

# GIGAswitch/FDDI System

---

## Manager's Guide

Part Number: EK-GGMGA-MG.B01

**This document contains information for managing a GIGAswitch/FDDI System after it is installed on a network.**

**Revision/Update Information:** This is a revised document.

Digital Equipment Corporation  
Maynard, Massachusetts

---

**First Printing, June 1993**  
**Second Printing, April 1995**

The information in this document is subject to change without notice and should not be construed as a commitment by Digital Equipment Corporation. Digital Equipment Corporation assumes no responsibility for any errors that may appear in this document.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such license.

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

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction document, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at the user's own expense.

© Digital Equipment Corporation 1995.

All Rights Reserved.

The postpaid Reader's Comments forms at the end of this document request your critical evaluation to assist in preparing future documentation.

The following are trademarks of Digital Equipment Corporation: CI, DEC, DECbridge, DECELMS, DECMCC, DECNDU, DECNET, DECNIS, DECserver, DF196, DF296, Digital, DSSI, GIGAswitch, HUBwatch, LAT, OpenVMS, PATHWORKS, POLYCENTER, ULTRIX, VAX, VMScluster, VAXstation, VMS, VT, VT220, and the DIGITAL logo.

The following are third-party trademarks: MS-DOS is a registered trademark of Microsoft Corporation. PostScript is a registered trademark of Adobe Systems, Inc. OpenView is a registered trademark of Hewlett Packard. OSF/1 is a registered trademark of Open Software Foundation, Inc. SunNet Manager is a registered trademark of Sun Microsystems. Windows is a registered trademark of Microsoft Corporation. All other trademarks and registered trademarks are the property of their respective holders.

This document was prepared using VAX DOCUMENT, Version 2.1.

---

# Contents

<b>Preface</b> .....	ix
<b>1 Overview of the GIGAswitch/FDDI System</b>	
General Description .....	1-1
GIGAswitch/FDDI System Features .....	1-2
Bridge Features .....	1-2
Performance Features .....	1-2
Management Interfaces .....	1-2
Special Management Features .....	1-3
Special System Features .....	1-3
GIGAswitch/FDDI System Modules .....	1-4
Logic Modules .....	1-5
Cooling and Power Modules .....	1-7
Hot Swap .....	1-9
Introduction to GIGAswitch/FDDI System Operation .....	1-11
Out-of-Band Management (OBM) .....	1-11
OBM Functions .....	1-11
Management Memory .....	1-12
SNMP Management .....	1-12
Firmware Download .....	1-13
FDDI Linecards .....	1-13
ATM Linecards .....	1-13
Switch Control Processor (SCP) .....	1-14
Security Keyswitch .....	1-14
Port Numbering .....	1-14
Front Panel Port Numbers .....	1-15
Sequential Port Numbers .....	1-16
<b>2 Preparing the GIGAswitch/FDDI System for Operation</b>	
Step 1: Install the GIGAswitch/FDDI System .....	2-2
Step 2: Start the OBM .....	2-3
OBM Terminal .....	2-3
LAT Connectivity .....	2-4
OBM Password .....	2-4
Step 3: Set the System Security and IP Addresses .....	2-5
Assign IP Address(es) .....	2-5
Designate Privileged Ports .....	2-5
Designate Bootserver Ports .....	2-5
Default Read-Write Community String .....	2-5
Set Security Keyswitch .....	2-6
Step 4: Connect the Datalinks .....	2-8
FGL Ports .....	2-8

Unshielded Twisted-Pair .....	2-8
Single-mode FDDI .....	2-8
Multimode FDDI .....	2-9
AGL-2 Ports .....	2-9

### 3 Firmware Upgrade Procedures

Upgrade Process .....	3-2
Upgrade Guidelines .....	3-2
Time to Upgrade .....	3-2
Step 1: Copy Image Files to Bootserver .....	3-4
Step 2: Set Port and Security Parameters .....	3-5
Step 3: Transfer the Image File .....	3-6
Warning .....	3-6
TFTP Firmware Transfer Procedure .....	3-6
TFTP Example .....	3-7
MOP Firmware Transfer Procedure .....	3-7
MOP Example .....	3-8
Step 4: Move the Image to the Target Module .....	3-9
MIB Objects .....	3-9
Loading the Image .....	3-9
Example .....	3-10
Downloading Firmware Without a Management Station .....	3-11
DECndu Plus .....	3-11
Ordering Information .....	3-11
Preparing to Load .....	3-11
Downline Load the File .....	3-12
Example .....	3-13
HUBloader .....	3-15
How HUBloader Works .....	3-15
Show Function .....	3-15
Load Function .....	3-15
Strategy for Upgrade with Backup SCP .....	3-17
Setting up Emergency SCP Firmware Download .....	3-18
Bootserver Setup for DECnet-VAX MOP .....	3-18
Bootserver Setup for ULTRIX MOP .....	3-19
Bootserver Setup for BOOTP .....	3-19

### 4 Filters

Purpose of this Chapter .....	4-1
Filtering Basics .....	4-2
Reasons for Filtering .....	4-2
Dynamic Filtering .....	4-2
Static Filtering .....	4-2
Advantages of Filtering .....	4-3
Restrictions .....	4-3
Filter Setup .....	4-4
Port Pattern Matrices .....	4-4
Matrix Example .....	4-5
Specifying the Matrix .....	4-6
Examples .....	4-7
The Default Filter Matrix .....	4-7
Changing the Default Filter Pattern .....	4-7

Creating a Filter Based on SA, DA, or PID . . . . .	4-8
Filter Matrix . . . . .	4-9
Disposition . . . . .	4-9
Combining Several Matrices . . . . .	4-10
Filtering and Broadcast Packets . . . . .	4-11
Filter Examples . . . . .	4-12
Blocking Traffic . . . . .	4-12
Multiple Computer Site . . . . .	4-13
Securing a Load Server . . . . .	4-15
Additional Means of Controlling Packet Flow . . . . .	4-16
Locking Down an Address . . . . .	4-16
Manual Mode . . . . .	4-16

## A Additional Filter Examples

Introduction . . . . .	A-1
Example 1: Filter for MOP Downline Load Requests . . . . .	A-2
Network Configuration . . . . .	A-2
MOP . . . . .	A-2
Desired Filter . . . . .	A-2
Creating the Reachability Matrix . . . . .	A-3
Creating the Filter . . . . .	A-3
Resulting Behavior . . . . .	A-4
Example 2: Filters for Multiple OpenVMS Clusters . . . . .	A-5
Network Configuration . . . . .	A-5
Desired Filters . . . . .	A-6
Two Strategies . . . . .	A-6
Multicast Address Filter . . . . .	A-7
Set Up I/O Port Pattern . . . . .	A-7
Limit Multicast Messages for Cluster-3 . . . . .	A-7
Limit Multiple Port Messages . . . . .	A-8
Protocol Type and SA Filters . . . . .	A-9
Set Up Filter Matrix . . . . .	A-9
Filter Specifications . . . . .	A-10
DECnet Phase IV Filters . . . . .	A-10

## B LEDs of Logic and Power Modules

Linecard LEDs . . . . .	B-2
PMD LEDs . . . . .	B-3
AGL-2 LEDs . . . . .	B-3
SCP Card LEDs . . . . .	B-4
CLK Card LED . . . . .	B-6
CBS Card LED . . . . .	B-7
Fan Tray Assembly LED . . . . .	B-8
ACFEU LEDs . . . . .	B-9
48V DCFEU LEDs . . . . .	B-9
PSA LEDs . . . . .	B-10

## C GIGAswitch/FDDI System Specifications

Physical Dimensions of the GIGAswitch/FDDI System .....	C-2
Electrical Information .....	C-3
AC Input Power Requirements .....	C-3
Power Cord Types .....	C-3
Environmental Information .....	C-5
Ventilation .....	C-6
EMI Susceptibility .....	C-6

## Glossary of GIGAswitch/FDDI System Terms

### Index

### Figures

2-1	Connecting the OBM Terminal .....	2-3
2-2	Security Keyswitch .....	2-6
2-3	Types of Linecard PMDs .....	2-8
4-1	Four-Port, Two User Community Configuration .....	4-6
4-2	Port Pattern Combinations .....	4-10
4-3	Multiple Department Configuration .....	4-13
4-4	Multiple Departments with the Installed System .....	4-14
4-5	College Campus Configuration .....	4-15
A-1	Three-Building Example .....	A-2
A-2	Filter Example Configuration .....	A-5

### Tables

1-1	Functions of the Logic Modules .....	1-6
1-2	Behavior when Inserted .....	1-9
1-3	Behavior when Removed .....	1-10
1-4	Front Panel Port Numbers .....	1-15
1-5	Sequential Port Numbers .....	1-16
2-1	Start OBM .....	2-4
2-2	Security Keyswitch Positions .....	2-7
3-1	Firmware Image .....	3-1
3-2	Approximate Upgrade Times .....	3-3
3-3	Image File Extensions .....	3-6
3-4	TFTP Firmware Upgrade Objects .....	3-6
3-5	MOP Firmware Upgrade Objects .....	3-7
3-6	Firmware Upgrade Objects .....	3-9
3-7	Description of DOWNLOAD SHOW DEVICE Command .....	3-12
3-8	Description of DOWNLOAD LOAD Command .....	3-13
4-1	I/O Port Matrix Table .....	4-5
4-2	Port Matrix Table .....	4-6
4-3	Sample Port Filter Entries .....	4-7
4-4	SAP Filter Entry Objects .....	4-8

4-5	Port Matrix Table .....	4-12
A-1	OpenVMS Clusters .....	A-6
B-1	Meaning of Module LEDs .....	B-2
B-2	Meaning of PMD LEDs .....	B-3
B-3	Meaning of SCP Indicators .....	B-5
B-4	Meaning of CLK LED .....	B-6
B-5	Meaning of CBS LED .....	B-7
B-6	Meaning of Fan Tray Assembly LED.....	B-8
B-7	Meaning of ACFEU LEDs .....	B-9
B-8	Meaning of 48 Vdc LEDs .....	B-9
B-9	Meaning of Security Keyswitch LEDs .....	B-10





---

# Preface

## Intended Audience

This guide is intended for network managers who will manage a GIGAswitch/FDDI System in an extended local area network (LAN).

