Access the VSD configuration (`VSD Config>`) prompt. (Refer to the Accessing and Exiting the VSD Configuration Prompt section for instructions.)
2	Enter **set vsd ip-host**.
3	Press Return. The following message is displayed: `VSD Number or Name (1): []?`
4	Enter the number or name of the VSD to which you want to assign the module's IP address. The factory default is 1.
5	Press Return. The module's IP address is associated with the specified VSD.
6	Verify that the IP address assigned to the IP host matches the subnet of the VSD. If it does not match, you should change the IP host address before completing the next step.
7	Restart the module for the setting to take effect. Refer to Chapter 10 for information about how to do so.

Chapter 10

Performing Routine Maintenance

Overview

Introduction

This chapter describes DIGITAL GIGAswitch GS2000 line card (GS2000) module maintenance procedures that you may need to perform periodically, and those that you should perform regularly.

In This Chapter

The following topics are covered in this chapter:

Accessing and Exiting the Boot Config Prompt

You must access the Boot config prompt (`Boot config>`) to configure and manage many of the parameters discussed in this chapter. The prompt is accessed from the Config prompt (`Config>`).

Accessing the Boot Config Prompt

To access the Boot config prompt, perform the following steps:

1	At the Config prompt, enter **boot**.

2	Press Return. The following message is displayed, followed by the Boot config prompt:
	`TFTP Boot/dump configuration`
	`Boot config>`

Exiting the Boot Config Prompt

You exit the Boot config prompt to return to the Config prompt.

Example

To return to the Config prompt (`Config>`) from the `Boot config>` prompt, enter **exit** and then press Return.

Restarting the Module

Certain module configuration tasks require that you restart the module for new configuration settings to take effect. The module is also started when power is applied.

Restarting the module causes reinitialization of the module software, using the same executable and configuration it is currently running. The executable (also known as the boot or image file) and configuration parameters are stored in the module's nonvolatile flash memory. Restarting the module also clears information stored in volatile memory, including all bridge table entries not saved to NVRAM, and drops any packets in the bridge. Recovery of the lost packets is the responsibility of the sending and receiving nodes.

Note

Restarting a module from a remote console terminates the console's Telnet session.

How to Restart the Module

To restart the module, perform the following steps:

Step	Action
1	At the Main prompt (`Main>`), enter **restart**.
2	Press Return. The following prompt is displayed: `Are you sure you want to restart the system? (Yes or [No]):` **No** is the default.
3	If you want to restart the module, enter **Yes** and press Return. The module is restarted. If you do not want to restart the module, press Return. The Main prompt is again displayed.

Note

You can also restart the module from the logon menu. Refer to Chapter 2 for information about how to do so.

Upgrading and Reinstalling Module Software

This section discusses the following topics:

- Installing the software
- Configuring installation file locations
- Viewing installation file locations
- Modifying installation file locations
- Canceling the installation procedure

An upgrade replaces the current version of software with a newer version. A reinstallation reloads the module with a copy of the current version of the software. You may need to reinstall the software if, for example, you have a problem upgrading to a newer version and need to reinstall the earlier version until the problem is resolved.

The steps you complete to perform an upgrade or reinstallation are the same. Therefore, for the purpose of this discussion, the term installation is used to mean either an upgrade or a reinstallation.

Installing the Software

The source software you use for an installation must be stored on a network host or server. You may want to preconfigure the network location of the software prior to performing an upgrade or reinstallation. (Refer to the Configuring Installation File Locations section for instructions.) Although preconfiguring the network location is not required, it reduces the number of steps you perform when installing the software.

The steps you perform to install the software vary, depending on whether you preconfigured the network location of the software to be installed.

Using a Preconfigured Network File Location

To upgrade or reinstall the module software, perform the following steps:

Step	Action
1	At the Main prompt (`Main>`), enter **reload**.
2	Press Return. The following prompt is displayed: `Are you sure you want to reload the system (Yes or No)?` **No** is the default.

Step	Action

3	If you want to reload the module software, enter **Yes** and press Return. The module performs a restart, taking itself off the network, reinitializes itself, and reconnects to the network in IP Host-Only Mode. The module software is copied from the preconfigured location and stored in NVRAM/flash memory. The following sequence of messages is displayed:
	`System restart...`
	`Copyright 1995-1996 Digital Equipment Corp.`
	`MOS Operator Control`
	`IP Host-Only Mode-Upgrading Operational Image...`
	`Network FLASH Upgrade Proceeding...`
	The installation is complete when the Load Status 1 and Load Status 2 LEDs flash alternating green and yellow for about 10 seconds, and then the LED pairs remain lit (either green or yellow) for another 10 seconds. This occurs about 45 seconds after the following message is displayed:
	`TFTP transfer complete: Status: OK.`
	After the installation or upgrade is successfully completed, hardware diagnostics are run. This takes about 1 minute.
	If the network location of the software to be installed is not preconfigured, the following message and the Main prompt is displayed:
	`Aborted, No boot entries defined. Configure a boot entry or use LOAD REMOTE.`
	If you do not want to reload the module software, press Return. The Main prompt is again displayed.
	Note: Refer to Table 10-1 for a full description of the LED lighting sequences during an upgrade.

4	If you are performing an upgrade, update the software version number according to the instructions in the Updating the Software Version Number section.

Using an Unconfigured Network File Location

To upgrade or reinstall the module software, perform the following steps:

Step	Action
1	At the `Boot config>` prompt, enter **load remote**.
2	Press Return. The following message is displayed: `Remote Host Address [0.0.0.0]?`

Step	Action
3	Enter the IP address of the host or server on which the software to be installed is located. The default address is `0.0.0.0`.
4	Press Return. The following message is displayed: `Remote Pathname []?`
5	Enter the path and file name that identifies where on the host or server the software is located. **Example: /usr/tftp/switch11.ldc**
6	Press Return. The following message is displayed: `First Hop Address [0.0.0.0]?`
7	Enter the IP address of the first hop router that routes to other networks. The first hop router and its address are needed if the remote host on which the software is located is not on a directly connected network. The default address is `0.0.0.0`.
8	Press Return. The following message is displayed: `TFTP Timeout Value [10]?`
9	Enter the desired TFTP timeout value. TFTP is the protocol the module uses to download the installation file. If the TFTP request is lost, TFTP retransmits the request several times. The timeout value affects the amount of time that passes before the next retry. The default timeout value of 10 seconds is recommended. A value greater than 10 seconds should be used if the path over which the installation is to occur is typically slow.
10	Press Return. The following message is displayed: `Are you sure you want to reload the system (Yes or No)?` **No** is the default.

Step	Action

11	If you want to reload the module software, enter **Yes** and press Return. The module performs a restart, taking itself off the network, reinitializes itself, and reconnects to the network in IP Host-Only Mode. The module software is copied and stored in NVRAM/flash memory. The following sequence of messages is displayed:
	`System restart...`
	`Copyright 1995-1996 Digital Equipment Corp.`
	`MOS Operator Control`
	`IP Host-Only Mode-Upgrading Operational Image...`
	`Network FLASH Upgrade Proceeding...`
	The installation is complete when the Load Status 1 and Load Status 2 LEDs flash alternating green and yellow for about 10 seconds, and then the LED pairs remain lit (either green or yellow) for another 10 seconds. This occurs about 45 seconds after the following message is displayed:
	`TFTP transfer complete: Status: OK.`
	After the installation or upgrade is successfully completed, hardware diagnostics are run. This takes about 1 minute.
	If you do not want to reload the module software, press Return. The Main prompt is again displayed.
	Note: Refer to Table 10-1 for a full description of the LED lighting sequences during an upgrade.

12	If you are performing an upgrade, update the software version number according to the instructions in the Updating the Software Version Number section.

LED Lighting Sequence During Load and Reload

The module's LEDs provide information regarding the progress of an installation or upgrade. If the TFTP file transfer is successful, a CRC of the image received at the module is performed. Table 10-1 describes the LED lighting sequences and the status of the upgrade they reflect.

Table 10-1: LED Lighting Sequence During Load/Reload

LED Lighting Sequence	Upgrade Status
• Load Status 2 LED: green • Load Status 1 LED: yellow	CRC is in progress.
• Load Status 2 LED: yellow • Load Status 1 LED: green	CRC detects an error.
• Load Status 2 LED: green • Load Status 1 LED: green	The image is being written to flash, following a successful CRC.
• Load Status 2 LED and Load Status 1 LED both flash alternating green and yellow for about 10 seconds, and then remain solidly lit (either green or yellow) for another 10 seconds	The process of writing the image to flash is complete.

Updating the Software Version Number

You should update the version number in configuration memory for newly upgraded software. The basic steps you perform to update the version number is shown in the following steps. However, refer to the instructions provided in the release notes sent with the software upgrade for detailed instructions.

To update the version number in configuration memory for an upgrade, perform the following steps:

Step	Action
1	At the `Config>` prompt, enter **update version-of-SRAM**.
2	Press Return. The version number is updated in configuration memory, and the `Config>` prompt is displayed.

Configuring Installation File Locations

To predefine the location of the file to be used for an upgrade or reinstallation, you specify the name of the installation file to be installed and the location of the server on which the file resides. You do not need to specify the module interface for transparent bridging. The upgrade operation defaults to the IP-HST address or the appropriate IP address if routing is enabled.

Specifying the File Name and Server Location

To specify the name of the file to be installed and the location of the server on which the file resides, perform the following steps:

Step	Action
1	At the Boot config prompt, enter **add boot-entry**.
2	Press Return. The following message is displayed: `remote host [0.0.0.0]?`
3	Enter the IP address of the remote host on which the installation file resides. The default address is `0.0.0.0`.
4	Press Return. The following message is displayed: `via gateway (0.0.0.0 if none) [0.0.0.0]?`
5	Enter the IP address of the first hop router, if any. The default address is `0.0.0.0`. The default should be used if there is no first hop router.
6	Press Return. The following message is displayed: `timeout in seconds [10]?`
7	Enter the desired TFTP timeout value. TFTP is the protocol the module uses to download the installation file. If the TFTP request is lost, TFTP retransmits the request several times. The timeout value affects the amount of time that passes before the next retry. The default timeout value of 10 seconds is recommended. A value greater than 10 seconds should be used if the path over which the installation is to occur is typically slow.
8	Press Return. The following message is displayed: `File name [ ]?`
9	Enter a path and file name for the location on the remote server where the installation file is located.
10	Press Return. The specified values are set and the Boot config prompt is displayed.

Displaying File Names and Server Locations

To view a list of the files to be installed and the location of the server on which the files reside, perform the following steps:

Step	Action
1	At the Boot config prompt, enter **list boot-entries**.
2	Press Return. A reference number is displayed for each configured interface, followed by a colon. The reference number is then followed by the location of each file to be used for installation, including the path and name of the file on the remote system, the IP address of the remote host on which the installation file resides, the IP address of the first hop router (if any), and the TFTP retransmission timer value.

Example

```
Boot config>list boot-entries

Boot files:
1: "/usr/bt/dvnee154.bin" on 192.9.1.2 through 0.0.0.0 for 3 secs
2: "/usr/bt/dvnee154.bin" on 192.9.2.2 through 192.9.1.4 for 3 secs
```

Modifying Installation File Locations

Modifying predefined installation file locations used for an upgrade or reinstallation includes the ability to change and delete the currently configured location of the installation file.

Changing the File Name and Server Location

To change the name of the file to be installed or the location of the server on which the file resides, perform the following steps:

Step	Action
1	At the Boot config prompt, enter **change boot-entry**.
2	Press Return. The following message is displayed: `Change which entry [1]?`

Step	Action
3	Enter the index number associated with the entry you want to change. The default is 1. The index number is the first number, followed by a colon, in each item listed when you display information about the location of the installation file using the **list boot-entries** command. Refer to the Displaying File Names and Server Locations section for additional information.
4	Press Return. The following message is displayed: `remote host [18.123.0.16]?`
5	Enter the new IP address of the remote host on which the installation file resides. The previously configured address is the default.
6	Press Return. The following message is displayed: `via gateway (0.0.0.0 if none) [0.0.0.0]?`
7	Enter the IP address of the first hop router, if any. The default address is `0.0.0.0`. The default should be used if there is no first hop router.
8	Press Return. The following message is displayed: `timeout in seconds [10]?`
9	Enter the desired TFTP timeout value. TFTP is the protocol the module uses to download the installation file. If the TFTP request is lost, TFTP retransmits the request several times. The timeout value affects the amount of time that passes before the next retry. The default timeout value of 10 seconds is recommended. A value greater than 10 seconds should be used if the path over which the installation is to occur is typically slow.
10	Press Return. The following message is displayed: `File name [user/lib/gw/gwimage.ldb]?`
11	Enter the path and file name for the location on the remote server where the installation file is located.
12	Press Return. The specified values are set and the Boot config prompt is displayed.

Deleting a File Name and Server Location

To delete the name of the file to be installed and the location of the server on which the file resides, perform the following steps:

Step	Action
1	At the Boot config prompt, enter **delete boot-entry**.
2	Press Return. The following message is displayed: `Delete which entry [1]?`
3	Enter the index number associated with the entry you want to delete. The default is 1. The index number is the first number, followed by a colon, in each item listed when you display information about the location of the installation file using the **list boot-entries** command. Refer to the Displaying File Names and Server Locations section for additional information.
4	Press Return. The specified location is no longer configured for use during installations.
5	To verify that the entry is deleted, use the **list boot-entries** command. The index numbers of the remaining entries are renumbered to avoid leaving a gap in the list of entries. For example, if entry 2 is deleted, entry 3 becomes entry 2, and so on. Refer to the Displaying File Names and Server Locations section for additional information.

Canceling the Installation Procedure

You can cancel the installation procedure before writing the image to flash memory begins. You do so by pressing Ctrl/C. You cannot use Ctrl/C to cancel installation while the image is being written to flash.

Caution

Do not power cycle the module while the image is writing to flash. The module may become disabled.

Backing Up and Restoring the Module

You can back up the module's configuration settings. Module configuration settings that are stored in NVRAM can be restored manually.

Automatic Image Recovery

The module automatically tries to reload the module's image if the currently installed image is corrupted. Although the current image is stored in NVRAM and does not need to be reloaded in the event of a power outage, the image can become corrupted due to an unusual event such as a power surge. The automatic download of a new image only occurs over the LDM port.

Location of Source Software

The source software used for automatic recovery must be stored on a network host or server. The location can be the same as that used for normal software upgrades or installations described in the Upgrading and Reinstalling Module Software section. If the module software image is corrupted, the module must look to an external device to determine the location of the software it must reload. Such a device is referred to as a BootP server. In this discussion, the module is referred to as a BootP client.

BootP Server and Clients

The BootP server contains a file that lists all the BootP clients for which the server is responsible, including the clients' IP addresses, and the locations and names of their boot files. This list of clients and boot file location information is maintained by the network administrator. If a module's image is corrupted, the module (BootP client) broadcasts a request to the BootP server. The request, in the form of a UDP packet, includes the client's MAC address. When the server receives the request, it looks up the client's address in its database of client information. If it locates the client's address in the database, the BootP server responds to the client, providing it with information about the location of the software it is to install. The module then initiates a TFTP request for a download of the software from the boot server on which the software resides.

Note

The BootP server can use any BootP software available on a variety of operating systems.

DIGITAL Online Services

GIGAswitch GS2000 software is also available through DIGITAL's Network Products Business Web pages. The DIGITAL Network Products Home Page on the World Wide Web is located at the following addresses:

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

Configuring Automatic Image Recovery

To configure your system for automatic recovery of the module's executable software, you must configure the BootP server. You do not need to configure the BootP client (the GIGAswitch GS2000 module). The image is automatically reloaded through the LDM port on the module.

The network node you use as a BootP server can use any operating system that supports the BootP utility. You must properly configure the server to include a BootP database that contains a list of all the BootP clients (modules) for which the server is responsible, including the clients' IP addresses, and the locations and names of their boot files. Refer to the operating system documentation provided by the system vendor for configuration instructions.

Backing Up Configuration Settings

Default configuration settings and most of the settings you configure are stored in a configuration database in the module's NVRAM. Although the configuration database does not need to be reloaded if there is a power outage, the database can become corrupted due to an unusual event such as a power surge. You can make a copy of the configuration database and back it up on a remote server or host. Should the module's configuration database be corrupted, you can then copy the backup to the module, minimizing the need to reconfigure custom settings you previously entered.

Use the Trivial File Transfer Protocol (TFTP) to back up the configuration database to a remote system, and to copy the backup to the module if the original database on the module is corrupted. The GIGAswitch GS2000 software includes a version of TFTP for this purpose.

Before You Begin

On some systems, you may need to create the file on the remote server or host to which the configuration database is backed up. This is the host file name you enter during the backup procedure specified in the Backing Up the Configuration Database section.

You must also configure the module's TCP/IP Host Services to include one IP address for the module, before attempting backup or restoral. Because the configured IP address is lost if NVRAM is corrupted, the address must be reconfigured before restoral. You can also reconfigure the module's host name (optional). Refer to Chapter 12 for information about configuring TCP/IP Host Services.

Backing Up the Configuration Database

To back up a module's configuration database to a remote system, perform the following steps:

Step	Action
1	At the Boot config prompt, enter **tftp put**.
2	Press Return. The following message is displayed: `local filename [CONFIG]?` CONFIG is the default file name. It cannot be changed.
3	Press Return. The following message is displayed: `remote host [0.0.0.0]?`
4	Enter the IP address of the host to which you want to copy the configuration database. The default (`0.0.0.0`) is an invalid address, and is meant only to show the format of the address.
5	Press Return. A message similar to the following is displayed: `host filename [0B070706.cfg]?` The filename's prefix is derived from a portion of the module's IP address converted to ASCII.
6	Enter the path, followed by a unique file name, to identify the location on the remote system where you want to back up the configuration database. The default is `0B070706.cfg`. It is recommended that you give the file a name that is descriptive of the module from which it originates. By doing so, you should more easily be able to distinguish between backup files derived from multiple modules. **Example: /usr/local/tftp/switch11.cfg**
7	Press Return. The following message is displayed when the transfer is completed: `TFTP transfer complete, Status: OK` Refer to the following table for a list of possible error messages and their meanings.

The following error messages may be displayed if an error occurs during the transfer:

Error Message	Meaning
`Unknown Error`	Protocol failure
`File Not Found`	Specified host file does not exist
`Access Violation`	File protection error
`Disk Full`	File system full during write
`Illegal Operation`	Undefined TFTP operation requested
`Unknown TID`	Unexpected TFTP packet received
`File Already Exists`	File already exists
`No Such User`	TFTP not supported on host

Restoring a Configuration Database

The configuration database can be restored to a module of the same type from which it was backed up. The restoral process includes verification of a "magic number" that ensures the configuration database is being restored on a module of the proper type. The message `Bad Magic Number` is displayed if you attempt to restore the database to a module of the wrong type. The module's host name is also checked to make sure the configuration is restored on the correct module. If the host name of the module to which the file is to be restored differs from that of the original module, the message `Is this acceptable? (Yes or [No])` is displayed. No is the default.

To restore a module's configuration database by retrieving it from a remote system, perform the following steps:

Caution

Do not power off or reset the module while restoring the configuration database. NVRAM may become corrupted, requiring you to reinstall the module's configuration database.

Step	Action
1	At the Boot config prompt, enter **tftp get**.
2	Press Return. The following message is displayed: `Local filename [CONFIG]? config` CONFIG is the default file name. It cannot be changed.
3	Press Return. The following message is displayed: `Remote host [0.0.0.0]?`
4	Enter the IP address of the host where the configuration database is backed up.
5	Press Return. The following message is displayed: `Host filename [ ]?`
6	Enter the path and file name that identifies the location and configuration database you want to restore. **Example: /usr/local/tftp/switch11.cfg**

7	Press Return. The following message is displayed when the transfer is complete:
	`TFTP transfer complete, status: OK`
	`An automatic RESTART will occur after writing CONFIG.`
	`Are you sure you want to write new CONFIG? (Yes or [No]):`
	The following message is displayed if there is not enough memory to buffer the file on the module:
	`TFTP transfer complete, Status: Out of Memory`

Step	Action
8	Enter **yes** if you want to continue. Enter **no** if you want to abort the procedure.

9	If you entered **yes**, the following message is displayed:
	`Updating CONFIG; Do Not Interrupt!`
	If you enter **no**, the following message is displayed and the procedure is aborted:
	`*** ERROR ***`
	`Write to Non-Volatile memory failed! CONFIG update aborted.`

Note

You cannot transfer a configuration database using the remote system's version of TFTP client.

Exiting and Canceling Backup or Restoration

The Boot config prompt is locked during backup or restoration of the configuration database. In order to:

- Exit the Boot config prompt and return to the Main prompt (`Main>`) while allowing the backup or restore to continue, press Ctrl/P.
- Cancel backup or restore, press Ctrl/C. The Boot config prompt is displayed.

Checking Available RAM

The module's volatile memory is used to store information such as bridge tables and various buffers. A predefined amount of volatile memory is allocated from the module's random access memory (RAM) at startup. If more volatile memory is required, additional RAM is variably allocated to volatile memory, as needed.

How to Check Available RAM

To check available RAM, perform the following steps:

Step	Action
1	At the Main prompt (`Main>`), enter **memory**.
2	Press Return. A message is displayed indicating the number of bytes in RAM that are busy, idle, and free.

Example

The following example shows how to check available RAM.

```
Main>memory

Number of bytes:  Busy = 28464,  Idle = 5632,  Free = 2926207
```

where,

Information Displayed	Description
`Busy`	Number of bytes in use (temporarily allocated) as volatile memory
`Idle`	Number of bytes previously allocated but freed and available for reuse
`Free`	Number of bytes never allocated from RAM

Note

The sum of Idle and Free memory equals the total available heap memory.

For More Information

Refer to Chapter 4 for more information about monitoring module memory.

Capturing Restart or Crash Messages and Diagnostic Data

The module logs messages and diagnostic data whenever the module is restarted or experiences a fatal error. You can display these messages to help troubleshoot problems and can download detailed diagnostic data for further problem analysis.

Displaying and Managing Restart or Crash Error Messages

The module generates informational messages whenever it is restarted and a problem is encountered, and whenever a fatal error such as a bug halt occurs. The restart messages, generated by diagnostic routines during power-up, are recorded in a diagnostic log. Messages related to fatal errors (crashes) are recorded in a crash log. Both logs are stored in NVRAM and, therefore, the information they contain remains intact after a restart or power outage.

You display the messages in these logs to determine the results of diagnostics and to detect crashes that might occur when you are not present. (The occurrence of a crash may not be obvious because the switch typically restarts automatically.) However, a detailed interpretation of the messages is possible only with the assistance of DIGITAL Customer Services, who can assist troubleshooting problems you encounter. Each log retains up to 254 messages. If the maximum of 254 messages is reached, each new message overwrites (wraps) the oldest existing message. Refer to the Determining When a Crash Occurs section for detailed information about how to read the crash log to determine when a crash occurs.

You can also delete messages from the logs if you want to make detection of new messages easier. You can delete messages either one at a time or you can delete all messages from a log.

Displaying Diagnostic or Crash Log Messages

You can display diagnostic or crash log messages from either the Config prompt (`Config>`) or the Monitor prompt (`Monitor>`). To display diagnostic log or crash log messages, perform the following steps:

Step	Action
1	At either the Config prompt or the Monitor prompt, enter **err-logs**.
2	Press Return. The `Error-Log>` prompt is displayed.
3	If you want to display the diagnostic log, enter **list diagnostic-log**. If you want to display the crash log, enter **list crash-log**.

Step	Action
4	Press Return. The list of messages contained in the specified log and the `Error-Log>` prompt is displayed.

Determining When a Crash Occurs

You can find out when a crash occurs by determining when a message is logged in relation to other messages, and by inserting a date/time stamp or similar marker at specific points in the crash log.

Message Sequence

Two numbers are automatically assigned to each message, a crash log entry number and a historical message number. The crash log entry number is displayed on the line preceding a message. It is used to identify messages you want to delete. The historical message number is used to determine when a specific message is logged in relation to other messages. The historical message number is displayed on the same line as the message. Refer to Figure 10-1 for an example.

The maximum number of crash log entries that can be recorded is 254. If this number is exceeded, the next message logged overwrites the oldest crash message starting at crash log entry number 1. However, when the historical message number reaches 254, it continues to increment by 1 to 255, 256, and so on as shown in Figure 10-1, up to and including 9999. It is then reset to 1. Therefore, the crash message having the highest historical message number is the most recent message logged. Using Figure 10-1 as an example, crash log entry number 5 with a historical entry number of 259 is a more recent entry than crash log entry number of 6 with a historical entry number of 6.

The crash log is cleared and the crash log entry number is reset to 1, if the total message record size is exceeded and a new message is logged. Because the length of each message is different, the speed with which the record becomes full varies, depending on the total number of characters of all messages logged.

If the time has been set using either the **Config>set time** or **Config>time host** commands, then a timestamp is saved with each crash message. If not, the uptime of the module is saved.

Figure 10-1: Sample Crash Log

```
CRASH LOG ENTRY NUMBER 1
255 Bus Error at Address 0xA00C2B0; Next Instr 0x11143C2;
CRASH LOG ENTRY NUMBER 2
256 Bus Error at Address 0xA00C2B0; Next Instr 0x11143C2;
CRASH LOG ENTRY NUMBER 3
257 Bus Error at Address 0xA00C2B0; Next Instr 0x11143C2;
CRASH LOG ENTRY NUMBER 4
258 User induced bughlt via DVT
CRASH LOG ENTRY NUMBER 5
259 User induced bughlt via DVT
CRASH LOG ENTRY NUMBER 6
6 User induced bughlt via DVT
CRASH LOG ENTRY NUMBER 7
7 Bus Error at Address 0xA00C2B0; Next Instr 0x11143C2;
CRASH LOG ENTRY NUMBER 8
8 February 12, 1997; 3:58 PM
CRASH LOG ENTRY NUMBER 9
9 (V1.5-001) Bus Error at Address 0x9404016;
  Next Instr 0x106AF04;
CRASH LOG ENTRY NUMBER 10
10 (V1.5-001) dmesv - deallocateVnBusAddrSpec
   - addr spec invalid
```

Crash Log Markers

You can insert a marker in the crash log so that you can identify when messages that follow a marker occur. The marker you enter is a free-form text entry. For example, if you enter the date and time, you will know that all messages that follow the marker occur after the specified date and time. If the marker you enter describes a particular system configuration change you make, you will know that all messages that follow the marker may be the result of the new configuration.

Markers appear as a message in the crash log, and are assigned a crash log entry number and historical message number. Refer to crash log entry number 8 in Figure 10-1 for an example.

To enter a crash log market, perform the following steps:

Step	Action
1	At the Config prompt, enter **err-logs**.
2	Press Return. The `Error-Log>` prompt is displayed.

Step	Action
3	Enter **writelog**.
4	Press Return. The following message is displayed: `Message [1-240 chars]?:`
5	Enter the desired text.
6	Press Return. The text of the marker you enter is logged in the crash log and the `Error-Log>` prompt is displayed.

Deleting All Diagnostic or Crash Log Messages

You can delete (clear) all messages from either the diagnostic or crash log, or from both logs. You can do so only from the Config prompt (`Config>`). The Monitor (`Monitor>`) prompt cannot be used to clear the logs. To delete all diagnostic log or crash log messages, perform the following steps:

Step	Action
1	At the Config> prompt, enter **err-logs**.
2	Press Return. The `Error-Log>` prompt is displayed.
3	If you want to delete all messages from the diagnostic log, enter **clear diagnostic-log**. If you want to delete all messages from the crash log, enter **clear crash-log**. If you want to delete all messages from both logs, enter **clear all**.
4	Press Return. All messages in the specified log are deleted and the `Error-Log>` prompt is displayed.

Deleting a Single Diagnostic or Crash Log Message

You can delete one message at a time from either the diagnostic or crash log. You can do so only from the Config prompt (`Config>`). The Monitor (`Monitor>`) prompt cannot be used to delete a message from the logs. To delete one message at a time from the diagnostic log or the crash log, perform the following steps:

Step	Action
1	At Config> prompt, enter **err-logs**.
2	Press Return. The `Error-Log>` prompt is displayed.

Step	Action
3	If you want to delete a message from the diagnostic log, enter **delete diagnostic-log**. If you want to delete a message from the crash log, enter **delete crash-log**.

4	Press Return.
	If you are deleting an entry from the diagnostic log, the following message is displayed:
	`diagnostic error-log entry number [ ]?`
	If you are deleting an entry from the crash log, the following message is displayed:
	`Crash log entry number [ ]?`

5	Enter the number of the message you want to delete. The crash log entry number is displayed on the line preceding a message. Refer to Figure 10-1 for examples of crash log entries and their associated numbers. **Example:** `diagnostic error-log entry number [ ]?`**235**
6	Press Return. The error entry associated with the number you entered is deleted, the message `Deleted Error Log Entry Number = 235` and the `Error-Log>` prompt are displayed. If the error entry you specified by number does not exist, the following message is displayed: `Error Log Entry Not Found`

Downloading Diagnostic Data for Problem Analysis

You can capture a "snapshot" of a failed module's status at the time of failure. This information can be used as a diagnostic tool by Digital Services representatives, should you require assistance.

Capture the diagnostic data by configuring your module to automatically download (dump) the information to one or more host systems when the module is reset due to a hardware or software failure. The data is also downloaded when the Reset/Dump button located on the module's front panel is pressed.

This section discusses the following topics:

- Configuring and enabling dump files
- Displaying dump status information
- Viewing dump file locations
- Modifying dump file locations

Configuring and Enabling Dump Files

You can configure up to eight remote locations to which diagnostic information is downloaded. It is recommended that you configure at least one location. Configuring multiple locations helps ensure that, in the event a download to one location is not successful, the download to another location is likely to succeed.

The module dumps files over the Load/Dump/Management (LDM) port only. The LDM port is located on the front panel of the module.

To configure the location of the host or server that is to receive a dump file, perform the following tasks:

Task	Description
1	Configure an IP address for the LDM port and enable TCP/IP host services.
2	Create a dump file on the TFTP server.
3	Specify the name of the dump file, and the location of the server to which the file is to be downloaded.
4	Enable dumping on the module.
5	Retain multiple dumps at a single location (enable unique-naming). This task is optional.
6	If routing is enabled, use the **add address** command to configure an IP address for the LDM port.
7	Perform a test dump.

Configuring an IP Address for the LDM Port

To be able to download information, the module must be configured with an in-band IP address and TCP/IP Host Services enabled.

If an IP address is not assigned to the LDM port, the LDM port defaults to the IP-HST address that has been configured for the module. You can specify a different IP address for the LDM port by using the **add address** command at the Boot config prompt.

Note

If routing is enabled, you must use the **add address** command at the Boot Config prompt to configure an IP address for the LDM port.

Refer to the Enabling and Disabling Host Services section for information on enabling TCP/IP Host Services.

Creating a Dump File on the TFTP Server

On most TFTP servers, you must create a file on the TFTP server with appropriate network access before a dump operation can be completed successfully.

Specifying the File Name and Server Location

To specify the name of the dump file and the location of the server to which the file is to be downloaded, perform the following steps:

Step	Action
1	At the Boot config prompt, enter **add dump-entry**.
2	Press Return. The following message is displayed: `remote host [0.0.0.0]?`
3	Enter the IP address of the remote host to which the dump file is downloaded. The default address is `0.0.0.0`.
4	Press Return. The following message is displayed: `via gateway (0.0.0.0 if none) [0.0.0.0]?`
5	Enter the IP address of the first hop router, if any. The default address is `0.0.0.0`. The default should be used if there is no first hop router.
6	Press Return. The following message is displayed: `timeout in seconds [10]?`
7	Enter the desired TFTP timeout value. TFTP is the protocol the module uses to download the dump file. If the TFTP request is lost, TFTP retransmits the request several times. The timeout value affects the amount of time that passes before the next retry. The default timeout value of 10 seconds is recommended. A value greater than 10 seconds should be used if the path over which the dump is to occur is typically slow.
8	Press Return. The following message is displayed: `file name [ ]?`
9	Enter the file name to be assigned to the dump file. **Example:** `file name [ ]?`**/usr/tftp/switch11.dmp**
10	Press Return. The specified values are set and the Boot config prompt is displayed.

Step	Action
11	Repeat steps 1 through 10 for each remote location you want to configure. You can configure a maximum of eight locations.

Enabling and Disabling Dumps

The module can dump diagnostic data to the remote system location you specify only after you enable dumping. Disabled is the default setting. Dumping remains disabled until you enable it, and remains enabled until you disable it. (Refer to the Displaying All Boot Config Settings section for information about how to determine whether dumping is enabled on a module.)

Enabling Dumping

To enable dumping of diagnostic data to the configured remote system location, perform the following steps:

Step	Action
1	At the Boot config prompt, enter **enable dumping**.
2	Press Return. Dumping is enabled and the Boot config prompt is displayed.

Disabling Dumping

To disable dumping of diagnostic data to the configured remote system location, perform the following steps:

Step	Action
1	At the Boot config prompt, enter **disable dumping**.
2	Press Return. Dumping is disabled and the Boot config prompt is displayed.

Retaining Multiple Dumps at a Single Location

You have the option of configuring the module to enable multiple downloads to the same path on a server without overwriting earlier dumps. You do so by configuring the module to assign a unique name to each dump file that is downloaded. If a unique name is not assigned to each file, then new dumps overwrite the previous file downloaded to the same location.

Note

Because most TFTP servers require that a dump file be created before the dump can occur, the **enable unique-naming** command may not be appropriate or useful.

If retaining multiple dumps (unique naming) is enabled, the module appends a random suffix of one to five hexadecimal characters to the base file name you specify according to instructions in the Specifying the File Name and Server Location section. Disabled is the default setting. Retaining multiple dumps remains disabled until you enable it, and remains enabled until you again disable it. (Refer to the Displaying All Boot Config Settings section for information about how to determine whether unique naming is enabled on a module.)

Enabling Multiple Dumps

To retain multiple dumps of diagnostic data to the same location on a server, perform the following steps:

Step	Action
1	At the Boot config prompt, enter **enable unique-naming**.
2	Press Return. Retaining multiple dump files is enabled and the Boot config prompt is displayed.

Disabling Multiple Dumps

To disable the retention of multiple dump files downloaded to the same location, perform the following steps:

Step	Action
1	At the Boot config prompt, enter **disable unique-naming**.
2	Press Return. Retaining multiple dump files downloaded to the same location is disabled and the Boot config prompt is displayed.

Performing a Test Dump

It is recommended that you perform a test dump of newly configured dump locations. Doing so helps verify that the diagnostic data is properly downloaded in the event of a hardware or software failure, or when the Reset/Dump button is pressed.

Note

For the dump command to work, dumping must first be enabled at the `Boot config>` prompt.

To test the newly configured dump location, perform the following steps:

Step	Action
1	At the Main prompt (`Main>`), enter **dump**.

2	Press Return. The following message is displayed:
	`Dumping will invoke a RESTART.`
	`Are you sure you want to dump memory? (Yes or [No])`

3	If you want to continue the download and initiate a restart, enter **Yes**. If you do not want to continue the download, enter **No**.
4	Press Return. If you entered **Yes**, the contents of module memory are downloaded to the remote host and file name you specified. The module is restarted and the GIGAswitch GS2000 module Installation Menu (Figure 2-1) is displayed. If you entered **No**, the Main prompt (`Main>`) is displayed.

Performing a Test Dump Using the Reset/Dump Button

The Reset/Dump button is located on the module. When you press this button, the contents of the module memory is downloaded to the host and filename you specified. The module is restarted and the module's Installation Menu is displayed.

Displaying Dump Status Information

You can display the status of the most recent dump attempted for a module. The following information is displayed for each configured dump location:

Information Displayed	Description
Status	Possible outcomes include `Successful`, `Failed`, and `Not Attempted`.
Pathname	The path and file name on the remote server for which the download is configured.
IP Address	The IP address of the remote system to which the dump is downloaded is displayed. If a first hop router is used, the IP address of the first hop router is also listed.

Note

A maximum of eight remote dump locations can be configured for each module.

To display the status and location of the most recent dump, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **dump information**.
2	Press Return. The status and location information about the most recent dump is displayed.

Example

`Monitor>`**dump information**

```
1:Dump Failed to "/usr/router1.dmp" on 1.2.3.4 error = TFTP protocol error
2:Dump Not attempted to "/usr/tftp/router1.dmp" on 10.23.2.5
3:Dump Successful to "/usr/tftp/router1.dmp" on 1.2.3.4
```

Viewing Dump File Locations

You can view the locations to which diagnostic data (dump files) are downloaded. To view a list of the file names to be assigned to dump files, and the location of the server on which the files are to reside, perform the following steps:

Step	Action
1	At the Boot config prompt, enter **list dump-entries**.
2	Press Return. A reference number is displayed for each configured interface, followed by a colon. The reference number is then followed by the location to which each dump file is to be downloaded, including the path and name of the file on the remote system, the IP address of the remote host to which the download occurs, the IP address of the first hop router (if any), and the TFTP retransmission timer value.

Example

```
Boot config>list dump-entries

Dump to:
1: "/usr/local/sw1.dmp" on 1.2.3.4 via 0.0.0.0 for 10 secs
2: "/usr/tftp/sw1.dmp" on 13.12.2.3 via 1.1.2.7 for 10 secs
```

Modifying Dump File Locations

Modifying the remote locations to which diagnostic data is downloaded includes the ability to change and delete the currently configured location.

Changing the File Name and Server Location

To change the name assigned to a dump file or the location of the server to which the download is to occur, perform the following steps:

Step	Action
1	At the Boot config prompt, enter **change dump-entry**.
2	Press Return. The following message is displayed: `Change which entry [1]?`
3	Enter the reference number associated with the entry you want to change. The default is 1. The reference number is the first number, followed by a colon, in each item listed when you display information about dump file locations using the **list dump-entries** command. Refer to the Viewing Dump File Locations section for additional information.

Step	Action
4	Press Return. The following message is displayed: `remote host [18.123.0.16]?`
5	Enter the new IP address of the remote host to which the dump file is downloaded. The previously configured address is the default.
6	Press Return. The following message is displayed: `via gateway (0.0.0.0 if none) [0.0.0.0]?`
7	Enter the IP address of the first hop router, if any. The default address is `0.0.0.0`. The default should be used if there is no first hop router.
8	Press Return. The following message is displayed: `timeout in seconds [3]?`
9	Enter the desired TFTP timeout value. TFTP is the protocol the module uses to download the dump file. If the TFTP request is lost, TFTP retransmits the request several times. The timeout value affects the amount of time that passes before the next retry. The default timeout value of 10 seconds is recommended. A value greater than 10 seconds should be used if the path over which the dump is to occur is typically slow.
10	Press Return. The following message is displayed: `File name [user/lib/gw/gwimage.ldb]?`
11	Enter the path and file name for the location on the remote server to which the dump file is downloaded.
12	Press Return. The specified values are set and the Boot config prompt is displayed.