## Structure of this Guide

This guide describes how to perform common management tasks for the GIGAswitch/FDDI System. The following table shows where to find information:

Refer to:	For Information About:
Chapter 1	Overview and features of the GIGAswitch/FDDI System
Chapter 2	Preparing the GIGAswitch/FDDI System for operation
Chapter 3	Firmware upgrade
Chapter 4	Filters
Appendix A	Filter examples
Appendix B	Logic and power module LEDs
Appendix C	GIGAswitch/FDDI System specifications
Glossary	Definitions of GIGAswitch/FDDI System terms

## Additional Resources

The following documents provide additional information:

- *Bridge and Extended LAN Reference Manual*, EK-DEBAM-HR
- *FDDI Single-mode Fiber (SMF) modPMD*, AV-QK1PA-TE
- IEEE 802.1d MAC Bridging Standard
- FDDI Standards (ISO 9314-1, 9314-2, 9314-3, 9314-4)

Documentation for your network management station (NMS) should also be available for regular use.

## Conventions

The following conventions are used in this guide:

**Bold typeface** A word or phrase is being emphasized to the reader.  
It also indicates MIB objects and filter disposition.

*Italic typeface* Indicates the complete titles of manuals.

Return Press the Return key on the keyboard.

Ctrl/O You must hold down the key labeled Ctrl while you press another key or a pointing device button.

---

## Overview of the GIGAswitch/FDDI System

### General Description

The GIGAswitch/FDDI System is a standalone data switch that implements the IEEE 802.1d bridge architecture. Packets are sent through a switching fabric consisting of a crossbar switch (CBS) which is capable of maintaining as many as 36 simultaneous connections between inputs and outputs. Up to 34 of the crossbar ports may be connected to external data links at any given time.

Connecting crossbar ports to data links is accomplished by linecards, each of which may provide up to four (4) such connections. The GIGAswitch/FDDI System currently supports three types of linecards:

- FGL-2 — 2 FDDI links
- FGL-4 — 4 FDDI links
- AGL-2 — 2 ATM links

Each data link is in turn attached to either an FDDI ring, a single FDDI endstation, a single ATM endstation, an ATM switch, an FDDI bridge, or another GIGAswitch/FDDI System.

---

## GIGAswitch/FDDI System Features

### Bridge Features

As a multi-port bridge the GIGAswitch/FDDI System performs the following functions:

- **Forwarding** — A packet entering the switch is forwarded to the appropriate output port (or ports), as determined by its destination address (DA).
- **Learning** — Source addresses (SA) are automatically learned so that the switch can send packets to the proper output ports.
- **Filtering** — Dynamic filtering assures that packets with destinations learned on a particular port are not forwarded to other ports.
- **Aging** — Learned addresses are automatically aged out so that packets are not lost when network nodes move.
- **Spanning Tree** — The GIGAswitch/FDDI System participates in the IEEE 802.1d Spanning Tree algorithm.

### Performance Features

The GIGAswitch/FDDI System supports several features that enhance performance:

- **Cut-through Forwarding** — Packets are forwarded into the crossbar and onto the output data link as soon as the destination address is known, thus reducing store-and-forward delays. Cut-through forwarding may be optionally disabled.
- **Full-Duplex Operation** — Point-to-point links can operate in full-duplex mode. Full-duplex operation may be optionally disabled.

### Management Interfaces

There are two management interfaces to the GIGAswitch/FDDI System:

- **Out of Band** — A terminal connected to an RS232 port on the GIGAswitch/FDDI System provides limited management functions, used primarily for setting initial operating parameters and system security.
- **SNMP Management** — The switch may be managed from anywhere in the network with any SNMP-based network management station (NMS).

### Special Management Features

Several special management features enable effective use of the GIGAswitch/FDDI System. Some of these are:

- **Management-defined Filters** — Management filters enable the flow of certain traffic through the switch to be specifically restricted. Filters can be conditioned on inbound port, outbound port, SA, DA, protocol type, or some combination of these. Filtering does not impose any performance penalty.
- **Rate Limiting** — Rate limits exist for flooded traffic. Rates can be independently set for multicast and unknown DA traffic. Rate limits prevent flooded traffic from monopolizing LAN bandwidth or switch resources.
- **Security** — Various security mechanisms enable a system manager to maintain the integrity of the system operation. The OBM facility supports an optional password. SNMP employs passwords known as "community strings." A security keyswitch provides physical security over management access to the GIGAswitch/FDDI System.

### Special System Features

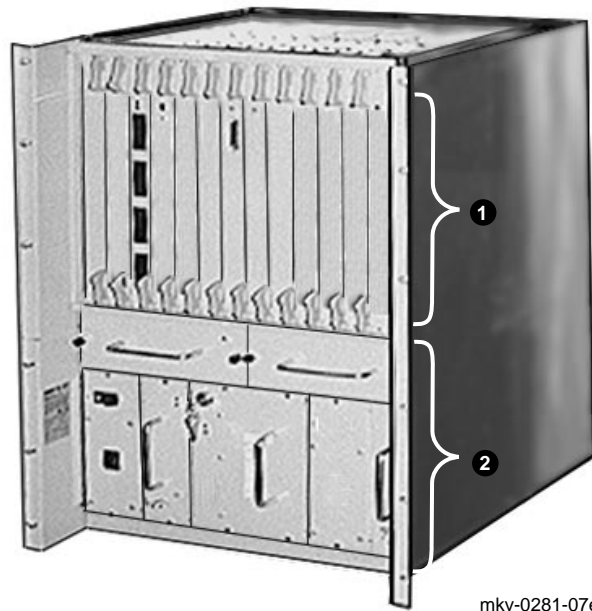
Other special features of the GIGAswitch/FDDI System architecture are:

- **Multiple Traffic Queues** — As packets arrive they are placed on one of several queues, which are serviced independently, to assure the fair and timely processing of packets. This assures, for example, that spanning tree messages will not be delayed behind a long queue of data packets.
- **Service Classes** — Protocols are assigned different service classes so that packet processing does not violate the assumptions of the upper layer protocols. For instance protocols which require in-order data link layer delivery are in one service class to assure this assumption is met.
- **Data Link Independence** — A modular design assures that the switch operates in a way that does not depend on the physical link type—assuring present and future compatibility with any user environment.

---

## GIGAswitch/FDDI System Modules

The GIGAswitch/FDDI System has two major sections of modules: logic modules and power modules.



mkv-0281-07e

---

Number	Location of the ...
❶	Logic modules
❷	Cooling and power modules

---

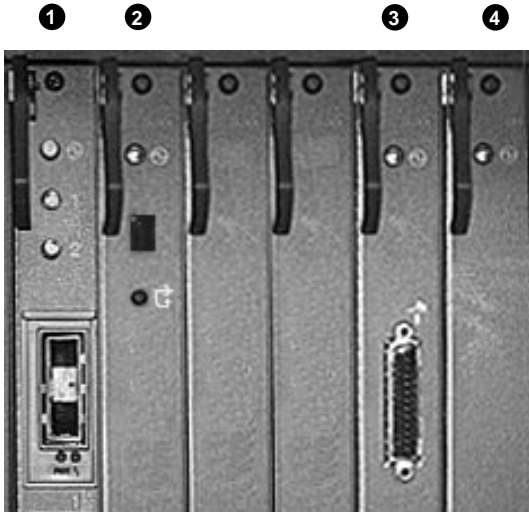
**Logic Modules**

The GIGAswitch/FDDI System logic modules include a logic backplane with 14 slots,<sup>1</sup> and the following four types of cards that control switching functions:

Module Types	Number per Switch
Linecards (FGL-2, FGL-4, AGL-2)	1–11
Switch control processor (SCP)	1 or 2
Clock module (CLK)	1
Crossbar switch (CBS)	1

Linecards may be configured with several types of physical interfaces. For FGL-2 and FGL-4, single mode and multimode fiber is supported, as well as UTP. The AGL-2 supports T3 and SONET OC-3 links (single mode and multimode).

The following figure and table identify the types of logic modules in the GIGAswitch/FDDI System. For information about module LEDs refer to Appendix B.



mk28123

<sup>1</sup> Backplane slots are numbered 1 through 14 from the left.

Table 1-1 Functions of the Logic Modules

Module	Function	Slot Position(s)
<b>① Linecard</b>		
FGL-2 linecard (shown)	Provides connections between 2 crossbar ports and 2 (SAS or DAS) FDDI datalinks.	1-6, 9-14
FGL-4 linecard (not shown)	Provides connections between 4 crossbar ports and 4 SAS FDDI datalinks. See note below.	5, 6, 9-12
AGL-2 linecard (not shown)	Provides connections between 2 crossbar ports and 2 ATM datalinks.	1-6, 9-14
<b>② SCP card</b>		
	Acts as a switch control processor (SCP). Forwards <i>multicast</i> packets and packets with unknown <i>destination addresses (DAs)</i> . Implements 802.1d Spanning Tree algorithm. Provides OBM and SNMP management agents.	1-6, 9-14
<b>③ CLK card</b>		
	Provides the clock signals for the GIGAswitch /FDDI System. Responsible for the central arbitration for the backplane bus. Identifies presence, model number, and type of module in slots 1 through 6 and 8 through 14. Permanently stores management parameters. Contains OBM port.	7 only
<b>④ CBS card</b>		
	Contains the crossbar switch chips. Interconnects the ports on the GIGAswitch /FDDI System. Allows multiple connections to exist at the same time.	8 only

---

**Note**

---

If a FGL-4 is placed in one of the 2 port slots (1-4, 13, 14) only the top 2 ports will operate.

With older versions of the CBS module slot 10 acts like a 2 port slot. See the *GIGAswitch/FDDI System Installation Guide* for more information.

---

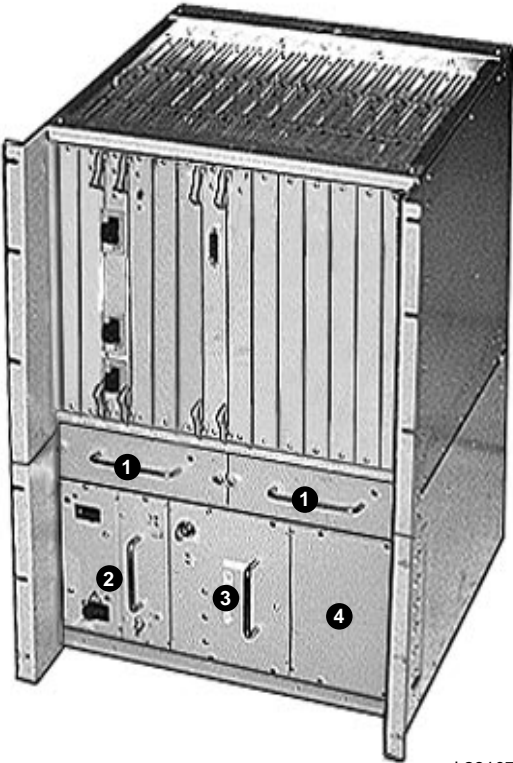


**Cooling and Power Modules**

The GIGAswitch/FDDI System also includes a power backplane and the following power and cooling modules:

Module Types	Number per Switch
Fan tray assembly	2
Power interface unit (ac or 48 Vdc)	1 or 2
Power status assembly (PSA)	1

The following figure and table identify the types of cooling and power modules in the GIGAswitch/FDDI System. For information on the cooling and power LEDs refer to Appendix B.



mk28107d

Number/Name	Function
❶ Fan tray assembly	Cools the GIGAswitch/FDDI System. The GIGAswitch/FDDI System houses two fan tray assemblies. Each fan tray assembly contains two fans.
❷ Power interface units <sup>1</sup>	
AC power interface unit (shown)	Converts ac primary power to regulated 48 Vdc to energize the discrete power modules on the logic cards. Also converts ac primary power to 12 — 26 Vdc to energize the fans.
48 Vdc power interface unit (not shown)	Converts 40 — 60 Vdc power from a battery source to 48 Vdc logic power and to 12 — 26 Vdc fan power.
❸ Power status assembly (PSA)	Contains the power system controller (PSC) that monitors and controls the cooling and power systems. A security keyswitch controls <i>in-band management</i> or <i>out-of-band management (OBM)</i> access.
❹ Slot for <i>backup</i>	Contains either a power supply filler panel, or a backup power interface unit (AC or 48 Vdc).

---

<sup>1</sup>Power interface units are also known as front-end units (FEUs).

---

**Hot Swap**

The following modules may be removed or inserted without affecting operation of the GIGAswitch/FDDI System (except, of course, the module being swapped):

- Linecards
- Switch control processor (backup)
- Fan tray assembly (redundant)
- Power interface unit (redundant)
- Power status assembly

The expected behavior when these modules are inserted into or removed from a running GIGAswitch/FDDI System is described in the following two tables.

**Table 1-2 Behavior when Inserted**

<b>Module</b>	<b>Behavior when Inserted</b>
Linecard	Module goes through normal self-test; then the forwarding database is loaded onto the module, and its ports enter the preforwarding state. If this results in a topology change, then other ports may also go into preforwarding as the spanning tree is recalculated.
SCP	The inserted SCP becomes the backup SCP. There will be no observable effect on the operation of the GIGAswitch/FDDI System.
Power supply	No interruption in service.
Fan tray	No interruption in service.
Power status assembly	No interruption in service.

**Table 1–3 Behavior when Removed**

<b>Module</b>	<b>Behavior when Removed</b>
Linecard	Packets en route to or from ports on the removed card may be lost.
SCP	If the backup SCP is removed no interruption will be observed. If the elected SCP is removed the GIGAswitch/FDDI System stops unless a backup SCP is present. In that case, the backup SCP becomes elected, and power cycles all linecards, resulting in an operational interruption while the linecards perform self-test, and the spanning tree is recalculated.
Power supply	No interruption in service if there is a redundant power supply present.
Fan tray	No interruption in service if there is a redundant fan tray present. The remaining fans will begin operating at maximum speed.
Power status assembly	No interruption in service. Temperature and fan speed can no longer be monitored. Fans will operate at maximum speed. Keyswitch position reverts to 3.

---

## Introduction to GIGAswitch/FDDI System Operation

This section discusses several GIGAswitch/FDDI System functions that are common to most GIGAswitch/FDDI System installations. For detailed information on any of these topics refer to that topic in the appropriate guide.

### Out-of-Band Management (OBM)

The GIGAswitch/FDDI System includes an asynchronous port on the CLK module which provides access to the OBM facility. A terminal can be connected (directly or via modem) to this port to control several GIGAswitch/FDDI System operational parameters. The same port also provides access to diagnostic procedures for the GIGAswitch/FDDI System.

OBM provides the ability to:

- Assign IP addresses to various GIGAswitch/FDDI System ports
- Designate ports as SNMP management paths
- Designate ports as firmware upgrade paths
- Show and change the state of system modules
- Observe or change the size or contents of various system tables

OBM is used primarily to set initial parameters for switch operation, and to set and show important operational parameters when SNMP management is unavailable (for example, when the link to the management station is not currently connected).

### OBM Functions

The major settings to be performed via the OBM interface are:

- **IP addresses** — In order for a (SNMP) management station to manage the GIGAswitch/FDDI System an IP address must be assigned. This is done on a per port basis. A single IP address may be assigned to several ports.

When an IP address is first assigned to a port by a user it is stored in nonvolatile memory, and reassigned whenever the switch is rebooted, unless explicitly deleted by the user.

In the absence of any assigned IP address the GIGAswitch/FDDI System send BOOTP requests out certain ports. When it gets the first response it assigns the IP address provided by the BOOTP server to the port on which it was received. Such an assignment is not stored in nonvolatile memory, and is not restored when the system is rebooted.

- **Privileged Ports** — The GIGAswitch/FDDI System can be (SNMP) managed only from ports designated as privileged. Use OBM to designate privileged ports. Designation is retained in the switch's nonvolatile memory. By default all ports are privileged.

- **Bootserver Ports** — New firmware for the switch's modules is loaded from servers via SNMP commands. The GIGAswitch/FDDI System only accepts firmware images from ports designated as bootserver ports. Use OBM to designate bootserver ports. This designation is retained in nonvolatile memory. Bootserver ports are also the ports over which BOOTP requests are sent. By default all ports are bootserver ports.

Other important parameters may also be set by OBM. They are described in later chapters. OBM commands and menus are described in detail in the OBM Guide.

## **Management Memory**

As indicated several parameters must be set correctly for proper GIGAswitch/FDDI System operation. These are stored in a nonvolatile memory (called management memory), on the CLK module. All configuration parameters to be retained across system reboots are stored in the management memory on the CLK module. The CLK module also contains the hardware addresses assigned to the GIGAswitch/FDDI System. Hence the CLK module really contains the unique identity of a GIGAswitch/FDDI System. If the CLK modules of two switches are interchanged, then the switches have effectively changed identities.

In addition to the nonvolatile memory on the CLK module there is nonvolatile memory on each module (except the CBS), which stores that module's firmware, and an error log for diagnostic purposes.

## **SNMP Management**

The GIGAswitch/FDDI System has an SNMP agent that allows SNMP-compliant network management stations (NMS) to read and set certain management parameters contained in management information bases (MIB). The GIGAswitch/FDDI System supports a wide range of standard MIBs as well as vendor and device-specific MIBs. For a detailed description of SNMP refer to the SNMP Guide. All MIBs supported by the GIGAswitch/FDDI System must be loaded onto the NMS before it can manage a GIGAswitch/FDDI System.

Any SNMP management station on the network can manage the GIGAswitch/FDDI System once it knows the GIGAswitch/FDDI System's IP address and read-write community string. In addition, Digital's HUBwatch product offers a special GIGAswitch/FDDI System management application which provides a useful graphical user interface for managing a GIGAswitch/FDDI System. This application runs on OSF, OpenVMS, and DOS Windows workstations. Relevant GIGAswitch/FDDI System MIBs are preloaded in the HUBwatch application.

## Firmware Download

Firmware download is accomplished via SNMP. The user specifies an image on a fileservers which the GIGAswitch/FDDI System will copy. The user then specifies which slot is to receive that image.

For users who wish to load firmware without a NMS, Digital provides two applications which performs the operations required to download new firmware to a GIGAswitch/FDDI System:

- DECndu Plus runs on OSF, OpenVMS, ULTRIX, and DOS systems.
- HUBloader is a Windows application.

Refer to Chapter 3 of this guide for information on downloading new firmware.

## FDDI Linecards

Two FDDI linecards are currently available. FGL-2 has two ports, each of which may be configured as a SAS or a DAS port. FGL-2s may occupy any slot except those occupied by the CLK (slot 7) and CBS (slot 8) modules.

FGL-4 has four ports, each of which must be configured as a SAS port. While FGL-4s may occupy the same slots as FGL-2s, only slots 5, 6, 9, 10<sup>1</sup>, 11, and 12 will support all four ports. In other slots only ports 1 and 2 of the FGL-4 are active.