Deleting a File Name and Server Location

To delete the name to be assigned to the dump file and the location of the server to which the file is downloaded, perform the following steps:

Step	Action
1	At the Boot config prompt, enter **delete dump-entry**.
2	Press Return. The following message is displayed: `Delete which entry [1]?`
3	Enter the reference number associated with the entry you want to delete. The default is 1. The reference number is the first number, followed by a colon, in each item listed when you display information about the configured location for the dump file using the **list dump-entries** command. Refer to the Viewing Dump File Locations section for additional information.
4	Press Return. The specified location is no longer configured for use during downloads.
5	To verify that the entry is deleted, use the **list dump-entries** command. Refer to the Viewing Dump File Locations section for additional information.

Displaying All Boot Config Settings

You can view a report that shows all module settings configured using the Boot config process, including the following information:

- IP address and subnet mask used during reload and dump operations
- Location and file name of boot files on remote systems
- Whether dumping is enabled
- Whether retaining multiple dumps at a single location (unique-naming) is enabled
- Locations and file names on remote systems to which diagnostic data is dumped

Refer to the Configuring Automatic Image Recovery, Capturing Diagnostic Data for Problem Analysis, and Retaining Multiple Dumps at a Single Location sections for detailed information about dumps, BootP software loads, and enabling multiple dumps, respectively.

To display all module settings that are configured from the Boot config prompt, perform the following steps:

Step	Action
1	At the Boot config prompt, enter **list all**.
2	Press Return. All module settings configured from the Boot config prompt are displayed.

Example

```
Boot config>list all

Interface addresses:
1: 192.9.1.1 on interface 0, mask 255.255.255.252
2: 192.9.223.39 on interface 5, mask 255.255.255.0

Boot files:
1: "/usr/bt/inst.ldb" on 192.9.1.2 through 0.0.0.0 for 3 secs
2: "/usr/bt/in.ldb" on 192.9.2.2 through 192.9.1.4 for 3 secs

Dumping disabled

Unique-naming disabled

Dump to:
1: "/usr/local/sw1.dmp" on 1.2.3.4 via 0.0.0.0 for 10 secs
2: "/usr/tftp/sw1.dmp" on 13.12.2.3 via 1.1.2.7 for 10 secs
```

Chapter 11

Event Logging and Reporting

Overview

Introduction

The Event Logging System (ELS) is a background process that records operational event messages for a DIGITAL GIGAswitch GS2000 line card. You can view this log of event messages from your console's CLI, or by making the events available to an SNMP-based agent such as the DIGITAL clearVISN MultiChassis Manager. You can also configure the ELS to record specific types of events and to eliminate others, depending on the level of operational detail you require. For example, you may want to view information that relates only to bridging, or information that relates only to communication between the module and an IPX server on an Ethernet LAN.

Event messages are recorded by ELS and displayed on your console in abbreviated form. Refer to the *Event Logging System Messages Guide* for expanded descriptions of all event messages, as well as an explanation of the message, possible causes of the event (if applicable), and possible actions you can take to correct error conditions.

In This Chapter

The following topics are covered in this chapter:

Event Messages and Related Concepts

You must understand how event messages are generated to be able to interpret the messages. Knowledge of the following concepts is also required if you want to narrow the scope of recorded messages, to focus on specific operations or problem areas.

Types of Events That Are Logged

The ELS records the following general types of events:

- System activity
- Status changes
- Service requests
- Data transmission and reception
- Data and internal errors

As events occur, ELS receives information from the module that identifies the source and nature of the events. The information is incorporated into the resultant event message which ELS generates and records. You can use the information to monitor module activity or to troubleshoot potential problems.

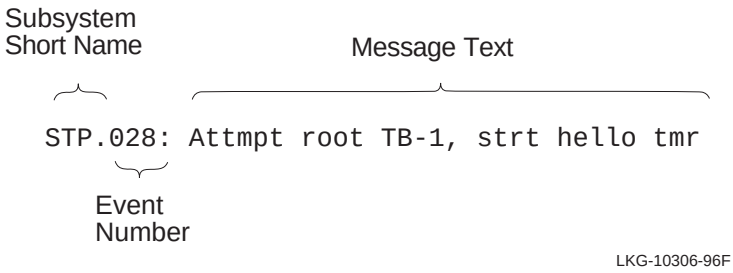
Elements of an Event Message

Event messages are composed of the following three elements:

- Subsystem
- Event number
- Message text

Figure 11-1 is an example of a message generated by an event. It identifies the subsystem, event number, and message text components.

Figure 11-1: Sample Message Generated by an Event



Subsystem

The Event Logging System divides module functionality into several operational subsystems. These include bridging, the Spanning Tree Protocol, and the Ethernet handler, for example. When an event occurs, a subsystem short name is added as a prefix to the event message. The short name identifies with which subsystem the event is related. In Figure 11-1, for example, the event short name is STP, indicating the event is related to a Spanning Tree Protocol operation. When you display the log of event messages, the prefix should help you to more accurately monitor module activity and isolate potential problems. Refer to Table 11-1 for a list of subsystems and their associated short names.

You can configure the ELS to record only those events generated by one or more specific subsystems, or all subsystems. Recording events for one or a few specific subsystems can help you focus on events related to a particular operation or set of operations. Refer to the Selecting Which Events Are Logged section for information about recording events generated by one or more subsystems.

Note

The subsystems that are active on a given module vary, depending on the specific hardware and software configured for the module.

Table 11-1: Event Subsystems and Associated Short Names

Subsystem Description	Subsystem Short Name
Router base and network library	GW
Address Resolution Protocol	ARP
Internet Protocol	IP
Internet Control Message Protocol	ICMP
Transmission Control Protocol	TCP
User Datagram Protocol	UDP
BootP relay agent	BTP
Trivial File Transfer Protocol	TFTP
Simple Network Management Protocol	SNMP
Source Routing Transparent Bridge	SRT
Spanning Tree Protocol	STP
Filter Library	FLT
IP Routing Information Protocol	RIP
Exterior Gateway Protocol	EGP
Open SPF-Based Routing Protocol	OSPF
OSPF Multicast extensions	MSPF
DECnet	DN
Xerox Networking Systems Protocol	XNS
Internetwork Packet Exchange Protocol	IPX
AppleTalk	APL
AppleTalk Phase 2	AP2
Apollo Domain Protocol	DDS
IP Protocol Net	IPPN
All subsystems	ALL

Event Number

The Event Logging System automatically assigns a unique number to each event message generated by a subsystem. In Figure 11-1, for example, the event number is 028. It is separated from the subsystem short name by a period. The short name and event number, together, identify an individual event. You can use the subsystem short name and event number as a parameter for specific ELS configuration and monitoring commands. Only the event indicated by the specified subsystem and event are affected by the ELS command.

Message Text

An abbreviated description of a specific event is provided in the text portion of an event message, as shown in Figure 11-1. For example, the message text `Attmpt root TB-1, strthellotmr`, indicates that the instance of STP on VSD 1 is declaring itself as root, and has restarted the BPDU Hello Timer. The *Event Logging System Messages Guide* provides expanded descriptions of all abbreviated messages, as well as an explanation of the message, possible causes of the event (if applicable), and possible actions you can take to correct error conditions.

Some event messages include fields that display variable values, such as network and interface numbers, source addresses, and error codes. Refer to the *Event Logging System Messages Guide* for a detailed discussion about these variables.

Logging Levels and Event Types

The logging level is a further classification of messages according to the type of event that generated a message. For example, a particular type of event might typically be caused by an unusual internal error. In such a case, ELS associates the UI-ERROR (unusual internal error) logging level with the event. Table 11-2 shows the full list of logging levels and the type of condition that generates events associated with the level.

Table 11-2: Logging Levels and Associated Event Types

Logging Level	Event Type
UI-ERROR	Unusual internal errors
CI-ERROR	Common internal errors
UE-ERROR	Unusual external errors
CE-ERROR	Common external errors
ERROR	Includes all *error* levels above
U-INFO	Unusual informational comment
C-INFO	Common informational comment
INFO	Includes all *comment* levels above
STANDARD	Includes all *error* levels and all *informational comment* levels (recommended default)
P-TRACE	Per packet trace
U-TRACE	Unusual operation trace message
C-TRACE	Common operation trace message
TRACE	Includes all *trace* levels above
ALL	Includes *all* logging levels

The logging level can be used for informational purposes, and to provide you with the ability to further narrow the scope of recorded events. Assume, for example, the following event message is displayed on your console:

`SNMP.005 no access; comm "`*`community`*`", hst `*`source_address`*

If you are interested in knowing the type of event that generated the message, you would look up the event using the subsystem short name and event number (`SNMP.005`) in the *Event Logging System Messages Guide*. The guide lists the logging level as U-TRACE, indicating the message is the result of an “unusual operation packet trace.”

If you want to narrow the scope of events recorded by ELS to only those involving unusual operation packet traces, you would specify U-TRACE as the logging level when configuring ELS. Refer to the Selecting Which Events Are Logged section for information about how to do so.

Preconfigured Logging Criteria (Groups)

You can preconfigure customized lists of one or more event numbers that you want to record. The customized lists are referred to as groups. You can subsequently configure ELS to record all occurrences of events listed in a group by simply entering the name of the group. Configuring ELS using groups is most useful when you have combinations of events that you regularly need to record. Using groups helps eliminate the need to enter the desired event numbers individually.

Selecting Which Events Are Logged

You can configure ELS to log specific types of events and to eliminate other events, depending on the level of detail you require. For example, you may want to log and view events that relate only to STP. Or, you may want to log events generated by both the STP and Ethernet Handler subsystems, and only events associated with the P-TRACE logging level. When you configure ELS to log events associated with a particular subsystem, event number, logging level, or group, those settings remain in effect until you either clear all configuration settings, or clear selected settings.

Modes of Configuration

You can configure ELS in nonvolatile memory and in volatile memory. ELS configurations that you set in nonvolatile memory (NVRAM) require that you restart the module to take effect. These settings survive power outages and module restarts. This method of setting values is most useful when configuring selection criteria for events that you want to monitor on a regular basis. You configure ELS in NVRAM from the Config prompt.

ELS configurations you set in volatile memory do not require that you restart the module to take effect. These settings do not survive power outages and module restarts unless you save them to a reserved portion of NVRAM (Refer to the Saving and Managing a Configuration in NVRAM section later in this chapter). Setting ELS configurations in volatile memory is most useful when configuring selection criteria you want to remain in effect only temporarily, and that you are likely to change from moment to moment as you troubleshoot a particular problem. You configure ELS in volatile memory from the Monitor prompt.

Commands Used to Log Events

You can view the log of event messages from your console's CLI, or by sending the events to SNMP. The process of sending specific events over SNMP is referred to as trapping. If sent to SNMP, the events are viewed using an SNMP-based agent such as the DIGITAL clearVISN MultiChassis Manager. The tasks you perform to select which events are logged are the same whether you plan to view the messages via the CLI, or through an SNMP agent. However, the commands you use are different. Table 11-3 lists the commands you use to record and clear events for viewing using the CLI, and the commands used to trap events and clear traps for SNMP.

Table 11-3: Commands Used to Log and Trap Event Messages

Command	Description
display	Specifies which events are logged by ELS so you can display them using the CLI.
nodisplay	Clears previously configured events so they are *not* logged by ELS for display using the CLI.
trap	Specifies which events are trapped and sent to SNMP.
notrap	Clears previously configured events so they are *not* trapped and sent to SNMP.

Refer to the Displaying the Event Log section for information about how to display the specified events through the CLI. For information about how to display events sent to SNMP, refer to the appropriate vendor documentation that supports the particular SNMP-based agent you are using.

Special Convention Used in This Section

The following sections present instructions for recording events you plan to view through the CLI and those instructions used to view events via SNMP. The steps you perform are the same for both viewing methods; however, the commands are different. A command used to trap events, or to clear a trap, are enclosed in parentheses and immediately follow the command used to record events to be viewed via the CLI.

Example

`ELS config>`**display** (**trap**) **subsystem** ***subsystem-shortname***

You can use only one command (**display** or **trap**) at a time. Do not enter the parentheses when using the SNMP-related commands.

Configuring ELS in Nonvolatile Memory

This section describes how to configure ELS in nonvolatile memory (NVRAM). Configurations you set in nonvolatile memory require that you restart the module to take effect. These settings survive power outages and module restarts. This mode is most useful when configuring selection criteria for events you want to monitor on a regular basis.

The following tasks are presented in this section:

- Recording and clearing events by subsystem
- Recording and clearing events by subsystem and logging level
- Recording and clearing all occurrences of an event
- Recording and clearing events by group
- Clearing all previously configured events
- Setting the maximum number of traps per second
- Viewing current configuration settings

Recording and Clearing Events By Subsystem

You can configure ELS to record all events generated by one or more subsystems. For example, you might want to log all events related to the ARP subsystem. Once you configure ELS to record all events generated by a subsystem, that setting remains in effect until you clear it. Assume, for example, you first configure ELS to record events generated by the STP subsystem, and you later decide you want to record events from only the ARP subsystem. In this situation, you must both clear the STP subsystem setting *and* configure ELS to record ARP subsystem events. If you do *not* clear the STP subsystem, events from both the STP and ARP subsystems are recorded.

Recording Events By Subsystem

To record events by subsystem, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **els**.
2	Press Return. The `ELS config>` prompt is displayed.
3	Enter **display** (**trap**) **subsystem** ***subsystem-shortname***, where ***subsystem-shortname*** is the short name for the desired subsystem. Refer to Table 11-1 for a list of short names, or enter **display** (**trap**) **subsystem ?** at the `ELS config>` prompt to display a list of short names on your console.

Step	Action
4	Press Return. The ELS is configured to record all messages generated by the specified subsystem using the Standard logging level, and the `ELS config>` prompt is displayed. If ELS was previously configured to record events from other subsystems or using other logging levels, those settings also remain in effect until you clear them.
5	If you want to configure ELS to display events generated by yet another subsystem, repeat steps 3 and 4.
6	Restart the module if you want the new configuration settings to take effect.

Example

`ELS config>`**display subsystem arp**

or

`ELS config>`**trap subsystem arp**

Clearing Events By Subsystem

To clear event recording by subsystem, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **els**.
2	Press Return. The `ELS config>` prompt is displayed.
3	Enter **nodisplay** (**notrap**) **subsystem** ***subsystem-shortname***, where ***subsystem-shortname*** is the short name for the subsystem you want to clear. Refer to Table 11-1 for a list of short names, or enter **nodisplay** (**notrap**) **subsystem ?** at the `ELS config>` prompt to display a list of short names on your console.
4	Press Return. The ELS is configured not to record messages generated by the specified subsystem, and the `ELS config>` prompt is displayed. If ELS was previously configured to record events from other subsystems, those settings remain in effect until you clear them.
5	If you want to clear event recording for yet another subsystem, repeat steps 3 and 4.

Step	Action
6	Restart the module if you want the new configuration settings to take effect.

Example

`ELS config>`**nodisplay subsystem arp**

or

`ELS config>`**notrap subsystem arp**

Recording and Clearing Events By Subsystem and Logging Level

You can configure ELS to record all events generated by a specific subsystem and associated with a particular logging level. For example, you might want to log all events related to STP that are caused by common external errors (the CE-ERROR logging level). Once you configure ELS to record all events generated by a subsystem and an associated logging level, those settings remain in effect until you clear them.

Assume, for example, you first configure ELS to record events generated by the STP subsystem and associated with the P-TRACE logging level, and you later decide you want to record STP events associated with only the U-TRACE logging level. In this situation, you must both clear the P-TRACE logging level from the STP subsystem *and* configure ELS to record STP events associated with the U-TRACE logging level. If you do *not* clear the P-TRACE logging level, STP events associated with both the P-TRACE and U-TRACE logging levels are recorded.

Recording Events By Subsystem and Logging Level

To record events by subsystem and logging level, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **els.**
2	Press Return. The `ELS config>` prompt is displayed.
3	Enter **display** (**trap**) **subsystem** ***subsystem-shortname logging-level***, where ***subsystem-shortname*** is the short name for the desired subsystem and ***logging-level*** is the desired logging level. Refer to Table 11-1 for a list of short names, or enter **display** (**trap**) **subsystem ?** at the `ELS config>` prompt to display a list of short names on your console. Refer to Table 11-2 for a list of logging levels, or enter **display** (**trap**) **subsystem** ***subsystem-shortname*** **?** at the `ELS config>` prompt to display a list of logging levels.

Step	Action
4	Press Return. The ELS is configured to record all messages generated by the specified subsystem and associated with the logging level, and the `ELS config>` prompt is displayed. If ELS was previously configured to record events associated with other logging levels in the same or other subsystems, those settings also remain in effect until you clear them.
5	If you want to configure ELS to record all events associated with other logging levels in the same or other subsystems, repeat steps 3 and 4.
6	Restart the module if you want the new configuration settings to take effect.

Example

`ELS config>`**display subsystem stp ce-error**

or

`ELS config>`**trap subsystem stp ce-error**

Clearing Events By Subsystem and Logging Level

To clear events by subsystem and logging level, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **els**.
2	Press Return. The `ELS config>` prompt is displayed.
3	Enter **nodisplay** (**notrap**) **subsystem** ***subsystem-shortname logging-level***, where ***subsystem-shortname*** is the short name for the desired subsystem and ***logging-level*** is the logging level you want to clear. Refer to Table 11-1 for a list of short names, or enter **nodisplay** (**notrap**) **subsystem ?** at the `ELS config>` prompt to display a list of short names on your console. Refer to Table 11-2 for a list of logging levels, or enter **nodisplay** (**notrap**) **subsystem** ***subsystem-shortname*** **?** at the `ELS config>` prompt to display a list of logging levels.
4	Press Return. The ELS is configured *not* to record messages generated by the specified subsystem and logging level, and the `ELS config>` prompt is displayed. If ELS was previously configured to record events associated with other logging levels in the same or other subsystems, those settings remain in effect until you clear them.

Step	Action
5	If you want to clear event recording associated with other logging levels in the same or other subsystems, repeat steps 3 and 4.
6	Restart the module if you want the new configuration settings to take effect.

Example

`ELS config>`**nodisplay subsystem stp ce-error**

or

`ELS config>`**notrap subsystem stp ce-error**

Recording and Clearing All Occurrences of an Event

You can configure ELS to record all occurrences of a particular event. For example, you might want to record each time STP restarts the BPDU Hello Timer. The event number for this event is STP.028.

Once you configure ELS to record all occurrences of an event, that setting remains in effect until you clear it. Assume, for example, you first configure ELS to record each time STP restarts the BPDU Hello Timer, and you later decide you want to record only when a BootP request is received on an interface (event number BTP.001). In this situation, you must both clear the STP.028 event number *and* configure ELS to record each time a BootP request is received on an interface. If you do *not* clear the STP.028 event number, all occurrences of both events (STP.028 and BTP.001) are recorded.

Recording All Occurrences of an Event

To record all occurrences of an event, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **els**.
2	Press Return. The `ELS config>` prompt is displayed.
3	Enter **display** (**trap**) **event** ***subsystem.event#***, where ***subsystem.event#*** is the event number for the event you want to record. Refer to the Viewing Current Configuration Settings section for information about how to display event numbers associated with one or all subsystems.

Step	Action
4	Press Return. The ELS is configured to record all occurrences of the specified event, and the `ELS config>` prompt is displayed. If ELS was previously configured to record all occurrences of other individual events, those settings also remain in effect until you clear them.
5	If you want to configure ELS to record all occurrences of another individual event, repeat steps 3 and 4.
6	Restart the module if you want the new configuration settings to take effect.