---

### Note

---

A GIGAswitch/FDDI System with a FGL-4 module in slot 10 must use a CBS module with an -02 variation.

---

Each port of a FGL-2 or FGL-4 linecard may be configured with the following physical medium dependent (PMD) modules:

- Single mode fiber (FC-PC connector)
- Multimode fiber (ANSI MIC connector)
- Unshielded twisted pair (TP-MIC connector)

The choice of PMD's will not affect overall operation of the GIGAswitch/FDDI System.

See the GIGAswitch/FDDI System Installation Guide to install PMDs and Chapter 2 of this guide to plug in various cable types.

## ATM Linecards

The AGL-2 linecard provides the ability for the GIGAswitch/FDDI System to send and receive packets over ATM links. There are two ports per linecard. They may be placed in any slot where a FGL-2 can go. The following types of physical layer devices are supported for each port:

- SONET OC-3 single mode fiber
- SONET OC-3 multimode fiber

---

<sup>1</sup> Older versions of the CBS module cause slot 10 to act as a 2 port slot. See the *GIGAswitch/FDDI System Installation Guide* for more information

- T3 (DS3) PHY

For more information on the AGL-2 linecards refer to the *GIGAswitch/FDDI System AGL-2 Reference Guide*.

### **Switch Control Processor (SCP)**

While the "identity" of the GIGAswitch/FDDI System is contained in the CLK module's management memory, its "intelligence" is contained in the SCP. An SCP may be placed in any slot where a FGL-2 can go. There is one active SCP per GIGAswitch/FDDI System. It is called the "Elected SCP" (or SCP). An additional SCP can be configured, called the "Backup SCP."

The SCP is responsible for the following GIGAswitch/FDDI System functions:

- OBM
- SNMP management
- 802.1d Spanning Tree algorithm
- Unknown address and multicast flooding
- System configuration
- Coordination of individual port learning databases
- Setting filters
- Reading and writing management memory
- Firmware download

Failure of the elected SCP causes the backup SCP (if present) to take over its functions. When this occurs all linecards are automatically reinitialized.

### **Security Keyswitch**

The security keyswitch controls access to the GIGAswitch/FDDI System's management features.

The security keyswitch controls the use of in-band or out-of-band management to modify GIGAswitch/FDDI System parameter settings. The keyswitch enables OBM access with or without a password. It also controls the use of SNMP set commands; however, it does not override the requirement for a read-write community string password when appropriate for SNMP commands.

### **Port Numbering**

Many management directives refer to GIGAswitch/FDDI System ports. As background to future sections which describe such directives, the two port numbering schemes available with the GIGAswitch/FDDI System are described below. Many operations can be performed with either of these numbering schemes. Other operations require the use of one or the other.



## Front Panel Port Numbers

A front panel port number (FPPN) identifies a GIGAswitch/FDDI System port by specifying the slot and the port number within that slot. A FPPN has the form X.Y, where X is the slot number and Y is the port number within that slot. The leftmost slot is slot 1; the rightmost slot is slot 14. The CLK module always occupies slot 7; the CBS module always occupies slot 8. So there are no FPPNs corresponding to those slots.

Slots 1—4, 13, and 14 provide connections to 2 ports each. Slots 5, 6 and 9—12 provide connections to 4 ports each. Ports within a slot are numbered from 1 starting at the top. FPPNs of the GIGAswitch/FDDI System ports are shown in Table 1–4:

**Table 1–4 Front Panel Port Numbers**

Slot Number	Ports			
	1	2	3	4
1	1.1	1.2	-	-
2	2.1	2.2	-	-
3	3.1	3.2	-	-
4	4.1	4.2	-	-
5	5.1	5.2	5.3	5.4
6	6.1	6.2	6.3	6.4
7	-	-	-	-
8	-	-	-	-
9	9.1	9.2	9.3	9.4
10	10.1	10.2	10.3	10.4
11	11.1	11.2	11.3	11.4
12	12.1	12.2	12.3	12.4
13	13.1	13.2	-	-
14	14.1	14.2	-	-

**Sequential Port Numbers**

Sequential port numbers (SPN) identify the GIGAswitch/FDDI System ports sequentially starting with the top port in slot 1 (SPN 1); ending with the bottom port in slot 14 (SPN 36). SPNs of the GIGAswitch/FDDI System ports are shown in Table 1–5:

**Table 1–5 Sequential Port Numbers**

Slot Number	Ports			
	1	2	3	4
1	1	2	-	-
2	3	4	-	-
3	5	6	-	-
4	7	8	-	-
5	9	10	11	12
6	13	14	15	16
7	-	-	-	-
8	-	-	-	-
9	17	18	19	20
10	21	22	23	24
11	25	26	27	28
12	29	30	31	32
13	33	34	-	-
14	35	36	-	-

A sequential port number should be used for setting any MIB variable that calls for bridge port number, SMT index, or MAC index.

---

## Preparing the GIGAswitch/FDDI System for Operation

This chapter describes the steps to begin GIGAswitch/FDDI System operations:

1. Install the GIGAswitch/FDDI System
2. Start the OBM
3. Set the system security and IP addresses
4. Connect the data links to linecards

These steps will bring the GIGAswitch/FDDI System to a useful operating condition. Steps 1 and 4 will provide a working bridge, but most installations require all four steps, plus additional specific steps to meet special operating requirements. Those will be described in later chapters.

---

## Step 1: Install the GIGAswitch/FDDI System

Physical installation of the the GIGAswitch/FDDI System is described in the *GIGAswitch/FDDI System Installation/Service Guide*. Carefully follow the instructions in that guide before you attempt to begin switch operation.

---

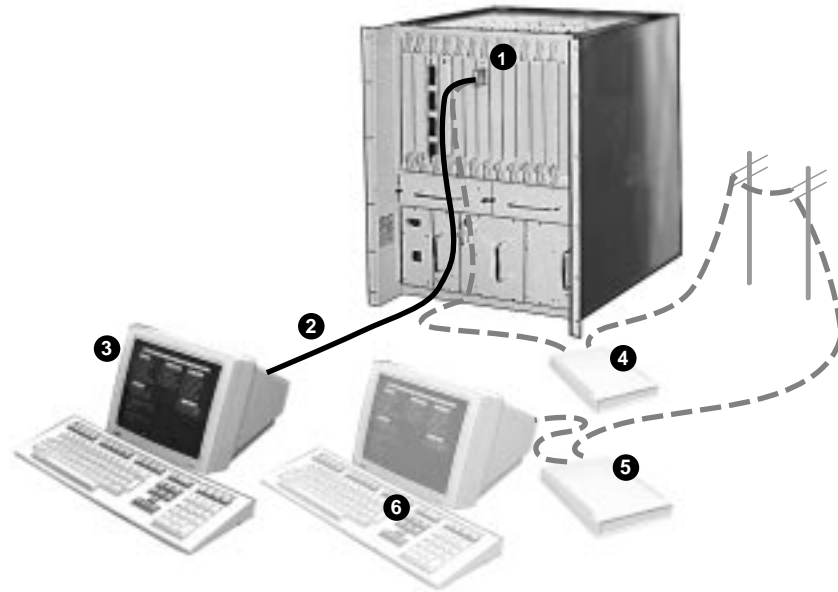
## Step 2: Start the OBM

An out-of-band management (OBM) port provides a limited set of functions for initialization, security, and diagnostics of the GIGAswitch/FDDI System.

### OBM Terminal

The OBM terminal connects directly, or through a modem, to the OBM port on the CLK card. A terminal, with modems meeting CCITT V.24, V.28, or V.32 standards, and associated cables are required. Figure 2-1 shows how to connect the OBM terminal.

Figure 2-1 Connecting the OBM Terminal



mkv-0281-51

Number	Function
①	OBM port
②	Cable, part number BC22D-xx <sup>1</sup> (xx = cable length in feet) (EIA RS232 connector)
③	OBM terminal—9600 baud
④	Modem—9600 baud
⑤	Remote modem
⑥	Remote OBM terminal

<sup>1</sup>BC22D cable meets Class A FCC requirements.

## Step 2: Start the OBM

Table 2–1 list the steps required to connect the OBM terminal and start the OBM session:

**Table 2–1 Start OBM**

Step	Action
1	Locate the OBM port, the cables, and the OBM terminal (or the modem, remote modem, and remote OBM terminal).
2	Connect the RS232 cable from the terminal (or modem) to the OBM port.
3	Install the remote modem and the remote OBM terminal, if needed.
4	Set up the terminal as follows: 9600 baud rate 8 bits, no parity 1 stop bit
5	Set the security switch to allow OBM access (position 2, 3, or 4).
6	Press <b>Ctrl/D</b> to get the CLK> prompt.
7	Press <b>Ctrl/O</b> to start the OBM session.

### **LAT Connectivity**

The OBM port may also be connected to a LAT port for remote OBM access. The LATserver must pass escape sequences.

When connecting to a terminal server with remote LAT access, set LATserver port autobaud (disable) and access (remote).

Note the following restrictions:

- Cannot use the DECserver 90L or 90L+
- Cannot use the DECserver 90TL or 90M

### **OBM Password**

Set the OBM password by using the OBM terminal.

1. Select the **Set OBM Password** option from the main menu.
2. The password must be between 8 and 16 characters long.

A password is not required. The default setting is no password. If you forgot the OBM password, turn the security keyswitch to position 4 for easy access mode to bypass the OBM password.

---

## Step 3: Set the System Security and IP Addresses

This section describes how to setup access and security features on the GIGAswitch/FDDI System so it can be managed using an SNMP network management station (NMS), and so that new firmware can be downloaded.

Some of these procedures refer to individual ports on the GIGAswitch/FDDI System. Chapter 1 describes how GIGAswitch/FDDI System ports are numbered.

For a NMS to successfully manage the GIGAswitch/FDDI System do the following:

- Assign IP addresses
- Designate privileged ports
- Designate bootserver ports

### Assign IP Address(es)

The NMS must address the GIGAswitch/FDDI System using the proper IP address. The port through which the NMS connects to the GIGAswitch/FDDI System must be assigned an IP address.

Use OBM to assign an IP address to one or more ports.

An address assigned this way is stored in nonvolatile management memory. It is reassigned whenever the GIGAswitch/FDDI System is rebooted. In the absence of an assigned IP address on some port a BOOTP request will be periodically sent over all bootserver ports. The first response received will result in the IP address provided by the BOOTP server being assigned to the port on which the response is received.

### Designate Privileged Ports

SNMP sets may only be performed through privileged ports. Use the OBM to designate one or more ports as privileged or to revoke privileged designation. By default all ports are privileged.

### Designate Bootserver Ports

Firmware images may be downloaded only through bootserver ports. Use the OBM to designate one or more bootserver ports or to revoke bootserver designation. By default all ports are bootserver ports.

### Default Read-Write Community String

Read and read-write community strings are required to perform SNMP *get* and *set* operations. The default read community string is "public."

### Step 3: Set the System Security and IP Addresses

The default read-write community string is the lowest system hardware address assigned to the GIGAswitch/FDDI System. Each switch is assigned a globally unique range of hardware addresses. They are stored in the CLK module. The address range is printed on a label on the front of the CLK card. This information can also be found by using OBM.

#### Set Security Keyswitch

This constitutes a physical level of security that can restrict management access.

The security keyswitch located on the power status assembly controls the ability to use in-band or out-of-band management to modify GIGAswitch/FDDI System parameter settings. The keyswitch can allow OBM access with or without a password. It also controls the use of SNMP set commands; however, it does not override the requirement for a read-write community string password.

In particular note the following behavior of the security keyswitch:

- If it is turned to position 1 (no access) during an OBM session, the OBM session shuts down.
- In position 4 it allows OBM access if the OBM password is forgotten.

Figure 2-2 shows the location of the security keyswitch. Table 2-2 lists the different types of access allowed by different settings of the security keyswitch.

**Figure 2-2 Security Keyswitch**

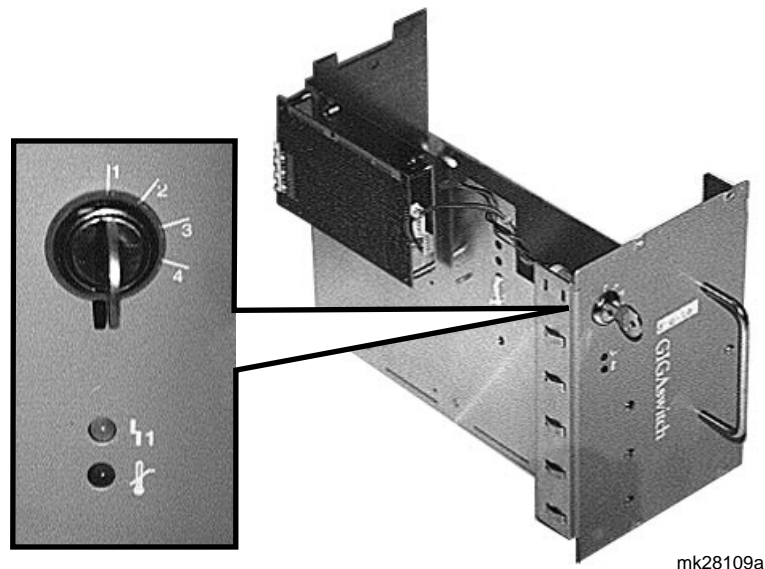




Table 2-2 Security Keyswitch Positions

Position	Function	Out-of-Band Access	In-Band Access
1	No access	No	No
2	Secure access	Password	Allows SNMP Get and GetNext requests only
3	Normal access	Password	Allows SNMP Get, GetNext, and Set <sup>1</sup> requests
4	Easy access <sup>2</sup>	Without password	Allows SNMP Get, GetNext, and Set <sup>1</sup> requests

<sup>1</sup>SNMP SET commands require any read-write community strings normally required on the network.

<sup>2</sup>Also called **world** access by the OBM terminal.

The security switch should be set to position 3 during initial setup.

---

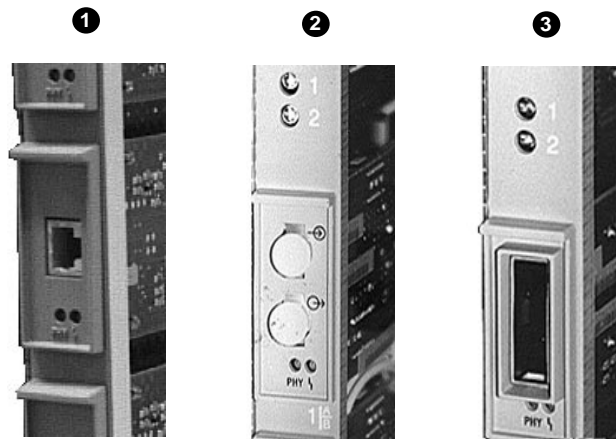
## Step 4: Connect the Datalinks

Cables need to be connected to the ports on the GIGAswitch/FDDI System linecards.

### FGL Ports

FGL ports contain one of three types of physical medium dependent modules (PMDs). Figure 2-3 shows the types of PMDs.

Figure 2-3 Types of Linecard PMDs



MK28171A

- ❶ Unshielded twisted-pair (TP-MIC connector)
- ❷ Single-mode fiber (FC-PC connector)
- ❸ Multimode fiber (ANSI MIC connector)

### Unshielded Twisted-Pair

The UTP accepts Category 5 unshielded twisted-pair (UTP) or Category 5 sheath-shielded, 100-ohm twisted-pair (TP) cable with a TP-MIC plug.

To connect the cable:

1. Align the release tab on the cable plug with the keyway on the UTP PMD.
2. Insert the plug into the connector, ensuring that the release tab snaps into the locked position.

### Single-mode FDDI

To install FDDI cables with single-mode connectors:

1. Remove the two protective caps from the connectors on the GIGAswitch/FDDI System.
2. Connect the fiber-optic cable to the appropriate connectors. Transmit (arrow-out) and receive (arrow-in) icons are marked on the handle of single-mode connectors.

3. Secure the connectors.
4. Verify that the other end of this cable is connected to a network device. If it is not connected, refer to the *Fiber Distributed Data Interface Network and Configuration Guidelines*.

**Multimode  
FDDI**

To install FDDI cables with multimode connectors:

1. Remove the protective dustcover from the GIGAswitch/FDDI System port by squeezing the locking clips on the sides and pulling out the cover.
2. Insert the FDDI cable connector in the correctly keyed orientation, pressing gently until the locking clips on the sides lock into place.

**AGL-2 Ports**

For information on the AGL-2 refer to the *GIGAswitch/FDDI System AGL-2 Manager's Reference Guide*, Chapter 3 Installation and Appendix E Guidelines and Installation for T3 and OC-3 AGL links.



---

## Firmware Upgrade Procedures

This chapter describes how to download new firmware.

The power system controller (PSC) and all logic modules can be loaded with new firmware images using SNMP commands from a network management station, DECndu Plus utility program or HUBloader.

Loadable firmware images that run on each module are described in Table 3-1.

**Table 3-1 Firmware Image**

<b>Module</b>	<b>Firmware Images</b>
SCP	Operational Firmware Bootblock Download Firmware
CLK	Operational Firmware
FGL-2	Operational Firmware
FGL-4	Operational Firmware
AGL-2	Operational Firmware Bootblock Backup Firmware
PSC	Operational Firmware

---

## Upgrade Process

The firmware upgrade process consists of the following steps:

1. Copy the proper image file and place it on a bootserver node.
2. Set the appropriate port and security parameters.
3. Transfer the image file from the bootserver to the GIGAswitch/FDDI System.
4. Move the image to the target module.

Once step 4 is completed the target module automatically reboots and runs the new firmware.<sup>1</sup>

The following sections describe these steps in detail.

### Upgrade Guidelines

Note the following important information about the firmware upgrade process:

- During the downline load process, the GIGAswitch/FDDI System firmware verifies the checksum of each image file before loading it. If a bad checksum is detected, the status available through SNMP returns as failed.
- GIGAswitch/FDDI System modules give the following indications when they are programming new images into flash. **Do not** power cycle a module or the GIGAswitch/FDDI System when Flash is being programmed.

SCP—Displays “D” on its hex display

PSC—Flashing amber on PSA LED

FGL—Flashing green module LED

CLK—No indication

Verify the new firmware image successfully loaded by using OBM or SNMP to check the firmware revision number.

### Time to Upgrade

The time it takes to upgrade each module depends on the time it takes to transfer the firmware code, the time to load the image to the module, and any powering off or rebooting required. Times depend on configuration and network load. Approximate times on a lightly loaded network are shown in Table 3-2.

---

<sup>1</sup> The exception to this is the AGL-2 backup image code.

Table 3–2 Approximate Upgrade Times

Module	TFTP doTransfer time	MOP doTransfer time	useTransfer time (including module reboot)
FGL-2	2 seconds	7 seconds	2 minutes 21 seconds
FGL-4	2 seconds	7 seconds	4 minutes 15 seconds
AGL-2	4 seconds	7 seconds	17 minutes
SCP	9 seconds	16 seconds	4 minutes

These times are only for reference. Transfer times vary widely depending on network traffic. Check the **transferStatus** to ensure successful completion of each step. Wait for the **transferStatus** to return the value "success," otherwise the upgrade could fail.