Example

`ELS config>`**display event stp.028**

or

`ELS config>`**trap event stp.028**

Clearing All Occurrences of an Event

To clear all occurrences of an event, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **els**.
2	Press Return. The `ELS config>` prompt is displayed.
3	Enter **nodisplay** (**notrap**) **event** ***subsystem.event#***, where ***subsystem.event#*** is the event number for the event you want to clear. Refer to the Viewing Current Configuration Settings section for information about how to display event numbers associated with one or all subsystems.
4	Press Return. The ELS is configured *not* to record all occurrences of the specified event, and the `ELS config>` prompt is displayed. If ELS was previously configured to record all occurrences of other individual events, those settings remain in effect until you clear them.
5	If you want to clear recording of all occurrences of other individual events, repeat steps 3 and 4.
6	Restart the module if you want the new configuration settings to take effect.

Example

`ELS config>`**nodisplay event stp.028**

or

`ELS config>`**notrap event stp.028**

Recording and Clearing Events By Group

You can configure ELS to record all occurrences of each event that is included in a group. For example, you might want to regularly record each time STP restarts the BPDU Hello Timer (event number STP.028), and each time a BPDU is received (event number STP.001). A group is a customized list of one or more event numbers that you define as members of a group. Configuring ELS using groups is most useful when you have combinations of events that you need to record regularly and helps eliminate the need to enter the desired event numbers individually. The name you assign to a group when you create it should reflect the type of events the group contains so that you can more easily distinguish between groups.

Once you configure ELS to record all occurrences of events that are members of a group, that setting remains in effect until you clear it.

Creating a New Group and Adding Events to an Existing Group

You must create a group before you can configure ELS to record all occurrences of events in a group.

To create a group or add events to an existing group, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **els**.
2	Press Return. The `ELS config>` prompt is displayed.
3	Enter **add** ***group-name subsystem.event-number***, where ***group-name*** is the name of a new group you want to create or is the name of an existing group to which you want to add an event, and ***subsystem.event-number*** is the name of the event you want to add to the group. The group name must begin with an alphabetic character. All subsequent characters can be alphabetic or numeric. ELS is case sensitive with respect to group names. The name you assign to a group should reflect the type of events the group contains, so that you can more easily distinguish between groups. For example, a group that is used to list particular types of Spanning Tree Protocol events might be named stp2.
4	Press Return. The group is created or modified with the specified event entries, and the `ELS config>` prompt is displayed.

Step	Action
5	Repeat steps 3 and 4 for each event you want to add to a group.
6	Restart the module if you want the new configuration settings to take effect.

Example

`ELS config>`**add stp2 stp.001**

and

`ELS config>`**add stp2 stp.028**

Deleting an Event From a Group and Deleting an Entire Group

You can delete either a single event from an existing group or you can delete a group and all of its contents.

To delete an event from a group or to delete and entire group, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **els**.
2	Press Return. The `ELS config>` prompt is displayed.
3	If you want to delete an event from a group, enter **delete** ***group-name subsystem.event-number***, where ***group-name*** is the name of the group containing the event you want to delete, and ***subsystem.event-number*** is the name of the event you want to delete. ELS is case sensitive with respect to group names. If you want to delete an entire group, including its contents, enter **delete** ***group-name*** **all**, where ***group-name*** is the name of the group you want to delete. Refer to the Viewing Current Configuration Settings section for information about how to display a list of current groups and the events that compose each group.
4	Press Return. The event or group is deleted as specified. If you are deleting the last event in a group, a message is displayed to notify you of the fact. If you are not deleting the last event in a group, the `ELS config>` prompt is displayed.

Step	Action
5	If you are deleting events from a group and you want to delete another event, repeat steps 3 and 4 for each event you want to delete from the group.
6	Restart the module if you want the deletion to take effect.

Example

`ELS config>`**delete stp2 stp.001**

and

`ELS config>`**delete stp2 all**

Recording All Occurrences of Events in a Group

To record all occurrences of events in a group, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **el**s.
2	Press Return. The `ELS config>` prompt is displayed.
3	Enter **di**splay (**t**rap) **g**roup ***group-name***, where ***group-name*** is the name of the group containing the events you want to record. Refer to the Viewing Current Configuration Settings section for information about how to display a list of current groups and the events that compose each group.
4	Press Return. The ELS is configured to record all occurrences of the events specified in the group, and the `ELS config>` prompt is displayed. If ELS was previously configured to record all occurrences of events in other groups, those settings also remain in effect until you clear them.
5	If you want to configure ELS to record all occurrences of events in another group, repeat steps 3 and 4.
6	Restart the module if you want the new configuration settings to take effect.

Example

```
ELS config>display group mygroup
```

or

```
ELS config>trap group mygroup
```

Clearing All Occurrences of Events in a Group

To clear all occurrences of events in a group, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **els**.
2	Press Return. The `ELS config>` prompt is displayed.
3	Enter **nodisplay** (**notrap**) **group** ***group-name***, where ***group-name*** is the name of the group for which you do *not* want to record events.
4	Press Return. ELS is configured *not* to record all occurrences of events in the specified group, and the `ELS config>` prompt is displayed. If ELS was previously configured to record all occurrences of events in other groups, those settings remain in effect until you clear them.
5	If you want to clear recording of events in another group, repeat steps 3 and 4.
6	Restart the module if you want the new configuration settings to take effect.

Example

```
ELS config>nodisplay group mygroup
```

or

```
ELS config>notrap group mygroup
```

Clearing All Previously Configured Events

You can clear ELS so that all events that it was previously configured to log are no longer recorded. This includes all events configured to be recorded by subsystem, by subsystem and logging level, by event number, and by group, and for both CLI and SNMP display. When you clear all previously configured events, no events are logged to ELS. Clearing ELS also resets the maximum number of traps per second to its default.

To clear ELS so that all events that it was previously configured to log are no longer recorded, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **els**.
2	Press Return. The `ELS config>` prompt is displayed.
3	Enter **clear**.

4	Press Return. The following message is displayed:
	`You are about to clear all ELS configuration information.`
	`Are you sure you want to do this (Yes or [No]):`

5	If you want to clear all ELS configuration information, enter **y**. If you do not want to clear all ELS configuration information, enter **n**.
6	Press Return. The `ELS config>` prompt is displayed.
7	Restart the module if you want the new configuration setting to take effect. All events for which ELS was previously configured to log are no longer recorded.

Setting Maximum Number of Traps Per Second

You can configure ELS to limit the number of events that are trapped per second. This option is most useful when conditions result in such large numbers, or "bursts," of events that you are overwhelmed by the data. Reducing the maximum number of traps per second effectively results in a sampling of the events.

The default value for the maximum number of traps per second is 0 (zero), meaning an unlimited number of traps per second is permitted. The maximum number of traps per second can be reset to its default setting by using the **clear** command. (Refer to the Clearing All Previously Configured Events section.)

To set the maximum number of traps per second, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **els**.
2	Press Return. The `ELS config>` prompt is displayed.
3	Enter **set pin**.

Step	Action
4	Press Return. The following message is displayed: `events/second [0]?`
5	Enter the maximum number of events per second you want trapped. The range of acceptable values is 1 through 57600 traps per second. The default is 0 (zero), an unlimited number of events per second.
6	Press Return. The maximum number of events trapped is set, and the `ELS config>` prompt is displayed.
7	Restart the module if you want the new configuration setting to take effect.

Viewing Current Configuration Settings

You can view several reports that detail the current ELS configuration settings in NVRAM. You may find these reports helpful if, for example, you want to check the settings before restarting the module and before displaying the event log. (Refer to the Displaying the Event Log section for information about how to display events.)

To view current configuration settings in NVRAM, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **els**.
2	Press Return. The `ELS config>` prompt is displayed.
3	Enter **list** ***command-option***, where ***command-option*** is the command you must enter to display the desired information. Refer to Table 11-4 for a list of commands, and for a description of the type of information that is displayed when you enter the command.
4	Press Return. A report containing the desired information is displayed and the `ELS config>` prompt is displayed.

Table 11-4: List Command Options and Descriptions

Command Option	Description
groups	Lists all group names and the events that compose each group.
pin	Displays the current maximum number of traps per second (pin).
status	Lists all event logging configurations by subsystem, subsystem and logging level, group, and event number. The information includes configurations for events that will be displayed through the CLI and those to be trapped for use by SNMP.
subsystem	Lists the short names for all possible subsystems, the number of different events that can be generated by the subsystem, and an expanded description of the subsystem short name.
subsystem *subsystem*	Lists all possible events that can be generated by a specified subsystem, where ***subsystem*** is the short name for the subsystem for which you want to list events. The information included for each event includes the event number, the logging level for the event, and a short description of the event.
subsystems all	Lists all possible events that can be generated by all subsystems. The information included for each event includes the event number, the logging level for the event, and a short description of the event.

Command Option	Description
all	Lists the following configuration information for events to be displayed through the CLI, and those to be trapped for use by SNMP: • Short names for all possible subsystems, the number of different events that can be generated by each subsystem, and an expanded description of each subsystem short name • All event logging configurations by subsystem, subsystem and logging level, group, and event number • The (pin) value for the maximum number of traps per second

Configuring ELS in Volatile Memory

This section describes how to configure ELS in volatile RAM. Configurations you set in volatile memory *do not* require that you restart the module to take effect. These settings *do not* survive power outages and module restarts. Configuring ELS in volatile memory is most useful when configuring selection criteria you want to remain in effect only temporarily, and that you are likely to change from moment to moment as you troubleshoot a particular problem.

The following tasks are presented in this section:

- Recording and clearing events by subsystem
- Recording and clearing events by subsystem and logging level
- Recording and clearing all occurrences of an event
- Recording and clearing events by group
- Clearing historical entries from the log
- Setting the maximum number of traps per second
- Saving and managing a configuration in NVRAM
- Restoring default settings
- Viewing current configuration settings

Recording and Clearing Events By Subsystem

You can configure ELS to record all events generated by one or more subsystems. For example, you might want to log all events related to the ARP subsystem. Once you configure ELS to record all events generated by a subsystem, that setting remains in effect until you clear it. Assume, for example, you first configure ELS to record events generated by the STP subsystem, and you later decide you want to record events from only the ARP subsystem. In this situation, you must both clear the STP subsystem setting *and* configure ELS to record ARP subsystem events. If you do *not* clear the STP subsystem, events from both the STP and ARP subsystems are recorded.

Recording Events By Subsystem

To record events by subsystem, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **els**.
2	Press Return. The `ELS>` prompt is displayed.
3	Enter **display** (**trap**) **subsystem** ***subsystem-shortname***, where ***subsystem-shortname*** is the short name for the desired subsystem. Refer to Table 11-1 for a list of short names, or enter **display** (**trap**) **subsystem ?** at the `ELS>` prompt to display a list of short names on your console.
4	Press Return. The ELS is configured to record all messages generated by the specified subsystem, and the `ELS>` prompt is displayed. If ELS was previously configured in volatile memory to record events from other subsystems, or if ELS was configured in NVRAM, those settings also remain in effect until you clear them.
5	If you want to configure ELS to display events generated by yet another subsystem, repeat steps 3 and 4.

Example

`ELS>`**display subsystem arp**

or

`ELS>`**trap subsystem arp**

Clearing Events By Subsystem

Clearing events in volatile memory causes ELS to stop recording any *new* events generated by the specified subsystem. Events already recorded (historical entries) are still displayed and may be visible at the upper portion of the log. Refer to the Clearing Historical Entries From the Log section for information about how to clear historical entries.

To clear event recording by subsystem, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **els**.
2	Press Return. The `ELS>` prompt is displayed.
3	Enter **nodisplay** (**notrap**) **subsystem** ***subsystem-shortname***, where ***subsystem-shortname*** is the short name for the subsystem you want to clear. Refer to Table 11-1 for a list of short names, or enter **nodisplay** (**notrap**) **subsystem ?** at the `ELS>` prompt to display a list of short names on your console.
4	Press Return. The ELS is configured not to record messages generated by the specified subsystem, and the `ELS>` prompt is displayed. If ELS was previously configured in volatile memory to record events from other subsystems, or if other subsystems were configured in NVRAM, those settings remain in effect until you clear them.
5	If you want to clear event recording for yet another subsystem, repeat steps 3 and 4.

Example

`ELS>`**nodisplay subsystem arp**

or

`ELS>`**notrap subsystem arp**

Recording and Clearing Events By Subsystem and Logging Level

You can configure ELS to record all events generated by a specific subsystem and associated with a particular logging level. For example, you might want to log all events related to STP that are caused by common external errors (the CE-ERROR logging level). Once you configure ELS to record all events generated by a subsystem and an associated logging level, those settings remain in effect until you clear them. Assume, for example, you first configure ELS to record events generated by the STP subsystem and associated with the P-TRACE logging level, and you later decide you

want to record STP events associated with only the U-TRACE logging level. In this situation, you must both clear the P-TRACE logging level from the STP subsystem *and* configure ELS to record STP events associated with the U-TRACE logging level. If you do *not* clear the P-TRACE logging level, STP events associated with both the P-TRACE and U-TRACE logging levels are recorded.

Recording Events By Subsystem and Logging Level

To record events by subsystem and logging level, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **els**.
2	Press Return. The `ELS>` prompt is displayed.
3	Enter **display** (**trap**) **subsystem** ***subsystem-shortname logging-level***, where ***subsystem-shortname*** is the short name for the desired subsystem and ***logging-level*** is the desired logging level. Refer to Table 11-1 for a list of short names, or enter **display** (**trap**) **subsystem ?** at the `ELS>` prompt to display a list of short names on your console. Refer to Table 11-2 for a list of logging levels, or enter **display** (**trap**) **subsystem** ***subsystem-shortname*** **?** at the `ELS>` prompt to display a list of logging levels.
4	Press Return. The ELS is configured to record all messages generated by the specified subsystem and associated with the specified logging level, and the `ELS>` prompt is displayed. If ELS was previously configured in volatile memory to record events associated with other logging levels in the same or other subsystems, or if other subsystems or logging levels were configured in NVRAM, those settings also remain in effect until you clear them.
5	If you want to configure ELS to record all events associated with other logging levels in the same or other subsystems, repeat steps 3 and 4.

Example

`ELS>`**display subsystem stp ce-error**

or

`ELS>`**trap subsystem stp ce-error**

Clearing Events By Subsystem and Logging Level

Clearing events in volatile memory causes ELS to stop recording any *new* events generated by the specified subsystem, and associated with the specified logging level. Events already recorded (historical entries) are still displayed and may be visible at the upper portion of the log. Refer to the Clearing Historical Entries From the Log section for information about how to clear historical entries.

To clear events by subsystem and logging level, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **els**.
2	Press Return. The `ELS>` prompt is displayed.
3	Enter **nodisplay** (**notrap**) **subsystem** ***subsystem-shortname logging-level***, where ***subsystem-shortname*** is the short name for the desired subsystem and ***logging-level*** is the logging level you want to clear. Refer to Table 11-1 for a list of short names, or enter **nodisplay** (**notrap**) **subsystem ?** at the `ELS>` prompt to display a list of short names on your console. Refer to Table 11-2 for a list of logging levels, or enter **nodisplay** (**notrap**) **subsystem** ***subsystem-shortname*** **?** at the `ELS>` prompt to display a list of logging levels.
4	Press Return. The ELS is configured *not* to record messages generated by the specified subsystem and logging level, and the `ELS>` prompt is displayed. If ELS was previously configured in volatile memory to record events associated with other logging levels in the same or other subsystems, or if other subsystems or logging levels were configured in NVRAM, those settings remain in effect until you clear them.
5	If you want to clear event recording associated with other logging levels in the same or other subsystems, repeat steps 3 and 4.

Example

`ELS>`**nodisplay subsystem stp ce-error**

or

`ELS>`**notrap subsystem stp ce-error**

Recording and Clearing All Occurrences of an Event

You can configure ELS to record all occurrences of a particular event. For example, you might want to record each time STP restarts the BPDU Hello Timer. The event number for this event is STP.028.

Once you configure ELS to record all occurrences of an event, that setting remains in effect until you clear it. Assume, for example, you first configure ELS to record each time STP restarts the BPDU Hello Timer, and you later decide you want to record only when a BootP request is received on an interface (event number BTP.001). In this situation, you must both clear the STP.028 event number *and* configure ELS to record each time a BootP request is received on an interface. If you do *not* clear the STP.028 event number, all occurrences of both events (STP.028 and BTP.001) are recorded.

Recording All Occurrences of an Event

To record all occurrences of an event, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **els**.
2	Press Return. The `ELS config>` prompt is displayed.
3	Enter **display** (**trap**) **event** ***subsystem.event#***, where ***subsystem.event#*** is the event number for the event you want to record. Refer to the Viewing Current Configuration Settings and Statistics section for information about how to display event numbers associated with one or all subsystems.
4	Press Return. The ELS is configured to record all occurrences of the specified event, and the `ELS>` prompt is displayed. If ELS was previously configured in volatile memory to record events based on other criteria, or if other event selection criteria were configured in NVRAM, those settings also remain in effect until you clear them.
5	If you want to configure ELS to record all occurrences of another individual event, repeat steps 3 and 4.

Example

`ELS>`**display event stp.028**

or

`ELS>`**trap event stp.028**

Clearing All Occurrences of an Event

Clearing events in volatile memory causes ELS to stop recording any *new* events that match the specified event number. Events already recorded (historical entries) are still displayed and may be visible at the upper portion of the log. Refer to the Clearing Historical Entries From the Log section for information about how to clear historical entries.

To clear all occurrences of an event, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **els**.
2	Press Return. The `ELS>` prompt is displayed.
3	Enter **nodisplay** (**notrap**) **event** ***subsystem.event#***, where ***subsystem.event#*** is the event number for the event you want to clear. Refer to the Viewing Current Configuration Settings and Statistics section for information about how to display event numbers associated with one or all subsystems.
4	Press Return. The ELS is configured *not* to record all occurrences of the specified event, and the `ELS>` prompt is displayed. If ELS was previously configured in volatile memory to record events based on other criteria, or if other event selection criteria were configured in NVRAM, those settings remain in effect until you clear them.
5	If you want to clear recording of all occurrences of other individual events, repeat steps 3 and 4.

Example

`ELS>`**nodisplay event stp.028**

or

`ELS>`**notrap event stp.028**

Recording and Clearing Events By Group

You can configure ELS to record all occurrences of each event that is included in a group. For example, you might want to regularly record each time STP restarts the BPDU Hello Timer (event number STP.028), and each time a BPDU is received from a specified MAC address (event number STP.001). A group is a customized list of one or more event numbers that you define as members of a group. Configuring ELS using groups is most useful when you have combinations of events that you need to record regularly and helps eliminate the need to enter the desired event numbers individually.

The name you assign to a group when you create it should reflect the type of events the group contains so that you can more easily distinguish between groups. Refer to the Configuring ELS in Nonvolatile Memory section for information about how to create, modify, and delete groups.

Once you configure ELS to record all occurrences of events that are members of a group, that setting remains in effect until you clear it.

Recording All Occurrences of Events in a Group

To record all occurrences of events in a group, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **els**.
2	Press Return. The `ELS config>` prompt is displayed.
3	Enter **display** (**trap**) **group** ***group-name***, where ***group-name*** is the name of the group containing the events you want to record.
4	Press Return. The ELS is configured to record all occurrences of the events specified in the group, and the `ELS>` prompt is displayed. If ELS was previously configured in volatile memory to record events based on other criteria, or if other event selection criteria were configured in NVRAM, those settings also remain in effect until you clear them.
5	If you want to configure ELS to record all occurrences of events in another group, repeat steps 3 and 4.