---

## Step 1: Copy Image Files to Bootserver

Ensure that the new firmware files are available on a bootserver node before attempting to load them into the GIGAswitch/FDDI System. When firmware for the GIGAswitch/FDDI System is released, it can be obtained on CD-ROM, or copied from the Internet. The Internet location and exact file names are provided when the firmware is released (for a standard upgrade), or upon purchase (for firmware containing new functionality).

If FTP is used to copy the image file, use image mode, not ASCII mode. If DECnet OSF is used to transfer the file, use the *-i* qualifier so the file is copied as an image file. If image mode is not used, an error message will be received during the upgrade, as the checksum for the image file fails verification. If this occurs, recopy the image file using the appropriate qualifier.



---

## Step 2: Set Port and Security Parameters

To perform an upgrade the management station (or the host running DECndu Plus) must be able to manage the GIGAswitch /FDDI System using SNMP. This requires the following:

- The port through which the NMS reaches the GIGAswitch /FDDI System must be a privileged port.
- The port through which the NMS reaches the GIGAswitch /FDDI System must have an assigned IP address.

In addition

- The port through which the server containing the firmware images reaches the GIGAswitch/FDDI System must be a bootserver port.
- The bootserver port must also have an assigned IP address.

Follow the directions in the *Out-of-Band Management (OBM) Guide* to effect these settings.

To execute the desired SNMP operations which will complete the final two steps, do the following:

- Determine the read-write community string.

If the read-write community string was previously set, use that name. If the community name was not set, use the default read-write community string.

The default read-write community string is the lowest system hardware address assigned to the GIGAswitch/FDDI System. Each switch is assigned a globally unique range of hardware addresses. They are stored in the CLK module. The address range is printed on a label on the front of the CLK card. This information can also be found using OBM.

Finally,

- Set the security switch to position 3 or 4 to enable SNMP set operations.

---

## Step 3: Transfer the Image File

This section describes the procedures used to transfer the image from a file server to the GIGaswitch/FDDI System. This step and the final load step may be performed together using either DECndu Plus or HUBloader. See the "Downloading Firmware Without a Management Station" section for a description of that process.

### Warning

This step must complete successfully before loading the image onto the target module. Check the status before attempting the final load procedures.

Table 3–3 indicates the transfer procedure that must be used for various image file types. Choose either the TFTP or MOP transfer procedure, and transfer the file type corresponding to the procedure of choice.

**Table 3–3 Image File Extensions**

File Extension	Transfer Method
.TFTP	TFTP
.MOP	ULTRIX MOP
.SYS	OpenVMS MOP
.RSX	TFTP or MOP

### TFTP Firmware Transfer Procedure

Table 3–4 lists the TFTP-related MIB objects that relate to firmware upgrades. The objects listed in this table are in the **gigaUpgradeSoftware doTransfer** group.

**Table 3–4 TFTP Firmware Upgrade Objects**

Object	Set To
<b>tftpDestination</b>	The IP address of the TFTP server containing the image file.
<b>transferFileName</b>	The name of the image file. <sup>1</sup>
<b>transferAction</b>	<b>doTFTP</b> . This command starts up a TFTP transfer.

---

<sup>1</sup>Typically only the file name has to be specified. The directory tree is defined by the TFTP server.

View the status of the **doTransfer transferStatus** object to see how the transfer went. The object should report "success." The **TransferSize** option will assist in monitoring the progress of the transfer, if it seems to be taking more time than expected.

**TFTP Example**

the following is an example using TFTP to copy the firmware file over the network. In this example:

- The read-write community string password is the default, which is its lowest hardware address (in this case it is *08002ba00200*). Note that it is enclosed in quotation marks.
- The GIGAswitch/FDDI System name is *giga1*.
- The IP address of the TFTP server is *16.20.36.7*.
- The name of the image file to be transferred is *bootimage.tftp*.
- The SHOW command shows all related attributes, including transfer status.

```
use default qualifier by password "08002ba00200"
use default entity snmp giga1 dec ema sysobjid bridges-
  gigaswitch gigaversion1 gigaupgradesoftware
set dotransfer tftpdestination 16.20.36.7
set dotransfer transferfilename "bootimage.tftp"
set dotransfer transferaction dotftp
show dotransfer all attributes
```

Successful completion indicates the image file has been transferred to the SCP. After successfully completing this procedure, proceed to the next section, "Move Image to the Target Module."

If the incorrect file name specification was inadvertently entered, wait for the failed status to be returned before retrying. The **doTransfer** operation cannot be stopped.

**MOP Firmware Transfer Procedure**

Table 3–5 lists the MOP-related MIB objects that relate to firmware upgrades. The objects listed in this table are in the **gigaUpgradeSoftware doTransfer** group.

**Table 3–5 MOP Firmware Upgrade Objects**

Object	Set To
<b>mopDestination</b>	The physical address of the MOP server. <sup>1</sup>
<b>transferFileName</b>	The name of the image file. <sup>2</sup>
<b>transferAction</b>	<b>doMOP</b> . This command starts a MOP load.

<sup>1</sup>Use the MOP multicast address: ab0000010000. On successive attempts, the **mopDestination** defaults to the address of the load host that responded to the previous request.

<sup>2</sup>Ensure that the file name length is within the limits set by the host's implementation of MOP. For most OpenVMS systems the limit is 16 characters.

View the status of the **doTransfer transferStatus** object to see how the transfer went. The object should report "success." The **transferSize** object will assist in monitoring the progress of the transfer, if it seems to be taking more time than expected.

### Step 3: Transfer the Image File

#### MOP Example

The following is an example of using MOP to copy the firmware file over the network. In this example:

- The read-write community string password has been set to *public*. This password is required for set commands. Note that it is entered in quotes. **Passwords are case sensitive.**
- The GIGAswitch/FDDI System name is *giga1*.
- The physical address of the MOP server is *08002b0602e5*.
- The name of the image file to be transferred is *bootimage.sys*.

```
use default qualifier by password "public"
use default entity snmp giga1 dec ema gigaswitch gigaupgradesoftware
set dotransfer mopdestination %x08002b0602e5
set dotransfer transferfilename bootimage.sys
set dotransfer transferaction domop
show snmp dotransfer all attributes
```

Successful completion indicates the image file has been transferred to the SCP. After successfully completing this procedure, proceed to the next section titled "Move Image to the Target Module."

If the incorrect file name specification was inadvertently entered, wait for the failed status to be returned before retrying. The **doTransfer** operation cannot be stopped.

---

## Step 4: Move the Image to the Target Module

Regardless of how the image file is transferred, the file must be moved to the target module to complete the upgrade procedure. This and the previous step may be performed in a single operation using either DECndu Plus or HUBloader. For information on that process see the section titled "Downloading Firmware Without a Management Station. "

### MIB Objects

Use the SET command to set two objects for this procedure. These objects are listed in Table 3–6.

**Table 3–6 Firmware Upgrade Objects**

Object	Set To
<b>copyToSlot</b>	The slot number that contains the target module
<b>copyAction</b>	doUpgrade: this activates the upgrade

### Loading the Image

Ensure that the proper slot is designated for the upgrade activity.

When upgrading multiple modules of the same type, the image file only needs to be transferred to the GIGAswitch/FDDI System once. Then each module can be loaded. Each module must be loaded separately. Only one slot number can be entered in the **copyToSlot** field. When upgrading the PSC (which is not contained in the card cage), enter a value of 7 for the **copyToSlot** field (the PSC firmware is loaded via the CLK card).

Poll **copyStatus** to ensure the upgrade goes well (note the **copyStatus** for an elected SCP upgrade cannot be polled because it automatically reboots). The response should be "inProgress" or finally "success". If the load procedure fails (the **copyStatus** is "failed"), repeat the procedure from the beginning.

If the image load fails, repeat the image load with the transferred firmware.

Check the **useTransfer TransferStatus** MIB object in the upgrade object group to verify when the FGL, clock card, or PSC firmware loading is done. When loading a backup SCP, ensure that the **useTransfer transferStatus** is "success", and that the new firmware version appears in the **slotstatus** table.

Step 4: Move the Image to the Target Module

**Example**

The following is a DECmcc Version 1.2 example of a downline load to slot 2 on a GIGAswitch/FDDI System named giga1.

---

**Note**

---

If the image file transfer is performed immediately before performing this procedure, the *use default qualifier by password...* command does not need to be reiterated.

---

```
use default qualifier by password "08002ba00200"  
use default entity snmp giga1 dec ema gigaswitch gigaupgradesoftware  
set usetransfer copytoslot 2  
set usetransfer copyaction dougrade  
show usetransfer all attributes
```

---

## Downloading Firmware Without a Management Station

The previous two steps may be performed together using either of the following Digital provided applications:

- DECndu Plus
- HUBloader

### DECndu Plus

The DECndu (Network Device Upgrade) Plus Version 1.0 utility allows users to update versions of software microcode resident in electrically alterable memory within supported hardware devices. The DECndu Plus Version 1.0 utility is installed on a load host and can be used to update the software microcode on eligible devices. SNMP/TFTP protocols are used to perform downline upgrades (see SPD 47.50.01).

### Ordering Information

For OpenVMS VAX operating system:

Software License: QL-0TYA9-AA  
 Software media and documentation: QA-0TYAA-H5  
 Software documentation only: QA-0TYAA-GZ

For ULTRIX/RISC operating system:

Software license: QL-0TZA8-AA  
 Software media and documentation: QA-0TZAA-H5  
 Software documentation only: QA-0TZAA-GZ

For MS-DOS:

Software license: QL-0U0AW-AA  
 Software media and documentation: QA-0U0AA-HC  
 Software documentation only: QA-0U0AA-GZ

### Preparing to Load

Perform the following before downline loading:

- Install DECndu Plus on the appropriate host system.
- Copy the files to be downloaded to the same or another host system that will act as the bootserver.

Identify the following before downline loading:

- IP address assigned to the selected GIGAswitch/FDDI System Port (for example: 16.20.36.23). Use the GIGAswitch/FDDI System OBM terminal to find the IP address for the selected port.
- Read-write community string for the GIGAswitch/FDDI system. The default read-write community string is the lowest Box LAN address that can be found using OBM.
- GIGAswitch/FDDI System module slot number (for example: the module in slot 12)

---

**Note**

---

For PSC code use slot 7, since the PSC is loaded via the CLK module.

---

**Downline Load the File**

Complete the following procedure to downline load the files:

1. Determine the status of the GIGAswitch/FDDI System module to be downline loaded (see Table 3-7).

```
$ DOWNLOAD SHOW DEVICE 16.20.36.23 /force=gigdescr /module=12
```

**Table 3-7 Description of DOWNLOAD SHOW DEVICE Command**

Command String	Description
<pre>\$ DOWNLOAD SHOW DEVICE 16.20.36.23 /force=gigdescr /module=12</pre>	<ul style="list-style-type: none"> <li>• DOWNLOAD SHOW DEVICE = Sends an SNMP get sysDescr if an IP address is used. This command displays a description of the device.</li> <li>• 16.20.36.23—IP address for the port by which the DECndu host is connected to the GIGAswitch /FDDI System..</li> <li>• /force=gigdescr—Forces DECndu Plus to go to the section of the SDDF.STP file that matches the device name.  <b>The device name for the GIGAswitch/FDDI System is gigdescr and NOT gigadescr as given in the example on page 3-10 of AV-Q1P4A-TE.</b></li> <li>• /module=12—Specifies the slot number in the GIGAswitch/FDDI System that DECndu Plus operations will affect.</li> </ul>

---

2. Perform the downline load (see Table 3-8).

```
$ DOWNLOAD load /module=12/password="08002b20d980" 16.20.36.23  
mom$load:fgl_op_200.rsx /force=GIGAswitch
```



**Table 3–8 Description of DOWNLOAD LOAD Command**

Command String	Notes
<pre>\$ DOWNLOAD LOAD /module=12 /password="08002b20d980" 16.20.36.23 mom\$load:fgl_op_200.rsx /force=GIGAswitch</pre>	<ul style="list-style-type: none"> <li>• <b>DOWNLOAD load</b>—Updates the specified device with the specified image.</li> <li>• <b>/module=12</b>—Specifies the slot number in the GIGAswitch/FDDI System that DECndu Plus operations will affect.</li> <li>• <b>password="08002b20d980"</b>—Specifies the read-write community string. The default read-write community string is the lowest Box LAN address for the GIGAswitch/FDDI System.</li> <li>• <b>16.20.36.23</b>—IP address for the port by which the DECndu host is connected to the GIGAswitch/FDDI System.</li> <li>• <b>mom\$load</b>—a logical for the location where images were installed in the load host (see example printout) for a definition of the logical</li> <li>• <b>fgl_op_200.rsx</b>—Name of the file to be downloaded.</li> <li>• <b>/force=GIGAswitch</b>—Forces DECndu Plus to go to the section of the SDDF.STP file that matches the device name.</li> </ul>

3. Verify the upgrade of the selected module (see Table 3–7).

**Example**

The following printout demonstrates the use of DECndu Plus to upgrade an FGL-2 module in slot 12 from version 1-71 to version 1-74.

```
$ DOWNLOAD SHOW DEVICE 16.20.36.23 /force=gigdescr /module=12
(c) Digital Equipment Corporation. 1993. All Rights Reserved.
[GIGDESCR] Getting GIGAswitch module Status.
3 - POWERUP

[GIGDESCR] Getting GIGAswitch module Type.
2 - FGL-2

[GIGDESCR] Getting GIGAswitch module Hardware Rev.
D
[GIGDESCR] Getting GIGAswitch module Firmware Rev.
1.71

$ DOWNLOAD load /module=12/password="08002b20d980" 16.20.36.23
mom$load:fgl_op_174.rsx /force=GIGAswitch
(c) Digital Equipment Corporation. 1993. All Rights Reserved.
```

## Downloading Firmware Without a Management Station

```
DECNDU: (TFTP) Target address = 16.20.36.23
[GIGAswitch ] Getting TFTP Server IP address.
0.0.0.0
[GIGAswitch ] Setting TFTP Server IP Address.
[GIGAswitch ] Getting TFTP Server IP address.
16.20.36.36
[GIGAswitch ] Getting firmware image file name.
[GIGAswitch ] Setting firmware image file name.
[GIGAswitch ] Getting firmware image file name.
MOM$LOAD:FGL_OP_174.RSX
[GIGAswitch ] Triggering image file transfer.
[GIGAswitch ] Starting TFTP Server
DECNDU: (TFTP) Blocks sent = 418
DECNDU: (TFTP) Transfer Complete.
[GIGAswitch ] Polling for file transfer completion.
5 - SUCCESS

[GIGAswitch ] Getting slot number.
0
[GIGAswitch ] Setting slot number.
[GIGAswitch ] Getting slot number.
12
[GIGAswitch ] Getting copyType.
3 - FGL-2

[GIGAswitch ] Triggering flash update.
[GIGAswitch ] Polling for load completion.
3 - IN_PROGRESS
3 - IN_PROGRESS
3 - IN_PROGRESS
3 - IN_PROGRESS
3 - IN_PROGRESS
3 - IN_PROGRESS
3 - IN_PROGRESS
3 - IN_PROGRESS
3 - IN_PROGRESS
3 - IN_PROGRESS
5 - SUCCESS

$ DOWNLOAD SHOW DEVICE 16.20.36.23 /force=gigdescr /module=12
(c) Digital Equipment Corporation. 1993. All Rights Reserved.
[GIGDESCR] Getting GIGAswitch module Status.
3 - POWERUP

[GIGDESCR] Getting GIGAswitch module Type.
2 - FGL-2

[GIGDESCR] Getting GIGAswitch module Hardware Rev.
D
[GIGDESCR] Getting GIGAswitch module Firmware Rev.
1.74
```

## **HUBloader**

HUBloader is a Windows application that can be used to do firmware upgrades for the GIGAswitch/FDDI System. It performs steps 3 and 4 of the firmware upgrade process.

HUBloader is bundled with a subset of the PATHWORKS IP stack similar to HUBwatch for Windows. A third party IP stack already installed on a PC should work just as well. However firmware upgrades require a TFTP Server to perform the actual loading. Third-party IP stacks need to include a TFTP Server to perform successful loads.

Some of the features incorporated into HUBloader are:

- Windows Interface
- Ability to do a SHOW and/or LOAD of a card's firmware (referenced by slot number)
- Two types of LOADs
  - From the user input information on the screen
  - From an editable file containing a list of cards
- Status box and status log file
- Selectable TFTP Server and load file
- Online Hyperhelp

## **How HUBloader Works**

HUBloader provides the ability to do two things—to SHOW information about a GIGAswitch/FDDI module, and to LOAD new firmware to the module.

Use the IP address of the GIGAswitch/FDDI System to identify it as the target of HUBloader.

## **Show Function**

The SHOW function will connect to the GIGAswitch/FDDI System and get the System Descriptor. Using the System Descriptor HUBloader will determine the system type, the current version of firmware for the designated slot, the latest version of firmware available for that type of module, and the corresponding load file.

## **Load Function**

By providing additional information the user can then LOAD firmware to the designated module. The user will also need to provide the IP address of the TFTP Server that will perform the load and the community string associated with the GIGAswitch/FDDI System. Note that the user does have the ability to overwrite any information provided by the SHOW function—in particular the user is free to specify any load file.

When the user selects a LOAD, HUBloader will put the GIGAswitch/FDDI System in a state where it requests that the identified TFTP Server load the system. At that point the TFTP load will occur independently of the HUBloader application. If using the TFTP Server from the local system, one may be able to examine the load status provided by the TFTP Server itself. The

TFTP Server provided with HUBloader will give such status. If the TFTP Server is at a remote site, there is probably no way to directly track the load status.

Because HUBloader runs independently of the actual TFTP Server load, HUBloader will periodically poll the agent being loaded for its System Descriptor. When HUBloader finds that the System Descriptor firmware version matches the latest firmware version associated with that agent it assumes that there was a successful load and discontinues polling the agent.

HUBloader also provides the ability to load a large number of modules listed in a load file. The load file contains one entry for each module to be loaded. Each entry contains the GIGAswitch/FDDI System's IP address, name, TFTP Server IP address, firmware load file, and community string. Each entry also contains the system type (G for GIGAswitch), and the associated slot number.

---

## Strategy for Upgrade with Backup SCP

If there are two SCPs use the following strategy to reduce the network impact from the SCP firmware upgrade:

1. Note which SCP is the elected switch engine. The SCP in the lower-numbered slot is generally the active (elected) SCP, with the other being available in standby mode. The HEX display will also indicate which is the elected SCP. The elected switch engine display reads **E**, the backup switch engine display reads **B**. In a remote upgrade, when the SCP is not physically visible, the GIGAswitch/FDDI System **slot scpSlot** MIB object contains this information.
2. Upgrade the backup SCP first. Load all necessary firmware images into the backup SCP. The SCP will reboot upon loading each new firmware image. Although it will reboot with each image, it will not impact the system because it is not currently the elected SCP.
3. Begin upgrading the elected SCP by loading the first image file, which will cause a failover to the backup SCP. At this point the backup SCP (which was already been upgraded), takes over all system SCP functions, and becomes the elected SCP. The original elected SCP now becomes the new backup SCP, so the upgrade procedure can be completed.