Example

`ELS>`**display group mygroup**

or

`ELS>`**trap group mygroup**

Clearing All Occurrences of Events in a Group

Clearing events in volatile memory causes ELS to stop recording any *new* events that match the specified group. Events already recorded (historical entries) are still displayed and may be visible at the upper portion of the log. Refer to the Clearing Historical Entries From the Log section for information about how to clear historical entries.

To clear all occurrences of events in a group, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **els**.
2	Press Return. The `ELS>` prompt is displayed.
3	Enter **nodisplay** (**notrap**) **group** ***group-name***, where ***group-name*** is the name of the group for which you do *not* want to record events.
4	Press Return. ELS is configured *not* to record all occurrences of events in the specified group, and the `ELS>` prompt is displayed. If ELS was previously configured in volatile memory to record events based on other criteria, or if other criteria are configured in NVRAM, those settings remain in effect until you clear them.
5	If you want to clear recording of events in another group, repeat steps 3 and 4.

Example

`ELS>`**nodisplay group mygroup**

or

`ELS>`**notrap group mygroup**

Clearing Historical Entries From the Log

You can clear ELS so that all *historical* entries in the log, matching the specified criteria, are deleted. This includes all events configured to be recorded by subsystem, by subsystem and logging level, by event number, and by group, and for both CLI and SNMP display. When you clear historical entries, new events continue to be recorded to the log, even if they match the criteria used to clear entries.

Clearing Historical Entries By Subsystem

To clear ELS so that all historical entries are deleted from the log by subsystem, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **els**.
2	Press Return. The `ELS>` prompt is displayed.

Step	Action
3	Enter **clear subsystem** ***subsystem-shortname***, where ***subsystem-shortname*** is the short name for the subsystem you want to clear. Refer to Table 11-1 for a list of short names, or enter **list subsystem ?** at the ELS> prompt to display a list of short names on your console.
4	Press Return. The ELS deletes all historical entries in the log that match the specified subsystem, and the ELS> prompt is displayed. If ELS was previously configured in volatile memory to record events from other subsystems, or if other subsystems were configured in NVRAM, those settings remain in effect until you clear them.
5	If you want to clear historical entries for yet another subsystem, repeat steps 3 and 4.

Clearing Historical Entries By Subsystem and Logging Level

To clear historical entries by subsystem and logging level, perform the following steps:

Step	Action
1	At the Monitor prompt (Monitor>), enter **els**.
2	Press Return. The ELS> prompt is displayed.
3	Enter **clear subsystem** ***subsystem-shortname logging-level***, where ***subsystem-shortname*** is the short name for the desired subsystem and ***logging-level*** is the logging level you want to clear. Refer to Table 11-1 for a list of short names, or enter **list subsystem ?** at the ELS> prompt to display a list of short names on your console. Refer to Table 11-2 for a list of logging levels, or enter **list subsystem** ***subsystem-shortname*** **?** at the ELS> prompt to display a list of events and associated logging levels.
4	Press Return. The ELS deletes historical entries from the log that match the specified subsystem and logging level, and the ELS> prompt is displayed. If ELS was previously configured in volatile memory to record events associated with other logging levels in the same or other subsystems, or if other subsystems or logging levels were configured in NVRAM, those settings remain in effect until you clear them.
5	If you want to clear historical entries associated with other logging levels in the same or other subsystems, repeat steps 3 and 4.

Clearing All Historical Entries of a Specific Event

To clear all historical entries of a specific event, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **els**.
2	Press Return. The `ELS>` prompt is displayed.
3	Enter **clear event** ***subsystem.event#***, where ***subsystem.event#*** is the event number for the event you want to clear. Refer to the Viewing Current Configuration Settings and Statistics section for information about how to display event numbers associated with one or all subsystems.
4	Press Return. The ELS deletes all historical entries of the specified event from the log, and the `ELS>` prompt is displayed. If ELS was previously configured in volatile memory to record events based on other criteria, or if other event selection criteria were configured in NVRAM, those settings remain in effect until you clear them.
5	If you want to clear recording of all occurrences of other individual events, repeat steps 3 and 4.

Clearing Historical Entries By Group

To clear all historical entries associated with events in a group, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **els**.
2	Press Return. The `ELS>` prompt is displayed.
3	Enter **clear group** ***group-name***, where ***group-name*** is the name of the group for which you do *not* want to record events.
4	Press Return. ELS deletes all historical entries associated with events in the specified group, and the `ELS>` prompt is displayed. If ELS was previously configured in volatile memory to record events based on other criteria, or if other criteria are configured in NVRAM, those settings remain in effect until you clear them.
5	If you want to clear recording of events in another group, repeat steps 3 and 4.

Setting Maximum Number of Traps Per Second

You can configure ELS to limit the number of events that are trapped per second. This option is most useful when conditions result in such large numbers, or "bursts," of events that you are overwhelmed by the data. Reducing the maximum number of traps per second effectively results in a sampling of the events.

The default value for the maximum number of traps per second in volatile memory is equal to the maximum number of traps/second value set for NVRAM. (Refer to the Configuring ELS in Nonvolatile Memory section.)

To set the maximum number of traps per second, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **els**.
2	Press Return. The `ELS>` prompt is displayed.
3	Enter **set pin**.
4	Press Return. The following message is displayed: `events/second [0]?`
5	Enter the maximum number of events per second you want trapped. The range of acceptable values is 1 through 57600 traps per second. A value of 0 (zero), indicates an unlimited number of events per second.
6	Press Return. The maximum number of events trapped is set, and the `ELS>` prompt is displayed.

Saving and Managing a Configuration in NVRAM

You can save an ELS volatile memory configuration in NVRAM. The configuration settings are saved in NVRAM, separate from the ELS NVRAM settings configured from the Config prompt. You may want to save volatile settings in NVRAM if, for example, you want to try a different ELS configuration, but want to retain the current settings for later use. You may also want to save volatile settings in NVRAM if you plan to continue to use the settings at a later time, and you want to ensure the settings are still available if a power outage or restart occurs.

You can retrieve and reload volatile ELS configuration settings you previously saved in NVRAM. Retrieving settings from NVRAM does not delete the settings from NVRAM. You must perform a separate operation to delete (remove) the saved NVRAM.

Saving Volatile Settings in NVRAM

To save a volatile ELS configuration in NVRAM, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **els**.
2	Press Return. The `ELS>` prompt is displayed.
3	Enter **save**.
4	Press Return. The volatile settings are stored in NVRAM, separate from ELS settings configured from the Config prompt. The `ELS>` prompt is displayed.

Retrieving Settings From NVRAM

To retrieve previously saved (volatile settings) from NVRAM, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **els**.
2	Press Return. The `ELS>` prompt is displayed.
3	Enter **retrieve**.
4	Press Return. The settings stored in NVRAM are retrieved and reloaded as an ELS volatile configuration, and the `ELS>` prompt is displayed. The NVRAM copy of the settings from which the reload occurred is retained. (Refer to the Deleting Settings Saved in NVRAM section for information about how to delete (remove) the NVRAM copy.)

Deleting Settings Saved in NVRAM

To delete (remove) previously saved (volatile) settings from NVRAM, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **els**.
2	Press Return. The `ELS>` prompt is displayed.
3	Enter **remove**.
4	Press Return. The settings stored in NVRAM are deleted and the `ELS>` prompt is displayed.

Restoring Default Settings

You can restore ELS volatile memory configuration defaults using the restore command. (Refer to Appendix B for a list of ELS volatile memory configuration default settings.) Restoring the default settings also stops ELS from recording events based on prior settings in volatile memory. However, ELS continues to record events that match selection criteria configured in NVRAM, if any.

To restore ELS volatile memory configuration defaults, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **els**.
2	Press Return. The `ELS>` prompt is displayed.
3	Enter **restore**.
4	Press Return. The default settings are restored and the `ELS>` prompt is displayed.

Viewing Current Configuration Settings and Statistics

Viewing Current Configuration Settings

You can view several reports that detail the current ELS configuration settings in volatile memory. Some reports include a count of specific events being recorded. You may find these reports helpful if, for example, you want to check the settings before displaying the event log. (Refer to the Displaying the Event Log section for information about how to display events.)

To view current configuration settings in volatile memory, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **els**.
2	Press Return. The `ELS>` prompt is displayed.
3	Enter **list** ***command-option***, where ***command-option*** is the command you must enter to display the desired information. Refer to Table 11-5 for a list of commands, and for a description of the type of information that is displayed when you enter the command.
4	Press Return. A report containing the desired information is displayed and the `ELS>` prompt is displayed.

Table 11-5: List Command Options and Descriptions

Command Option	Description
active *subsystem-name*	Lists the following information about a specific subsystem, where ***subsystem-name*** is the subsystem: • Events configured for logging (active events). A *D* in the `Active` column of the report indicates the event is configured to be logged for display through the module's CLI. A *T* in the `Active` column of the report indicates the event is configured to be trapped for remote (SNMP) management. • Number of occurrences of each event.
event *event-name*	Displays the following information about the specified event, where ***event-name*** is the name of the event: • Logging level. • Short form of the message. • Whether the event is configured for logging (active event). A *D* in the `Active` column of the report indicates the event is configured to be logged for display through the module's CLI. A *T* in the `Active` column of the report indicates the event is configured to be trapped for remote (SNMP) management.
groups	Lists all group names and the events that compose each group.
pin	Displays the current maximum number of traps per second (pin).
subsystems	Lists the short names for all possible subsystems, the number of different events that can be generated by the subsystem, and an expanded description of the subsystem short name.

Command Option	Description
subsystem *subsystem*	Lists all possible events that can be generated by a specified subsystem, where ***subsystem*** is the short name for the subsystem for which you want to list events. The information included for each event includes the event number, the logging level for the event, and a short description of the event.
subsystems all	Lists all possible events that can be generated by all subsystems. The information included for each event includes the event number, the logging level for the event, and a short description of the event.
all	Lists the following configuration information: • Short names for all possible subsystems, the number of different events that can be generated by each subsystem, and an expanded description of each subsystem short name. • All configured groups and the events specified for each group. • The (pin) value for the maximum number of traps per second.

Example

ELS>**list active stp**

```
Event      Active  Count
STP.003    D       0
STP.004    D       0
STP.005    D       0
STP.006    D       0
STP.007    D       0
STP.008    D       0
STP.009    D       0
STP.013    D       0
STP.014    D       0
STP.015    D       0
STP.016    D       0
STP.021    D       0
STP.022            4397
STP.024    D       0
STP.026    D       0
STP.028    D       4397
STP.029    D       0
STP.030    D       0
STP.032    D       0
STP.033    D       0
STP.034    D       0
```

Viewing Configuration Memory Statistics

You can view statistics about ELS configuration volatile memory categorized by subsystem. The report includes the following information for each subsystem:

- Subsystem short name
- Maximum number of events (vector) for the subsystem
- Current number of events that can be generated by the subsystem
- Number of bytes (string) used for all message storage by the subsystem
- Number of events that are active in the subsystem
- Dynamic memory in use by the subsystem

The report also includes totals for each of the above bulleted items, the maximum number of events (vector) of all subsystems, the maximum number of subsystems, and total heap memory size.

To view configuration memory statistics, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **els**.
2	Press Return. The `ELS>` prompt is displayed.
3	Enter **statistics**.
4	Press Return. A report containing configuration memory is displayed, and the `ELS>` prompt is displayed.

Displaying the Event Log

The event log records all event messages until the buffer is full. Each new event then overwrites the oldest existing event in the log. The event log also displays new messages on your console as they occur. The categories of information and level of detail displayed varies, depending on how you configure ELS. (Refer to the Selecting Which Events Are Logged section for information about how to record and display selected information.)

You can display the log of recorded event messages using either the CLI, or using an SNMP-based agent such as DIGITAL's clearVISN MultiChassis Manager. This section describes how to display the log using the CLI. Refer to the appropriate documentation supporting the particular SNMP agent you are using for information about displaying events.

Choosing the Method of Display

You can display the event log from the CLI either directly or indirectly. When displaying the event log directly, you view events only. You cannot perform any other task while viewing the log using this method.

Displaying the event log indirectly enables you to view events while entering commands from any CLI prompt (`Main>`, `Config>`, `Monitor>`, `Bridge>`, and so on). Although this method causes the command line to scroll off the screen as events are displayed, it enables you to more easily view the effect of configuration changes as you make them. This capability may also be of particular use if you need to view events that occur immediately after startup, but that might otherwise scroll off the screen if you first had to access the event log from the Main prompt (`Main>`), as described in the Displaying and Exiting the Event Log section. Displaying the event log indirectly applies only to a terminal or a printer attached to the setup port. It does not affect output accessed via remote devices.

You can set the method of display (direct or indirect) from either the `Config>` prompt or the Monitor prompt (`Monitor>`). Setting the method of display from the `Config>` prompt takes effect immediately, without restarting the module. Because it is stored in NVRAM, the setting survives resets and loss of power. Setting the method of display from the Monitor prompt (`Monitor>`) also takes effect immediately, without restarting the module. However, because the setting is stored in volatile memory it does not survive resets and loss of power.

To choose the method of display, perform the following steps:

Step	Action
1	At either the Config> prompt or the Monitor prompt (Monitor>), enter **set output** ***method-of-display***, where ***method-of-display*** is either the **default** or the **console** command option. The **default** command sets the method of display to direct (you can only view events). The **console** command sets the method of display to indirect (you can view events while entering commands). The default is the **default** command.
2	Press Return. The chosen method of display is set. If you set the method of display to **default**, refer to the Displaying and Exiting the Event Log section for information about how to view the event log directly. If you set the method of display to **console**, the event log is automatically displayed at any CLI prompt you access.

Displaying and Exiting the Event Log

Only one user at a time can access the event log. If another user attempts to access the log while you are using it, the message `Current Process has been Redirected` is displayed and you are returned to the Main prompt (`Main>`). The user who accessed the log receives all redirected output from the log that did not yet display on your screen. The log is displayed at the other user's terminal until the user to whom the output is redirected cancels it.

Displaying the Event Log Directly

To display the event log directly (the method of display is set to **default**), perform the following steps:

Step	Action
1	At the Main prompt (`Main>`) enter **Events**.
2	Press Return. The event log is displayed. All existing event messages are displayed. New event messages are also added to the display as they occur.

Displaying the Event Log Indirectly

If you set the method of display to **console**, the event log is automatically displayed at any CLI prompt you access. If you log out after setting the method of display to **console** and then log in again, the stream of events that are output to the console are immediately displayed. To terminate the stream of output, at the Main prompt enter **halt 2** and press Return.

Exiting the Event Log

If you are viewing the event log directly, enter the intercept character to exit the event log. The default intercept character is Ctrl/P. Refer to Chapter 2 for information about changing the intercept character.

If you are displaying the event log indirectly, you can cancel display of events by entering **set output default** command at either the Config or Monitor prompt. Refer to the Choosing the Method of Display section for information about how to do so.

Advanced Methods for Viewing Events

Refer to Appendix A for information about the following topics that may be useful when viewing the event log directly.

- Viewing output from multiple processes (Events and Config, for example) simultaneously (**divert** command)
- Canceling display of output to a console (**flush** command)
- Terminating process output (**halt** command)

Printing ELS Output

You can obtain a hard copy printout of event messages, including startup messages, by attaching a printing terminal to the setup port on the module. You must then configure the module so that events are displayed directly, as described in the Displaying the Event Log section.

Chapter 12

Configuring Remote Management

Overview

Introduction

You can configure, monitor, and manage DIGITAL GIGAswitch GS2000 line card modules from a remote device using the CLI, a graphical interface, or both. To configure and manage the module remotely using the CLI, you must establish a remote console session. To configure and manage a module using a graphical interface, you must install a MIB-based management system such as the DIGITAL MultiChassis Manager (optional). MultiChassis Manager is a component of the DIGITAL clearVISN network management product.

You must configure certain network parameters and protocols before you can configure a module from a remote console session or from a MIB-based system. This chapter describes how to configure those network connections and protocols.

In This Chapter

The following topics are covered in this chapter:

Configuring the Module for Remote Console Sessions

This section describes how to configure the module to accept remote console sessions. Remote sessions are established by running Telnet on a remote workstation, PC, or terminal server, and connecting through any of the following interfaces:

- The console port
- Any module network interface (FDDI, ATM ELAN, or ATM Bridge Tunnel)

Refer to the module installation and configuration documentation for information about cable installation.

To configure the module for remote console sessions, you must configure TCP/IP Host Services or optionally, IP routing. You must configure TCP/IP Host Services to identify an IP address that can be used to Telnet to a module and establish a remote session. To configure TCP/IP Host Services, refer to the Configuring TCP/IP Host Services section later in this chapter. If IP routing is configured, TCP/IP HST services is automatically disabled (not used).

Configuring the Module for MIB-Based Management Systems

This section describes how to configure the module for remote management using MIB-based management systems.

You must perform the following tasks to configure the module for MIB-based management:

Task	Description
1	Configure TCP/IP Host Services.
2	Configure SNMP.

Configuring TCP/IP Host Services

You must configure TCP/IP Host Services to identify the IP address to which SNMP protocol messages are sent. To configure TCP/IP Host Services, refer to the Configuring TCP/IP Host Services section later in this chapter.

Configuring SNMP

This section describes how to configure and manage the Simple Network Management Protocol (SNMP) to support MIB-based management systems. SNMP is a communications protocol used to configure devices on the network and collect management information from them. The information collected includes such information as traffic overloads, data throughput, and errors. You can then view the collected information using any MIB-based management system such as the DIGITAL clearVISN MultiChassis Manager.

This section assumes you are familiar with SNMP concepts and MIB-based management systems.

Adding and Deleting a Community

SNMP includes a default community named “public.” The public community is assigned write-read-trap access by default. You should change the access assigned to the public community to read-trap and add at least one other community with write-read-trap access. Refer to the Setting Community Access section later in this chapter for information about how to set access.

To add or delete a community to the list of SNMP communities, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **snmp**.
2	Press Return. The `SNMP Config>` prompt is displayed.
3	If you want to add a new community, enter **add community** ***name***, where ***name*** is the name you want to assign to the new community. If you want to delete an existing community, enter **delete community** ***name***, where ***name*** is the name of the community you want to delete.
4	Press Return. The following message is displayed: `Community name []?`
5	Enter a name for the community. The name can be composed of up to 32 alphanumeric characters and cannot include spaces, tabs, or Escape key sequences.
6	Press Return. The community is added or deleted as specified and the `SNMP Config>` prompt is displayed.

Adding and Deleting an Address for a Community

You can specify one or more addresses for each community. However, you can add addresses only one at a time. If you do not specify an address for a community, requests are accepted from any host. The address is also used to specify the hosts that receive the traps. If no address is specified, no traps are generated.

To add an address for a community, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **snmp**.
2	Press Return. The `SNMP Config>` prompt is displayed:
3	If you are adding an address, enter **add address**. If you are deleting an address, enter **delete address**.
4	Press Return. The following message is displayed: `Community name []?`

Step	Action
5	Enter the name of the community for which you want to assign or delete an address. The name can be composed of up to 32 alphanumeric characters and cannot include spaces, tabs, or Escape key sequences.
6	Press Return. The following message is displayed: `IP Address [0.0.0.0]?`
7	Enter the IP address you want to add to or delete from the community.
8	Press Return. If you are adding an address, the following message is displayed: `IP Mask [255.255.255.255]?` If you are deleting an address, go to step 10.
9	Enter the IP mask for the address.
10	Press Return. The address is added or deleted as specified, and the `SNMP Config>` prompt is displayed.

Creating and Managing MIB Views

You can add a MIB view or delete an existing view.

Adding Views

You can add a new view or add a portion (subtree) of the MIB to an existing view. More than one subtree can be added to an existing view.

To create a new view or add a subtree to an existing view, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **snmp**.
2	Press Return. The `SNMP Config>` prompt is displayed.
3	Enter **add subtree**.
4	Press Return. The following message is displayed: `View name []?`

Step	Action
5	If you want to create a new view, enter a name that is not already being used. If you want to add a subtree to an existing view, enter the name of an existing view. The name can be composed of up to 32 alphanumeric characters and cannot include spaces, tabs, or Escape key sequences.
6	Press Return. The following message is displayed: `MIB OID name []?`
7	Enter the numeric value of the MIB Object ID (OID) for which you want to create a new view or add to an existing view. **Example:** `MIB OID name []?`**1.3.6.1.4.1.2**
8	Press Return. The view is created or added to an existing view, and the `SNMP Config>` prompt is displayed.

Deleting Subtrees and Views

To delete a subtree and view, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **snmp**.
2	Press Return. The `SNMP Config>` prompt is displayed.
3	Enter **delete subtree**.
4	Press Return. The following message is displayed: `View name []?`
5	Enter the name of the view you want to delete or the name of the view containing the subtree you want to delete.
6	Press Return. The following message is displayed: `MIB OID name []?`
7	Enter the numeric value of the MIB Object ID (OID) associated with the view you want to delete. **Example:** `MIB OID name []?`**1.3.6.1.4.1.2**

Step	Action
8	Press Return. If you are deleting the last subtree in the view, the subtree and its associated view are deleted, and the `SNMP Config>` prompt is displayed. If subtrees other than the one you are deleting are associated with the specified view, only the specified subtree is deleted and the `SNMP Config>` prompt is displayed. The specified view and all remaining subtrees associated with the view remain intact.

Setting and Managing Community Views and Access

You can assign one or more views and one of three access types to a community.

Setting Community Views

To assign a view to a community, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **snmp**.
2	Press Return. The `SNMP Config>` prompt is displayed.
3	Enter **set community view**.
4	Press Return. The following message is displayed: `Community name []?`
5	Enter the name of the community to which you want to assign a view.
6	Press Return. The following message is displayed: `View name []?`
7	If you want to assign all MIB views (subtrees) to the community, enter the name of the view you want to assign to the community followed by a space and **all**. If you want to assign a selected MIB view (subtree) to the community, enter the name of the view you want to assign to the community followed by a space and the subtree number.
8	Press Return. The specified views are assigned to the community and the `SNMP Config>` prompt is displayed.

Setting Community Access

The default community named “public” is assigned write-read-trap access by default. You should change the access assigned to the public community to read-trap, and add at least one other community with write-read-trap access.

To set read, write, or trap access to a community, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **snmp**.
2	Press Return. The `SNMP Config>` prompt is displayed.
3	Enter **set community access** ***command-option***, where ***command-option*** is one of the community access options listed in Table 12-1.
4	Press Return. The specified access option is assigned to the community and the `SNMP Config>` prompt is displayed.

Table 12-1: Community Access Options

Command Option	Description
read-trap	Sets read access and trap generation for the specified community.
write-read-trap	Sets write and read access and trap generation for the specified community.
trap-only	Sets the trap port to the specified community.

Setting the Trap Port

To specify the User Datagram Protocol (UDP) trap port to which traps are sent, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **snmp**.
2	Press Return. The `SNMP Config>` prompt is displayed.
3	Enter **set trap_port**.
4	Press Return. The following message is displayed: `UDP port [162]?`
5	Enter the UDP port number for the trap port that is to receive traps. The default is the standard trap port (**162**).
6	Press Return. The specified UDP port number is assigned and the `SNMP Config>` prompt is displayed.

Enabling and Disabling SNMP

To enable or disable SNMP, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **snmp**.
2	Press Return. The `SNMP Config>` prompt is displayed.
3	If you want to enable SNMP, enter **enable snmp**. If you want to disable SNMP, enter **disable snmp**. The factory default is enabled.
4	Press Return. SNMP is enabled or disabled as specified, and the `SNMP Config>` prompt is displayed.
5	Restart the module for the new configuration settings to take effect.

Enabling and Disabling Traps

You can enable or disable one trap at a time or all traps simultaneously. To enable or disable a trap, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **snmp**.
2	Press Return. The `SNMP Config>` prompt is displayed.
3	If you want to enable a trap, enter **enable trap** ***trap-type***. If you want to disable a trap, enter **disable trap** ***trap-type***. The ***trap-type*** must be one of the command options specified in Table 12-2.
4	Press Return. The following message is displayed: `Community name []?`
5	Enter the name of the community to which you want to assign the trap type.
6	Press Return. The specified trap type is enabled or disabled for the specified community, and the `SNMP Config>` prompt is displayed.

Table 12-2: Trap Type Options

Command Option	Description
cold_start	A cold start trap (0) occurs when the transmitting device is reinitializing and the agent's configuration or the protocol entity implementation may be altered.
warm_start	A warm start trap (1) occurs when the transmitting device is reinitializing but the agent's configuration or the protocol entity implementation does not change.
link_down	A link down trap (2) occurs when there is a failure in one of the communication links represented in the agent's configuration.
link_up	A link up trap occurs when a previously inactive network link becomes active.
auth_fail	An authentication failure trap occurs when the sending entity is the addressee of a protocol message that is not properly authenticated.
egp	EGP neighbor loss traps occur when an EGP neighbor and peer are marked down and no longer a peer. The egpNeighborLoss trap-PDU contains the name and value of the egpNeighAddr instance for the affected neighbor as the first element of its variable bindings.
enterprise	Enterprise-specific traps occurrences vary, depending on the event. The specific-trap field identifies the particular trap that occurs.
all	Enables or disables all traps specified in this table.

Displaying and Monitoring SNMP

This section describes how to display current SNMP configuration parameters and how to monitor statistics about the number of defined variables and the size of the MIB.

Monitoring Defined Variables and MIB Size

To display information about the number of defined variables and the size of the MIB, perform the following steps:

Step	Action
1	Access the Monitor prompt (`Monitor>`).
2	Enter **statistics**.
3	Press Return. The desired information and the Monitor prompt (`Monitor>`) are displayed.

Example

```
Monitor>statistics

Number of defined variable handlers = 776
Size of MIB = 35496 bytes
```

Displaying Current Configuration Parameters

You can display information about the following parameters assigned to communities:

- Access
- IP address and mask
- Trap types
- Views and subtrees associated with a views
- All the above information in one report

Displaying Selected Parameters

To display selected parameters assigned to communities, perform the following steps:

Note

You can display parameters by community from both the `SNMP Config>` prompt, as described in this section, and from the Monitor prompt (`Monitor>`). To display the same information from the Monitor process, access the Monitor prompt and enter **list community** ***option*** as described in the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **snmp**.
2	Press Return. The `SNMP Config>` prompt is displayed.
3	Enter **list community** ***option***, where ***option*** is one of the command options specified in Table 12-3.
4	Press Return. The information associated with the specified option is displayed and the `SNMP Config>` prompt is displayed.

Table 12-3: Community Command Options

Command Option	Description
access	Displays the access assigned to each community.
address	Displays the IP address and IP mask assigned to each community.
traps	Displays the trap types enabled for each community.
view	Displays the views assigned to each community.

Displaying All Parameters in a Report

To display all parameters assigned to communities, perform the following steps:

Note

You can display all parameters from both the `SNMP Config>` prompt, as described in this section, and from the Monitor prompt (`Monitor>`). To display the same information from the Monitor process, access the Monitor prompt and enter **list all**.

Step	Action
1	At the Config prompt (`Config>`), enter **snmp**.
2	Press Return. The `SNMP Config>` prompt is displayed.
3	Enter **list all**.
4	Press Return. The report and the `SNMP Config>` prompt is displayed.

Example

SNMP Config>**list all**

```
SNMP is disabled
Trap UDP port: 162
          Community Name                Access
-------------------------------  ------------------
public                           Read, Trap
salem                            Trap Only

         Community Name             IP Address         IP Mask
-------------------------------  ---------------  ---------------
public                           All              N/A
salem                            All              N/A
         Community Name                  Enabled Traps
-------------------------------  -------------------------------
public                           None
salem                            Cold Restart

          Community Name                      View
-------------------------------  -------------------------------
public                           All
salem                            lancaster

           View Name                          Sub-Tree
-------------------------------  -------------------------------
lancaster                        1.3.6.1.4.1.2
                                 1.3.6.1.4.1
                                 1.3.6.1.4.1.3
```

Identifying the Location of the Module

You can specify the physical location of the module if it is serving as an SNMP node. For example, you may want to indicate that a module is located in Building 2, third floor, room 2. The information you specify is available to SNMP-based management agents as a MIB object. The information you can enter to identify the location is limited to 80 characters.

To identify the location of the module for MIB-based management systems, perform the following steps:

Step	Action
1	At the Config> prompt, enter **set location**.
2	Press Return. The following message is displayed: Location of this node [ ]?

Step	Action
3	Enter the location of the module. (**Building 2**, for example.) The location description you enter can be up to 80 characters long.
4	Press Return. The information you enter is set.

Example

`Config>`**set location Building 2, 3rd floor**

Identifying a Contact Person Responsible for the Module

You can specify the name of a contact person who is responsible for the module, if it is serving as an SNMP node. For example, you may want to indicate that Jane Doe is the switch administrator. You may also decide to provide a phone number to contact the administrator. The contact information you specify is available to SNMP-based management agents as a MIB object. The information you can enter to identify the contact person is limited to 80 characters.

To identify the contact person for MIB-based management systems, perform the following steps:

Step	Action
1	At the `Config>` prompt, enter **set contact-person**.
2	Press Return. The following message is displayed: `Contact person for this node []?`
3	Enter the information needed to identify the person responsible for the module (**Jane Doe, ext. 5555**, for example). The contact description you enter can be up to 80 characters long.
4	Press Return. The information you enter is set.

Example

`Config>`**set contact-person Jane Doe, ext. 5555**

Displaying Contact Person and Location Information

You can display the name of a contact person who is responsible for the module and the location of the module for a module serving as an SNMP node. You may want to do so, for example, to verify that the information is correct.

To display contact person and location information for MIB-based management systems, perform the following steps:

Step	Action
1	At the `Config>` prompt, enter **list configuration**.
2	Press Return. A report is displayed, including information about the contact person for, and location of, the module.

Configuring TCP/IP Host Services

GIGAswitch GS2000 modules can serve as IP end nodes in a network. As an IP end node, a module supports several IP protocols including, for example, Telnet, SNMP, TFTP, and Ping. These protocol functions are available through TCP/IP Host Services. Telnet and SNMP provide two vehicles for remotely managing modules. TFTP is used to back up and restore module configurations. Ping is used to diagnose network problems. Refer to Chapter 10 for information about backing up and restoring module configurations.

When the module is to serve as an IP end node, you must perform the following tasks before any of these IP protocols (Telnet, SNMP, and so on) can be used:

Task	Description
1	Configure the module's in-band IP address and subnet mask using either TCP/IP HST services or IP routing. The following procedure explains the steps involved when you use TCP/IP HST services. To configure IP routing, see the *DIGITAL GIGAswitch GS2000 Line Card Router Management* manual.
2	Select the VSD on which you want a module IP end node to reside.
3	Configure a default gateway.
4	Enable or disable router discovery and RIP listening.
5	Enable or disable TCP/IP Host Services.
6	Restart the module.

Configuring the Module's In-Band IP Address and Subnet Mask

You can set, change, or delete the in-band IP address of the module from either the installation menu, or by using the module CLI.

Refer to the appropriate module installation and configuration manual for information about how to set the in-band address using the installation menu.

When changing the IP address, the VSD associated with the IP-HST address might need to be changed. The CLI allows you to set both of these values in a single operation. However, the installation menus do not allow the configuration of the VSD associated with the IP-HST address. Changing the IP-HST address takes effect immediately.

Assigning an IP End Node to a VSD

Assume, for example, each of three VSDs represents a different IP subnet. You must select the VSD on which the IP end node is to reside. If you select VSD 1, then you must assign an IP address and subnet mask to the IP end node that is valid for VSD 1's subnet. IP nodes directly attached to VSD 1's subnet can initiate an ARP request for, and connect to, the module directly. IP nodes connected to other subnets (VSD 2, for example) must connect to the module through a router.

You do not need to assign an IP address to the module or assign the address to a VSD if you do not want to use any of the IP end node protocols' features (remote management, network backup and restoration, and so on).

Restrictions

Assigning an IP host to a VSD affects only in-band management (IP packets received over FDDI or ATM network interfaces).

To set the IP address and subnet mask of the module using the CLI, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **hst**.
2	Press Return. The `TCP/IP-Host config>` prompt is displayed.
3	Enter **set ip-host address** and press Return. The following message is displayed: `IP-Host address [16.20.48.48]?`
4	Enter the IP address of the module and press Return. The following message is displayed: `Address mask [255.0.0.0]?`
5	Enter the address subnet mask and press Return. The default subnet mask is `255.0.0.0` if the address is a Class A IP address, `255.255.00` if the address is a Class B address, and `255.255.255.0` if the address is a Class C address. The IP address and address mask are set, and the `TCP/IP-Host config>` prompt is displayed.

Configuring a Default Gateway

A default network gateway may be required if routers are included in your network. The default network gateway is used when trying to send packets to IP destinations that are not on the same subnet as the module. All packets on this router whose destination address is not found in the routing table, are routed to this destination.

The default gateway setting is not required if Router Discovery is enabled. It is also not typically needed if RIP listening is enabled. For example, if your system receives RIP messages containing a default route, then you do not need to configure a default gateway.

To set or change default gateways for the module using the CLI, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **hst**.
2	Press Return. The `TCP/IP-Host config>` prompt is displayed.
3	Enter **add default-gateway** and press Return. The following message is displayed: `Default-Gateway address [0.0.0.0]?`
4	Enter the IP address of the router to be used as the default gateway, and press Return. The address of the default gateway is added and the `TCP/IP-Host config>` prompt is displayed.

Enabling and Disabling Router Discovery and RIP Listening

You may want to enable Router Discovery or RIP Listening if routers are included in your network. Router Discovery is the ability of the module to learn of default routers by receiving ICMP Router Discovery messages. RIP Listening is the process of building routing table entries listening to the RIP protocol. Although you can enable both Router Discovery and RIP Listening at the same time, typically only one or the other is needed.

To enable or disable Router Discovery or RIP Listening using the CLI, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **hst**.
2	Press Return. The `TCP/IP-Host config>` prompt is displayed.
3	If you want to enable or disable Router Discovery, enter either **enable** or **disable**, followed by **router-discovery**. The default is enabled. If you want to enable or disable RIP Listening, enter either **enable** or **disable**, followed by **rip-listening**. The default is disabled.
4	Press Return. The process is enabled or disabled as specified, and the `TCP/IP-Host config>` prompt is displayed.

Enabling and Disabling Host Services

TCP/IP Host Services must be enabled to establish in-band remote console sessions. You should disable host services only if you want to limit access to the module via a local session through the setup port.

To enable or disable TCP/IP Host Services using the CLI, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **hst**.
2	Press Return. The `TCP/IP-Host config>` prompt is displayed.
3	If you want to enable Host Services, enter **enable services**. If you want to disable Host Services, enter **disable services**. The default is enabled.
4	Press Return. TCP/IP Host Services is enabled, and the `TCP/IP-Host config>` prompt is displayed. **Note:** Configuration of IP-HST services takes effect immediately.

Note

If IP routing is enabled, IP-HST services are disabled automatically. Once routing is enabled, connectivity to the module must be made through one (or more) of the configured routing interfaces. (See the *DIGITAL GIGAswitch GS2000 Line Card Router Management* manual.) When routing is enabled for the first time, any configuration information for IP-HST services can be automatically copied to the default routing interface.

Displaying TCP/IP Host Services Settings

You can display all TCP/IP Host Services configuration settings. To display the information, perform the following steps:

Step	Action
1	At the Config prompt (`Config>`), enter **hst**.
2	Press Return. The `TCP/IP-Host config>` prompt is displayed.
3	Enter **list all**, and press Return. The settings are displayed and the `TCP/IP-Host config>` prompt is displayed.

Example

```
TCP/IP-Host config>list all

IP-Host IP address : 0.0.0.0
Address Mask       : 0.0.0.0

No Default Gateway address currently configured.

TCP/IP-Host Services Enabled and operational.

TCP/IP-Host Services offered on VSD 1, DEFAULT.
Module not in Hub -- VNbus tags not used!

RIP-LISTENING Disabled.

Router Discovery Enabled.
```

Monitoring and Managing TCP/IP Host Services

This section describes how to use TCP/IP Host Services to monitor and manage network connections. You can perform the following tasks using TCP/IP Host Services:

- Display routing tables.
- Display the bridge's interface addresses.
- Test a network connection using the **ping** command.
- Display a list of routers.
- Display a path to a destination device.
- Display the VSD on which TCP/IP host services is available.

Displaying the Routing Table

You can display the routing table generated through Router Discovery and RIP Listening. Refer to the Enabling and Disabling Router Discovery and RIP Listening section for information about configuring these functions.

To display the routing table, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **hst**.
2	Press Return. The `TCP/IP Host>` prompt is displayed.
3	Enter **dump**.
4	Press Return.
5	The routing table and the `TCP/IP Host>` prompt are displayed.

Example

```
TCP/IP Host>dump

Type   Destination net  Mask      Cost    Age   Next hop(s)
 Dir*  11.7.0.0         FFFF0000   1        0     BDG/0
Routing table size: 768 nets (61440 bytes), 1 nets known
```

Displaying the Bridge's Interface Addresses

You can display the transparent bridge's interface number and IP address mask. To display the bridge's interface addresses, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **hst**.
2	Press Return. The `TCP/IP Host>` prompt is displayed.
3	Enter **interface addresses**.
4	Press Return.
5	The bridge's interface addresses and the `TCP/IP Host>` prompt are displayed.

Example

```
TCP/IP Host>interface addresses

Ifc  Name       IP Address(es)    Mask(s)               Status
 18  BDG/18     0.0.0.0           0.0.0.0               Up
```

Testing a Network Connection Using the Ping Command

You can use the **ping** command to help isolate problems in an internetwork environment. When initiated, **ping** causes the bridge to send ICMP Echo Requests once per second to a specified destination, and to detect a response.

This process is done continuously, incrementing the ICMP sequence number with each additional packet. Matching received ICMP Echo responses are reported with their sequence number and the round trip time. The granularity (time resolution) of the round trip time calculation is (depending on the platform) usually about 20 milliseconds.

Note

The number of data bytes in the ICMP message, excluding the ICMP header, is 56 bytes, and the TTL used is 60 hops.

To **ping** a device, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **hst**.
2	Press Return. The `TCP/IP Host>` prompt is displayed.
3	Enter **ping** ***ip-address***, where ***ip-address*** is the address of the device for which you want to perform a test.
4	Press Return. The test is initiated.
5	Press any key. The process is completed. The results of the response and the `TCP/IP Host>` prompt are displayed.

Example

```
TCP/IP Host>ping 16.20.48.79

PING 16.20.48.79: 56 data bytes
----16.20.48.79 PING Statistics----
3 packets transmitted, 0 packets received, 100% packet
loss
```

Note

If IP routing is enabled, you can enter the ping command from the IP Protocol Console (IP>), accessed from the `Monitor>` prompt.

Displaying a List of Routers

You can display a list of currently known routers that were learned through one of the following operations:

- Static configuration (Refer to the Configuring a Default Gateway section.)
- Received ICMP redirects
- ICMP Router Discovery messages, if configured (Refer to the Enabling and Disabling Router Discovery and RIP Listening section.)
- RIP updates, if configured (Refer to the Enabling and Disabling Router Discovery and RIP Listening section.)

To display a list of currently known routers, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **hst**.
2	Press Return. The `TCP/IP Host>` prompt is displayed.
3	Enter **routers**.
4	Press Return.
5	The list of routers and the `TCP/IP Host>` prompt are displayed.

Example

```
TCP/IP Host>routers
routers
Type Router           Priority   Lifetime Accessed
```

Displaying the Path to a Destination Device

You can display the complete path (hop by hop) from the module to a particular destination device. This is an implementation similar to the UNIX traceroute tool. For each successive hop, the process sends out three probes and prints the IP address of the responder, together with the round trip time associated with the response. If a particular probe does not receive a response, an asterisk is printed. Each line in the display relates to this set of three probes, with the left-most number indicating the distance from the router executing the command (in router hops).

To display the path to a destination, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **hst**.
2	Press Return. The `TCP/IP Host>` prompt is displayed.
3	Enter **trace** ***address***, where address is the IP address of the device to which you want to display the path.
4	Press Return.
5	The trace is initiated. The trace is completed when the destination is reached, an ICMP Destination Unreachable is received, or the path length reaches 32 router hops. The `TCP/IP Host>` prompt is redisplayed when the trace is competed.

Note

If IP routing is enabled, you can enter the **traceroute** command of the IP Protocol Console (IP>), accessed from the `Monitor>` prompt.

Interpreting Unexpected Results

When the probe receives an unexpected result, the following indications can be printed:

- !N — Indicates an ICMP Destination Unreachable (network unreachable) was received.
- !H — Indicates an ICMP Destination Unreachable (host unreachable) was received.
- !P — Indicates an ICMP Destination Unreachable (protocol unreachable) was received.

Since the probe is a UDP packet sent to a strange port, a port unreachable is expected. The exclamation point (!) indicates that the destination was reached, but the reply sent by the destination was received with a TTL of 1. This result typically indicates an error in the destination, prevalent in some versions of UNIX. The destination is inserting the probe's TTL in its replies. This results in a number of lines consisting of a number of asterisks before the destination is finally reached.

Displaying the VSD on Which TCP/IP Host Services Is Available

You can display the number and name of the VSD on which Host Services is available. This is the VSD to which you assigned the module's IP Host address. The default is the default VSD number 1. (Refer to the Configuring a Default Gateway section for information about assigning the module's IP Host address to a VSD.)

To display the number and name of the VSD on which Host Services is available, perform the following steps:

Step	Action
1	At the Monitor prompt (`Monitor>`), enter **hst**.
2	Press Return. The `TCP/IP Host>` prompt is displayed.
3	Enter **vsd**.
4	Press Return.
5	The number and name of the VSD and the `TCP/IP Host>` prompt are displayed.

Example

```
TCP/IP Host>vsd

TCP/IP-Host Services offered on VSD 1, DEFAULT.
Module not in Hub -- VNbus tags not used!
```

Connecting to Other Devices Using Telnet

You can connect to any remote system from a module's local or remote session by using Telnet. To do so, perform the following steps:

Step	Action
1	Access the Main prompt (`Main>`).
2	Enter **telnet** ***ip-address terminal-type***, where ***ip-address*** is the IP address of the device you want to access, and ***terminal-type*** is an optional parameter you can enter to identify the type of terminal you are using. The ***terminal-type*** can be up to 80 characters long, and helps define the characteristics of the Telnet session for the remote device.
3	Press Return. The module attempts to establish a session with the remote device.

Chapter 13

Monitoring Network Activity

Overview

Introduction

The DIGITAL GIGAswitch GS2000 line card provides the RMON agent for monitoring network activity.

The RMON agent allows you to configure the module so that it independently monitors its own MIB variables and network traffic.

This chapter explains how to configure and monitor the RMON agent.

In This Chapter

The following topics are covered in this chapter:

About the Module RMON Agent

The module Remote Network Monitoring (RMON) agent allows you to configure the module so that it independently monitors its own MIB variables and network traffic. The module RMON agent supports the Alarm and Event MIB groups and adheres to RMON MIB RFC 1757 for Ethernet objects.

RMON Alarm and Event Groups

The alarm group allows you to configure the module so that it monitors its own MIB variables. If the value of a monitored variable crosses its configured thresholds, the RMON agent generates an event. The event group associates an event with a set of actions. Two actions are defined: generate an SNMP trap message and add an entry to the event group log table.

You can configure alarms and events from a network management application, such as a MIB browser, that uses SNMP. You can also use the module CLI to read and write MIB variables in the alarm and event groups.

You can separately configure the Event Logging System (ELS) to generate an ELS event whenever an alarm generates an RMON event. Otherwise, the RMON event group and ELS are independent of each other.

Alarms and events are stored in NVRAM (nonvolatile RAM) memory and are preserved if you power cycle the module. You can delete individual table entries by using the RMON CLI **delete** command or you can use SNMP to set the table entry status to invalid. You can also use the **clear** RMON command from the Config prompt to delete all RMON table entries.

If you use SNMP to create, delete, or modify alarm and event table rows, you must follow the conventions for EntryStatus as specified in the RMON MIB (RFC 1757). You are not required to follow the EntryStatus conventions when you configure alarm and event table rows from the CLI. The CLI correctly transitions row status.

The number of alarm and event table entries is limited to 256.

You cannot write more than one alarm table or event table row at a time in a single SNMP set PDU (Protocol Data Unit). If you do not specify all the values for a row in a set PDU, the default values specified in Table 13-1 and Table 13-2 are used. The CLI uses these default values only the first time you enter an alarm or event from the CLI. Then the CLI uses the values you last entered as a default.

Table 13-1 shows the variables and the default values for the **set alarm** command.

Table 13-1: RMON Set Alarm Command Parameters

Alarm Variable	Default Value	Description
Alarm Index	1	
Alarm Status	valid	
Alarm Interval	1	
Alarm Variable	[0.0]	
Alarm Sample Type	deltaValue	
Alarm Value	0	
Startup Alarm	risingOrFallingAlarm	
Rising Alarm Threshold	0	
Falling Alarm Threshold	0	
Rising Event Index	0	
Falling Event Index	0	
Alarm Owner	Null string	
Alarm Description	Null string	

Table 13-2 shows the variables and the default values for the **set event** command.

Table 13-2: RMON Set Event Command Parameters

Event Variable	Default Value	Description
Event Index	1	
Event Status	valid	
Event Description	Null string	
Event Type	log-and-trap	
Event Community	Null string	
Event Owner	Null string	

RMON Command Line Interface

You can configure RMON alarms and events from a network management application, such as a MIB browser, that uses SNMP. You can also use the module CLI to read and write MIB variables in the alarm and event groups.

Accessing the RMON Configuration Process

To access the RMON configuration process using the CLI, perform the following steps:

Step	Action
1	From the Main prompt (`Main>`), enter the following command: `Main>`**config** The `Config>` prompt is displayed.
2	At the `Config>` prompt, enter the following command: `Config>` **rmon**
3	Press Return. The following prompt is displayed: `RMON Config>`

Once you have entered the RMON configuration process, you can execute the commands in Table 13-3.

Table 13-3: RMON Configuration Commands:

Command	Command Options	Description
add	alarm event	
set	alarm event log-table-max	
delete	alarm event log	
list	alarm all event log	

Accessing the RMON Monitor Process

To access the RMON monitor process through SNMP, perform the following steps:

Step	Action
1	From the Main prompt (`Main>`), enter the following command: `Main>` **monitor** The `Monitor>` prompt is displayed.
2	At the `Monitor>` prompt, enter the following command: `Monitor>`**rmon**

3	Press Return. The following prompt is displayed:
	`RMON user console`
	`RMON>`

Once you have entered the RMON monitor process, you can execute the commands in Table 13-4.

Table 13-4: RMON Monitor Commands

Command Type	Command Parameters
delete	log table
list	alarm all event log
monitor	
exit	

RMON Example

The following sections provide a configuration example. In this example, whenever the number of received SNMP packets increases, the module generates a *risingAlarm* trap to the community *rmon-trap* that has an IP address of *16.20.48.46*.

Configuring an SNMP Community

The following procedure describes how to configure SNMP with a new community named *rmon-trap* with an IP address of *16.20.48.46*:

Step	Action
1	At the `Config>` prompt, enter **snmp**. `SNMP Config>` **add comm rmon-trap** `SNMP Config>` **add addr rmon-trap** `IP address [0.0.0.0]?` **16.20.48.46** `IP Mask [255.255.255.255]?`
2	Press Return. The SNMP community *rmon-trap* is now configured.

Configuring an RMON Trap

The following sections describe how to configure RMON so that it generates a rising alarm trap if the MIB variable *snmpInPkts.0* (oid 1.3.6.1.2.1.11.1.0) increases by more than zero over a 1-second interval. This is accomplished by creating an event entry and an alarm entry.

Creating an Event Entry

To create an event entry with an event type *snmp-trap* and an event community *rmon-trap*, perform the following steps:

Step	Action
1	At the `Config>` prompt, enter **rmon**.
2	At the `RMON Config>` prompt, enter **add event**. `Event Description []?` Enter the ASCII string for event description and press Return. `Event Type [log-and-trap]?` **snmp-trap**. `Event Community []?` **rmon-trap** `Event Owner []?` Enter the ASCII string for event owner and press Return.
3	Press Return. The following is displayed: `Creating Event with index` *n* The RMON event entry is complete.

Creating an Alarm Entry

To create an alarm entry for the above event entry, perform the following steps:

Step	Action

1	At the `RMON Config>` prompt, enter **add alarm**.
	`Alarm Interval [1]?`
	`Alarm Variable []?` **1.3.6.1.2.1.11.1.0**
	`Alarm Sample Type [deltaValue]?`
	`Startup Alarm [risingOrFallingAlarm]?` **risingalarm**
	`Rising Alarm Threshold [0]?` **1**
	`Falling Alarm Threshold [0]?`
	`Rising Event Index [0]?` ***n*** (Use the value from the add event entry.)
	`Falling Event Index [0]?`
	`Alarm Owner []?`
	`Alarm Description []?`

2	Press Return. The following is displayed: `Creating Alarm with index` *n* The RMON alarm entry is complete.

Summary

In the RMON example, whenever the module receives an SNMP request (snmpInPkts.0 increases by 1 or more), it sends an RMON risingAlarm trap.

Appendix A

Advanced Console Management

Overview

Introduction

This appendix discusses local and remote console session management tasks that may be of interest to advanced DIGITAL GIGAswitch GS2000 line card users.

In This Appendix

The following topics are covered in this appendix:

Process Aliases and IDs

The module prompts are each associated with an operational process, each of which is assigned a process ID (PID). The Config and Monitor prompts and Events are each associated with a single PID. The module Main prompt (`Main>`) is associated with three processes, each of which is associated with a PID. The processes associated with module prompts, and their PIDs, are shown in the following table:

Module Prompts	Process Names	PIDs
Main	LOpCon	1
	MOpCon and ROpCon	9 and 10
Config	Config	6
Monitor	Monitor	5
Events	Events	2

LOpCon and ROpCon are the main operator control processes that manage communication between consoles and lower level processes. LOpCon is the process that supports a (single) locally connected console session through the console port. ROpCon is the process that supports up to two remote console sessions. The functions supported by LOpCon and ROpCon are the same.

Viewing Process Status and PIDs

You can view information about any process including the name of the process, the process ID (PID), the status of the process, the console to which output is currently routed, and the IP address of any user logged in remotely via ROpCon.

To view process status information and PIDs, perform the following steps:

Step	Action
1	At the Main prompt (`Main>`), enter **status**.
2	Press Return. A list of processes is displayed, as shown in the following example.

Example

```
Main>status

Pid   Name        Status    TTY    Comments
1     LOpCon       RDY      TTY0
2     Events       DET       --    Event Logger
3     Tasker       RDY       --    Tasker
4     Debugger     IOW       --
5     Monitor      DET       --    To Monitor Brouter
6     Config       DET       --    To Configure Brouter
7     SNMP         IDL       --
8     DEChub       IDL       --
9     ROpCon       IDL      TTY1
10    ROpCon       IDL      TTY2
```

Refer to the Process List Output section for a description of each item in the process list.

Process List Output

The process list includes the following information.

Output	Description
Pid	Process ID (PID).
Process	Name of the process. Tasker, MOSDDT, SNMP, and DEChub are processes reserved for use by DIGITAL Services.

Output	Description
Status	Status of the process. Refer to the status descriptions in the following table for a list of process status conditions and descriptions.
TTY	Output terminal, if any, to which the process is currently connected. TTY0 indicates a local console. TTY1 or TTY2 indicate Telnet consoles. “Sink” indicates that a process was flushed. Two dashes (- -) indicate that a process was halted.
Comments	The user’s login IP address provided when a user is logged in using Telnet (ROpCon).

The following table lists the process status conditions that can be displayed in the Status column, and a description of each.

Status	Description
IDL	The process is idle and waiting for completion of an external event, such as asynchronous I/O.
RDY	The process is ready to run and is waiting to use the CPU.
IOW	The process is waiting for synchronous I/O to complete.
DET	The process has output ready to be displayed and is either waiting to be attached to a display console, or waiting to have its output diverted to a specified console.
FZN	The process is “frozen” due to an error. This usually means the process is trying to use a device that is faulty or incorrectly configured.

Viewing Output from Multiple Processes

You can display the output from several processes simultaneously, at any terminal, by diverting output to the terminal. This capability is most commonly used to redirect event log output messages to a specific terminal while running another process at the same time.

To divert (display) process output to a particular console, perform the following steps:

Step	Action
1	Determine the PID of the process you want to divert, and the number of the console (tty#) to which you want to divert the output. (Refer to the Viewing Process Status and PIDs section.)
2	At the Main prompt (`Main>`), enter **divert**, followed by the process ID and the console number. For example, entering **divert 2 1** redirects Event Logging System messages generated by the Events process (PID 2) to a remote console (tty1). (Refer to Chapter 11 for information about the Event Logging System.)
3	Press Return. The output from the specified process is diverted to the console indicated.

Canceling Display of Output to a Console Session

You can cancel the display of output from a specific process to your console session. Doing so cancels only the display of output to your session. Other users accessing the same process can still view output from the process. You must use the **config**, **monitor**, **events**, or **divert** command to reaccess the process and redisplay output. (Refer to the Viewing Output from Multiple Processes section for information about using the **divert** command.)

To cancel (flush) process output to a particular console, perform the following steps:

Step	Action
1	Determine the PID of the process you want to stop displaying. (Refer to the Viewing Process Status and PIDs section.)
2	At the Main prompt (`Main>`), enter **flush**, followed by the process ID. For example, entering **flush 2** cancels the display of Event Logging System messages generated by the Events process (PID 2).
3	Press Return. The output from the specified process is no longer displayed on your console.

Terminating Process Output

You can terminate all output from a specific process to all console sessions. Doing so cancels not only the display of output to your console session, but also to console sessions of other users. You must use the **config**, **monitor**, **events**, **divert**, or **flush** commands to reaccess the process and redisplay output. (Refer to the Viewing Output from Multiple Processes section for information about using the **divert** command. Refer to the Canceling Display of Output to a Console Session section for information about using the **flush** command.)

To terminate process output to all console sessions, perform the following steps:

Step	Action
1	Determine the PID of the process you want to stop displaying. (Refer to the Viewing Process Status and PIDs section.)
2	At the Main prompt (`Main>`), enter **halt**, followed by the process ID. For example, entering **halt 2** terminates the display of Event Logging System messages generated by the Events process (PID 2).
3	Press Return. The output from the specified process is terminated.

Appendix B

Plug and Play Default Settings

Overview

Introduction

The DIGITAL GIGAswitch GS2000 line card features plug and play operation. Once installed, the module begins handling network traffic running transparent bridging on each port, by default. This appendix lists the default settings that are used when the module is first installed. You may need to alter the default settings to maximize network performance, to enable special functions such as Virtual Local Area Networks (VLANs), and to set IP addresses for remote management.

In This Appendix

The following topics are covered in this appendix:

Module-Wide Default Settings

Table B-1 lists the default settings for parameters that affect module-wide operations.

Table B-1: Module-Wide Defaults

Setting	Default
Enabling and disabling ID and password prompts	Disabled
Inactivity timer	0 (zero) — Turns off the inactivity timer, so that an established session remains active no matter how long a console is inactive. The inactivity timer affects only those consoles linked to modules on which ID and password prompting is enabled.
Hostname	No host name
Time zone offset	0 (zero) — Indicates no offset from GMT.
Time host synchronization frequency	0 (zero) — Indicates the module is not to poll the time host to synchronize clocks.
Routing	Disabled

Nonspecific Interface Default Settings

Table B-2 lists the default settings common to all interface types (FDDI and ATM).

Table B-2: Nonspecific Interface Defaults

Setting	Default
Enabling and disabling an interface	Enabled
ARP Refresh Timer	20 minutes
ARP Auto-Refresh	Disabled

FDDI Interface Default Settings

Table B-3 lists the default settings for all FDDI interface configurations.

Table B-3: FDDI Defaults

Setting	Default
Station type (DAS or SAC)	DAS
Link Error Rate Cutoff	8 (0.00000001 bits per second)
Link Error Rate Alarm	8 (0.00000001 bits per second)
Status Report Policy (SMT notification)	On
Maximum Token Rotation Time (t-max-lower-bound)	167 milliseconds **Note:** The software rounds the specified value to the nearest multiple of 5.24288 milliseconds. For example, the default value of 167 milliseconds is interpreted by the software as 167.77216 milliseconds.
Requested Token Rotation Time (t_req)	8 milliseconds **Note:** The software rounds the specified value to the nearest multiple of 20.48 microseconds. For example, the default value of 8 milliseconds is interpreted by the software as 7.9872 milliseconds.
Valid Transmission Time (tvx-timer)	2.5 milliseconds **Note:** The software rounds the specified value to the nearest multiple of 20.48 microseconds. For example, the default value of 2.5 milliseconds is interpreted by the software as 2.51904 milliseconds.
Ring purger	Off
Full-duplex (or half-duplex mode)	On (Full-duplex mode)

ATM Interface Default Settings

The following tables list the default settings for all ATM interface configurations. Table B-4 shows the type of ATM logical interfaces (ELAN or Bridge Tunnel) that are automatically established after installation, and the conditions under which they are active. Table B-5 lists the ATM physical interface default settings. Table B-6 lists the default parameter settings for each type of default connection shown in Table B-4.

Table B-4: Interface Defaults at Startup

Type of Connection Established/Logical Interface	Conditions Under Which Connection Is Established
ELAN/2	The module ATM interface is connected to a DIGITAL GIGAswitch/ATM system.
FDDI ATM Bridge Tunnel/16	The module ATM interface is connected to a DIGITAL GIGAswitch/FDDI AGL2 module.
Ethernet ATM Bridge Tunnel/ 17	The module ATM interface is connected to the ATM interface of a VNswitch module.

Table B-5: Physical Interface Default Parameters

Setting	Default
Transmission type	SONET
Transmission timing	local (front panel interface) loop (interface to the DEChub backplane)
Payload scrambling	On (enable)
Testing the ModPHY card (loopback)	Off

Table B-6: Logical Interface Default Parameters

Setting	Default
ELAN Name	No name
Identifying the LES address	Automatic (mode)
Expected ARP Response Time	1 second
LE_ARP Request Retries	1
Aging Time (for LE_ARP cache entries)	300 seconds
Forward Delay Time (for LE_ARP cache entries)	15 seconds
Maximum Frame Size	1516 octets
Maximum Unknown Frame Count	1 frame
Maximum Unknown Frame Time	1 second
Control Timeout	120 seconds
VCC Timeout	20 minutes
Flush Timeout	4 seconds
Path Switching Delay	6 seconds

Bridge Default Settings

Table B-7 lists the default settings for all bridge configurations.

Table B-7: Bridge Defaults

Setting	Default
Rate Limiting (per filter basis)	No (disabled)
Module-wide Rate Limiting	Disabled
Module-wide Rate Limiting frames/second	400
Bridge Priority	32768
Port Path Cost	0 (Causes STP to calculate the Path Cost)
Port Priority	128
Bridge-Max-Age	20
Bridge-Hello-Time	2
Bridge-Forward-Delay	15
Bridge port STP state	Enabled
Manual Mode	No (disabled)
Bridge port state	Enabled
IP fragmentation	Enabled (not configurable)
IPX translation	Disabled
No Frame Interval	300 seconds
Aging Time	300 seconds

Bridge Default Settings

Setting	Default
VSDs	All bridge ports on a module are members of a default VSD. The default VSD is numbered VSD 1 and is assigned the name “Default.” The number and name cannot be changed. When more than one module is resident in a switch, all ports on all modules are, by default, members of the same (default) VSD. Ports that are members of the default VSD operate as a traditional bridge without VLANs.

Maintenance Default Settings

Table B-8 lists the default settings for maintenance procedures.

Table B-8: Maintenance Defaults

Setting	Default
Diagnostics downloads (dumps)	Disabled

ELS Configuration Default Settings

Table B-9 lists Event Logging System default configurations for nonvolatile memory (NVRAM). Table B-10 lists Event Logging System default configurations for volatile memory.

Table B-9: ELS NVRAM Configuration Defaults

Setting	Default
Display by subsystem	No subsystems
Trap by subsystem	No subsystems
Display by subsystem and logging level	No subsystems or logging levels
Trap by subsystem and logging level	No subsystems or logging levels
Display by event number	No events
Trap by event number	No events
Display by group	No groups
Trap by group	No groups
Maximum traps per second	0 (Indicates an unlimited number of traps per second is permitted.)
Set output (displaying events directly from the log, not from a CLI prompt)	Default (Events can be viewed by entering **Events** at the Main prompt.)

Table B-10: ELS Volatile Memory Configuration Defaults

Setting	Default
Display by subsystem	No subsystems
Trap by subsystem	No subsystems
Display by subsystem and logging level	No subsystems or logging levels
Trap by subsystem and logging level	No subsystems or logging levels
Display by event number	No events
Trap by event number	No events
Display by group	No groups
Trap by group	No groups
Maximum traps per second	Equal to the current setting for maximum traps per second applied to NVRAM configuration

Remote Management Default Settings

Table B-11 lists the default settings for remote management.

Table B-11: Remote Management Configuration Defaults

Setting	Default
Enabling and disabling access via modem	Disabled
OBM port speed	9600 baud
OBM RTS state (Enabled or Disabled)	Disabled
Router Discovery	Enabled
RIP Listening	Disabled
(Host) Services	Enabled
Address subnet mask (for Host Services)	`255.0.0.0`, if the address is a Class A IP address `255.255.00`, if the address is a Class B IP address `255.255.255.0`, if the address is a Class C IP address
SNMP	Enabled
One SNMP community	Public
Access to SNMP public community	Write-read-trap

Appendix C

Counters

Overview

Introduction

This appendix provides an overview of the counters and the effect of packets on counters as packets flow through the module.

In This Appendix

The following topics are covered in this chapter:

Packet Counter Overview

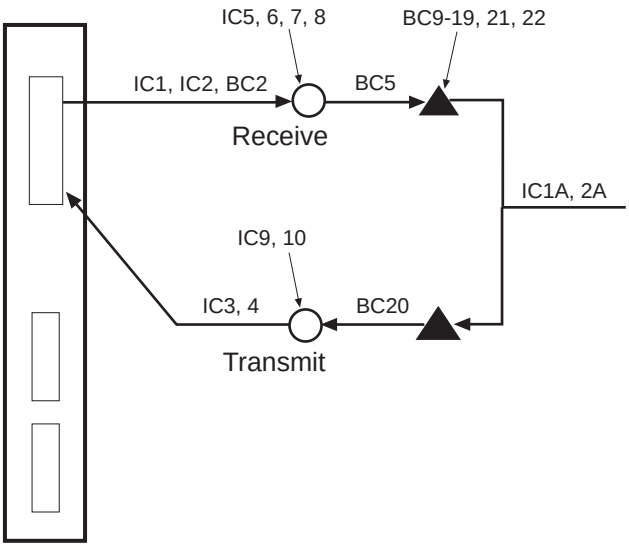
The module contains packet counters allowing users to observe the amount and types of traffic being processed at various locations. The counters keep track of both sent and received traffic, and are broken down into categories to indicate how many packets have reached various different outcomes (terminated, dropped, bridged, routed, flooded, fragmented, and so on).

Packet counters exist at four internal distinct layers to help the user trace packets as they flow within the module. The four layers discussed here are logical interfaces, bridge ports, VLAN interfaces, and the IP router. When a packet is received by an entity within a layer, the packet is either dropped, processed, or passed on to one or more entities within the next layer. When a packet is dropped at a particular layer, an error counter within that layer increments. The effects of the packet is not seen in counters at any layers it does not reach. Packets that are successfully processed at a layer increment non-error counters within that layer. Packets sent to the next layer increment non-error counters in that subsequent layer as well.

Figure C-1 illustrates the four layers and shows the relationships between logical interfaces, bridge ports, VIs, and the IP router. The figure shows which counters are incremented for the various paths a packet can take within a module.

Packets arriving at the module enter the physical interface and can then travel through each of the four layers. Physical interfaces are the connection jacks for cables, and have a one-to-one or one-to-many (in the case of an ATM physical interface) relationship with interfaces. Logical interfaces, shown as circles in Figure C-1, are the lowest layer where counters are used. All packets received and sent are counted by logical interface counters. Error counters for interfaces catch some basic types of errors appropriate to the level of decoding the packet has undergone at this point (for example, a bad FCS) or other errors that are not necessarily associated with a specific higher-level protocol (for example, buffer overflow). If such an error is detected on an interface, the packet being sent or received is discarded, and the appropriate interface error counter is incremented. Otherwise, it is passed to a bridge port (where bridging runs on all interfaces).

Figure C-1: Packet Flow



Packets arriving at a bridge port (dark triangle in Figure C-1) are first subject to the effects of bridging. They may be dropped for numerous reasons (destination address filtering, STP port state, and so on), each of which causes a single bridge error or increment a dropped packet counter for that port. If a packet is not dropped, its destination address determines whether it is unicast to another port, flooded out all ports, terminated, and/or delivered to routing. If the packet is bridged out other ports, the bridge attempts to translate and enqueue the packet for sending, if necessary. A failure in this process causes a dropped packet and the error counter increments for the received port. A success means that the packet is sent out other ports and counted by them as well. If a received packet is not dropped or sent out by bridging, it is terminated (such as an STP BPDU) and/or submitted to routing.

VLAN interfaces (VIs) receive all packets destined to routing. VIs, which are groups of bridge ports, are paired one-to-one with VLANs. VIs submit packets for routing on behalf of any ports within their VLAN. VI counters keep track of the total number of packets submitted to routing from their VLAN. Outbound packets sent by routing also go through a VI for transmission on a VLAN. VI transmit counters increment once for each packet sent by routing, although multiple packets may be sent on one or more ports (whose counters are incremented as well). Packets sent or received on VIs cannot be dropped by the VI. All errors, overflows, and so on, at the router layer are detected and counted in other layers.

Packets reaching the router may be terminated and are counted by routing. The module IP counters count transmitted, received, and error packets across all VIs and do not display this information on a per-VI basis.

Interface Counters

Table C-1 describes each interface counter (IC) associated with the module. Interface counters IC1A, IC2A, IC3A, and IC4A are identical to IC1, IC2, IC3, and IC4, except the "A" counters represent VI counters.

Table C-1: Interface Counter Descriptions

Interface Counter Number	Name and Definition
IC1, IC1A	**Unicast packets received** Unicast packets received on an interface.
IC2, IC2A	**Multicast packets received** Multicast packets received on an interface.
IC3, IC3A	**Unicast packets transmitted** Unicast packets transmitted on an interface.
IC4, IC4A	**Multicast packets transmitted** Multicast packets transmitted on an interface.
IC5	**Input overflow drops** Input queue overflows on an interface (received packet is dropped). Note: Some of these packets may be counted in bridge port counters BC14 and BC15.
IC6	**Input error drops** Invalid packets/errored packets received on an interface (packet is dropped). Examples of this are packets which are of an invalid length (are shorter than the length given within the packet or are too short to contain the required packet fields).
IC7	**Input unknown protocol drops** Packets received on an interface which are destined to an unknown protocol (packet is dropped).
IC8	**Input congestion control drops** Packets received on an interface which were flow controlled (dropped) due to congestion on the packet's receive and transmit interfaces. Note: Some of these packets may be counted in bridge port counter BC22 as well.

Interface Counter Number	Name and Definition
IC9	**Output overflow drops** Outbound packets dropped on an interface due to an output queue overflow. Note: Some of these packets may be counted in bridge port counter BC22 as well.
IC10	**Output error drops** Outbound packets dropped on an interface because of one of the following: • The interface is down or going down while the packet is transmitted. • The data link hardware chip aborts sending the packet. • The maximum bridge latency of the packet for the associated bridge port has expired. • The packet was too large to be transmitted on the interface. Note: Some of these packets may be counted in bridge port counters BC23 and BC24 as well.

Bridge Port Counters

Table C-2 describes each bridge port counter (BC).

For most of the dropped packet counters, note that the counter is incremented only if the packet dropped completely—meaning that it is not sent out *any* ports.

For example, assume the case that a packet arrives with an unknown DA and requires flooding and translation to other ports. If the packet can be succesfully sent out at least one of these ports, counters BC9, BC10, BC11, BC12, BC13, BC14, BC15, and BC16 will not be incremented. Counter BC20, however, will be incremented if the packet *fails* to make it out at least one port.

Table C-2: Bridge Port Counter Descriptions

Bridge Port Counter Number	Name and Description
BC1	**Port restarts** Number of times this bridge port's associated interface has passed a self-test, indicating that the port has restarted.
BC2	**Total frames received by interface** Number of packets recieved on this bridge port's associated interface (including those eventually discarded due to errors). This is the same as the sum of unicast and multicast packets received on the ports associated interface.
BC3	**IP frames fragmented** Number of IP packets received on this port's associated interface that were fragmented due to a smaller frame size on the transmit interface's datalink.
BC4	**IP frames not fragmented** Number of IP packets received on this port's associated interface that bridging attempted to fragmnet but could not because the DONT_FRAGMENT bit was set in the IP header. These packets were discarded.
BC5	**Frames submitted to bridging** Number of packets received on this bridge port. This includes packets that may eventually be bridged, routed, filtered, or dropped.
BC6	**Frames submitted to routing** Number of IP packets received on this port's associated interface that were delivered to routing.
BC7	**Frames with unknown destination address** The number of packets received on this bridge port for which the bridge's forwarding database had no destination address.
BC8	**Frames causing learning transactions** Number of packets recieved on this bridge port whose source address (SA) is not learned or was known on another port and thus caused a learning transaction.

Bridge Port Counter Number	Name and Description
BC9	**Source address filter drops** Number of packets completely dropped (not sent out any port) because of their source address. A packet's source address (SA) can be filtered for two reasons: **1** A user-configured source address (SA) filter was defined. **2** The source address (SA) is a multicast addresses (these are always filtered).
BC10	**Destination address filter drops** Number of packets completely dropped (not sent out any port) because of their destination address. A packet can be filtered for one of two reasons: **1** A user-configured destination address (DA) filter was defined. **2** The destination address (DA) was received on the source address (SA) port (natural bridge filtering).
BC11	**Protocol filter drops** Number of packets completely dropped (not sent out any port) because of a user-configured protocol filter.
BC12	**Address rate limiting drops** Number of packets completely dropped (not sent out any port) because of a user-configured limit on the number of packets per second that may be sent to the destination address (DA).
BC13	**Protocol rate limiting drops** Number of packets completely dropped (not sent out any port) because of a user-configured limit on the number of packets per second that may be sent with this protocol type.
BC14	**Input buffer overflows** Number of packets completely dropped (not sent out any port) due to a lack of input buffers. Note: Some of these packets may be counted in interface counter IC5 as well.

Bridge Port Counter Number	Name and Description
BC15	**Input queue overflows** Number of packets completely dropped (not sent out any port) due to congestive input loss. Note: Some of these packets may be counted in interface counter IC5 as well.
BC16	**Source or destination port blocked drops** Number of packets completely dropped (not sent out any port) due to either the source or destination port not being in the forwarding state.
BC17	**Terminating queue overflows** Number of terminating packets dropped because of an overflow in the termination queue.
BC18	**Fragmentation queue overflows** Number of packets received with a known unicast destination address (DA) which were dropped because they required fragmentation before being sent out the transmit port, and the fragmentation queue overflowed.
BC19	**Translate flood queue overflows** Number of packets received that needed to be flooded to multiple ports, some of which required translation, but were not successfully sent out all ports due to an overflow in the translate flood queue.
BC20	**Translation failures** Number of packets completely dropped (not sent out any port) because the packet could not be translated to a different data link. For example, the length of the packet was less than the minimum required for the received data link.
BC21	**Frames sent by bridging** Number of packets transmitted on this bridge port. This includes packets that were bridged from other ports as well as locally originated (including routed) packets. It includes packets that may eventually be dropped at the bridge port's associated interface, but not packets that were dropped by the bridge port itself.

Bridge Port Counter Number	Name and Description
BC22	**Transmit queue overflows** Number of packets that were dropped and not sent on this bridge port due to an overflow in the transmit queue.
BC23	**Transmit errors** Number of packets that were dropped and not sent on this bridge port due to an error in transmission. Note: Some of these packets may be counted in interface counter IC10.
BC24	**Too big to send on port drops** Number of packets that were dropped and not sent on this bridge port because they were too large. The packet was not fragmented due to one of the following: • Fragmentation is disabled. • The packet contains an unfragmentable protocol. • There were errors within the packet that prevented it from being fragmented. • The “do not fragment” bit was set within the packet. Note: Some of these packets may be counted in interface counter IC10 as well.

Counter Relationships

Some simple relationships exist between interface counters, bridge port counters, and VI counters. For a given packet in Figure C-1, the following relationships exist. Refer to the Interface Counters and Bridge Port Counters sections for a complete list of the counters.

Receive Relationships

Example 1

IC1 + IC2 = BC2

(Unicast packets received + Multicast packets received = Total frames received by the interface)

Sum of the unicast and multicast packets received on an interface total all of them.

Example 2

BC2 ≥ BC5

(Total frames received by interface ≥ Frames submitted to bridging)

Some packets received on an interface may be dropped before being submitted to bridging.

Example 3

BC5 ≥ BC6

(Frames submitted to bridging ≥ Frames submitted to routing)

Only some packets submitted to bridging will be submitted to routing. The rest are either dropped or bridged.

Example 4

BC6 ≤ IC1A + IC2A

(Frames submitted to routing ≤ Unicast packets received + Multicast packets received)

The packets submitted to routing by a port's VI may represent only a portion received by that VI since the VI's VLAN may contain other ports.

Transmit Relationships

Example 5

IC3 + IC4 ≤ BC20

(Unicast packets transmitted + Multicast packets transmitted ≤ Translation failures)

Some packets sent by bridging may be dropped at the interface layer.

Management Interfaces

The counters supported on the module can be viewed through various management interfaces (CLI, SNMP, WWW). These displays are shown below with the counters labeled.

CLI

Example 1

```
Monitor>statistics
Monitor>stat
Ifc Name             Unicast       Multicast         Packets
                    Pkts Rcv        Pkts Rcv           Trans
0   VNbus/0                2               0             362
1   FDDI/1                 2               0               2
2   ALEC/2                 2               0               2
3   ALEC/3                 2               0               2
4   ALEC/4                 4              12               6
5   ALEC/5                 2               0               2
6   ALEC/6                 3               0               3
7   ALEC/7          (IC1)  3        (IC2)  0  (IC3)+(IC4)  3
8   ALEC/8                 3               0               3
9   ALEC/9                 3               0               3
10  ALEC/10                3               0               3
11  ALEC/11                3               0               3
12  ALEC/12                3               0               3
13  ALEC/13                3               0               3
14  ALEC/14                3               0               3
15  ALEC/15                0               0               0
16  AFBT/16                0               0               0
17  AEBT/17        (IC1A)  0       (IC2A)  0 (IC1A)+(IC1A)  0
Monitor>
```

Example 2

```
Monitor>error
                  Input      Input      Input      Input     Output     Output
Nt Interface    Discards     Errors  Unk Proto  Flow Drop   Discards     Errors
0  VNbus/0             0          0          0          0          0          0
1  FDDI/1              1          0          0          0          0          0
2  ALEC/2              1          0          0          0          0          0
3  ALEC/3              1          0          0          0          0          0
4  ALEC/4              8          0          0          0          0          0
5  ALEC/5              1          0          0          0          0          0
6  ALEC/6              2          0          0          0          0          0
7  ALEC/7              2          0          0          0          0          0
8  ALEC/8        (IC5) 2    (IC6) 0    (IC7) 0    (IC8) 0    (IC9) 0    (IC10) 0
9  ALEC/9              2          0          0          0          0          0
10 ALEC/10             2          0          0          0          0          0
11 ALEC/11             2          0          0          0          0          0
12 ALEC/12             2          0          0          0          0          0
13 ALEC/13             0          0          0          0          0          0
14 ALEC/14             0          0          0          0          0          0
15 ALEC/15             0          0          0          0          0          0
16 AFBT/16             0          0          0          0          0          0
17 AEBT/17             0          0          0          0          0          0
Monitor>
```

Example 3

```
Monitor>interface statistics 1

Monitor>int stat 1
                     Self-Test     Self-Test      Maintenance
Ifc Ifc' Name           Passed        Failed           Failed
  1   1  FDDI/1             1             1                0

Monitor>
```

Example 4

```
BRIDGE>list count port 1
BRIDGE>list count port 1
Counters for port 1, interface FDDI/1:
Port restarts:                                0 (BC1)
Total frames received by interface:           2 (BC2)
IP frames fragmented:                         0 (BC3)
IP frames not fragmented:                     0 (BC4)
Frames submitted to bridging:                 2 (BC5)
Frames submitted to routing:                  0 (BC6)
Frames with unknown dest address:             0 (BC7)
Frames causing learning transactions:         0 (BC8)
Dropped, source address filtering:            0 (BC9)
Dropped, dest address filtering:              0 (BC10)
Dropped, protocol filtering:                  0 (BC11)
Dropped, address rate limiting:               0 (BC12)
Dropped, protocol rate limiting:              0 (BC13)
Dropped, input queue overflow:                0 (BC14)
Dropped, source or dest port blocked:         1 (BC15)
Dropped, terminating queue overflow:          0 (BC16)
Dropped, fragmentation queue overflow:        0 (BC17)
Dropped, translate flood queue overflow:      0 (BC18)
Dropped, translation failure:                 0 (BC19)
Frames sent by bridging:                      2 (BC20)
Dropped, transmit queue overflow:             0 (BC21)
Dropped, transmit error:                      0 (BC22)
Dropped, too big to send on port:             0 (BC23)

BRIDGE>
```

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V