---

**Note**

---

Connectivity to the management station (and everything else) will be lost during failover, since all linecards will be reinitialized.

---

Ensure the LED on each SCP reflects the proper initial (E or B) prior to completing the upgrade. Continue loading until all image files are loaded in this second SCP.

4. Ensure each image transfer on any module is complete by viewing correct firmware revisions. This can be done by viewing the Slot Configuration through the OBM. This information is also contained in the GIGAswitch/FDDI System **slot SlotTable \* slotCardFwRev** MIB object, where \* represents the desired slot number. Note that because the PSC is not contained in a slot, its firmware information is contained in a separate MIB object, **psc pscFwRev**.

---

## Setting up Emergency SCP Firmware Download

During GIGAswitch/FDDI System initialization, the SCP checks its operational image code. If it detects that the operational firmware on the SCP is corrupt, it alternately flashes D/E on the SCP hex display. Then, it sends out BOOTP and MOP boot requests so that a good copy of the firmware replaces the corrupt image. Here are examples of how to set up a bootserver to respond to this eventuality.

### Bootserver Setup for DECnet-VAX MOP

The following is an example for setting up a bootserver for DECnet-VAX MOP:

```
NCP> Define Node GIGA1 Address 13.100
NCP> Define Node GIGA1 Hardware Address 08-00-2b-a0-02-4c
NCP> Define Node GIGA1 Service Circuit xNA-0 (SVA-0,QNA-0,etc.)
NCP> Define Node GIGA1 Load File bootimage.sys
NCP> Define Circuit xNA-0 Service Enabled
```

In this example, an entry is created in the DECnet node database for a GIGAswitch/FDDI System with the DECnet node address 13.100 and node name GIGA1. Although the GIGAswitch/FDDI System does not use DECnet, a DECnet node entry is created because MOP uses the DECnet node name database to look up hardware addresses from boot requests.

The hardware address should be set to the LAN address of the GIGAswitch/FDDI System port through which the bootserver will receive the boot request. This address can be obtained through the OBM Show LAN Addresses command under the Configuration Menu.

The service circuit is set to the DECnet circuit name for the LAN controller on the bootserver over which the boot request will be received.

The load file name is the file name of the operational firmware. Usually, load files are placed in the MOM\$LOAD: area, but they can be placed elsewhere as long as the location is specified in the load file command. The load files and load directory should be protected such that MOP will be able to read the files.

The DECnet circuit must be set to Service Enabled prior to providing bootserver assistance, otherwise the boot requests will not be serviced.

After doing the NCP DEFINE commands, it is necessary to reload the DECnet network, or to repeat the commands by using the NCP SET command instead of NCP DEFINE. SET commands affect the volatile (running) network; DEFINE commands affect the permanent database for future reboots. The SET CIRCUIT SERVICE ENABLED command cannot be executed on DECnet-VAX on a circuit with the state on.

The circuit must be set to off, and the service enabled; then the circuit must be set to on, as shown in the following example:

```
NCP> Set Circuit xNA-0 State Off
NCP> Set Circuit xNA-0 Service Enabled
NCP> Set Circuit xNA-0 State On
```

Note that this affects DECnet connectivity, so do not use remote DECnet access to perform this procedure.

### Bootserver Setup for ULTRIX MOP

An entry must be added to the nodes database for the GIGAswitch/FDDI System. It does not require a DECnet address. The entry follows.

```
/etc/addnode giga1 -h 08-00-2b-a0-02-4c -l /usr/lib/mop/  
bootimage.mop
```

Where:

- The *-h* specifies the hardware address. This should be set to the LAN address of the GIGAswitch/FDDI System port through which the bootserver will receive the boot request. This address can be obtained through the OBM Show LAN Addresses option under the Configuration Menu.
- The *-l* specifies the load file location and name. Normally, MOP load files are placed in the /usr/lib/mop directory.

The mop\_mom load listener must be started. This is done by entering:

```
/etc/mop_mom
```

This command is normally placed in the /etc/rc.local file. Refer to the man pages for mop\_mom for additional details.

### Bootserver Setup for BOOTP

Here is an example of a /etc/bootptab file:

```
giga1 1 08:00:2b:a0:02:4c 192.208.101.14 bootimage.tftp
```

In this example, the default load file is defined as bootimage.tftp.

The hardware address in the example is set to 08-00-2b-a0-02-4c. This should be set to the LAN address of the GIGAswitch/FDDI System port through which the bootserver will receive the boot request. This address can be obtained through the OBM Show LAN Addresses option under the Configuration Menu.

The BOOTP and TFTP daemons must also be started. Usually these are configured in the /etc/inetd.conf by file including a line of the form:

```
bootp dgram udp wait /usr/etc/bootpd bootpd -i -d  
tftp dgram udp nowait /usr/etc/tftpd tftpd -r /usr/users/  
bootfiles
```

The default load file area is set up as /usr/users/bootfiles.

It may be necessary to "kill -HUP ###," where ### is the process ID for inetd, to force inetd to reread the configuration file.





**Purpose of this Chapter**

This chapter explains basic filtering concepts and how the GIGAswitch/FDDI System handles filtering. Filters can be created with a network management station (NMS) to help resolve potential traffic problems or security problems on the network.

This chapter describes use of the management information base (MIB) objects in the **filterByReferencedExpression** group. This group of objects provides the easiest specification and assignment method for filter values. Although filters can be created by using the **filterByBitmapValue** group of MIB objects, the filter design and specification is more complex, and provides no additional filtering functionality over the **filterByReferencedExpression** group. For additional filter examples refer to Appendix A.

---

## Filtering Basics

### Reasons for Filtering

Filters can be used to reduce unnecessary system or network loads, or to constrain network traffic so it reaches its intended destinations and no unnecessary network devices.

Filtering can also assist with network security, allowing network managers to isolate privileged network traffic or parameter modification privileges to a small subset of network nodes. Filters can isolate network devices during network troubleshooting. They can control BOOTP or *address resolution protocol (ARP)* requests, or downline load traffic. They can also restrict certain protocols to specific sections of the network.

### Dynamic Filtering

Two types of filtering may occur in an operational GIGAswitch/FDDI System: dynamic and static. Dynamic filtering occurs automatically, with no manager specification or intervention required. This filtering is common to most bridges. Dynamic filtering keeps a packet from traversing a datalink when its destination is known to be elsewhere.

As network traffic flows through the GIGAswitch/FDDI System the source MAC address (SA) of each packet is observed, and the switch notes the port of arrival. This association of MAC address to port is known as the forwarding database, or translation table.

The forwarding database is used to assure a unicast packet is sent only to the port corresponding to its destination address (DA), thus filtering (blocking) its transmission to all other ports.

In particular, a packet whose DA is known to be on the port of arrival is not sent through the crossbar at all.

### Static Filtering

Static filtering is the result of management-set filters. These are directives to transmit or block certain packets, depending on inbound or outbound port, SA, DA, or protocol type—or some combination of these. The following sections describe how to use static filtering.

**Advantages of Filtering**

The GIGAswitch/FDDI System allows flexibility in setting up filters. A flexible SNMP specification syntax is used to create matrices that specify certain input ports can only connect with certain output ports. This provides an input/output (I/O) port pattern that is stored for future use. These I/O port patterns are then applied to various DA, SA, and protocol ID (PID) instances. When a packet enters the GIGAswitch/FDDI System, any applicable filters are called into play based on DA, SA, and PID, and are combined in a logical manner.

**Restrictions**

GIGAswitch/FDDI System filtering will **not** effect the splitting of the GIGAswitch/FDDI System into multiple bridges with separate spanning trees or separate learning domains.

---

## Filter Setup

To set up filters for the GIGAswitch/FDDI System, perform the following tasks:

- Decide which ports should be able to intercommunicate, and design an I/O port pattern matrix based on this decision.
- Specify the I/O port pattern matrix by using the appropriate MIB objects.
- Apply the I/O port pattern matrix to the desired SA, DA, or PID by specifying the correct filter table entries. Choose the filter disposition as described below.
- Create additional filters that will logically combine to create the desired traffic flow response.

### Port Pattern Matrices

When filters are set up on a 2-port bridge, a decision must be made whether to filter (block) a packet or forward it through the bridge.

With the GIGAswitch/FDDI System the complexity increases. There are 36 crossbar ports and the filter/forward decision may vary depending on both input and output port. An I/O port pattern matrix is used to represent whether any input port is allowed to forward packets (or not) to the 36 possible output ports. This I/O port pattern matrix can also be called a *reachability matrix* because it indicates which input ports can reach which output ports.

This matrix is designated by using the **ebrNportMatrixNameTable**. Entries are created in this table (**ebrNportMatrixNameEntry**) and these entries taken together form the table itself. To create an entry, specify the following:

- **ebrNportMatrixName** — Each port pattern created should have a meaningful name, pertaining to the purpose it is used for. This name should be 32 characters or less (some management stations have more restrictive requirements).
- **ebrNportMatrixStatus** — If the matrix is being created the status should be *permanent*. If the matrix is being removed the status should be *invalid*.
- **ebrNportMatrixValue** — This is the port pattern itself for the matrix being created.

The I/O port pattern may be pictured as a matrix of 0s and 1s. Table 4-1 shows how to map the input ports of the system to the rows and the output ports of the system to the columns of the matrix:

Table 4-1 I/O Port Matrix Table

Output Port	1	2	3	4
<b>1</b>				
<b>Input</b>	<b>2</b>			
<b>Port</b>	<b>3</b>			
	<b>4</b>			

We will use a **1** to indicate an intention to pass the packet, and a **0** to indicate an intention to block the packet. A matrix can be set up for any instance of I/O traffic flow. Place the 0 or 1 in the space where the desired input port (row) and output port (column) intersect.

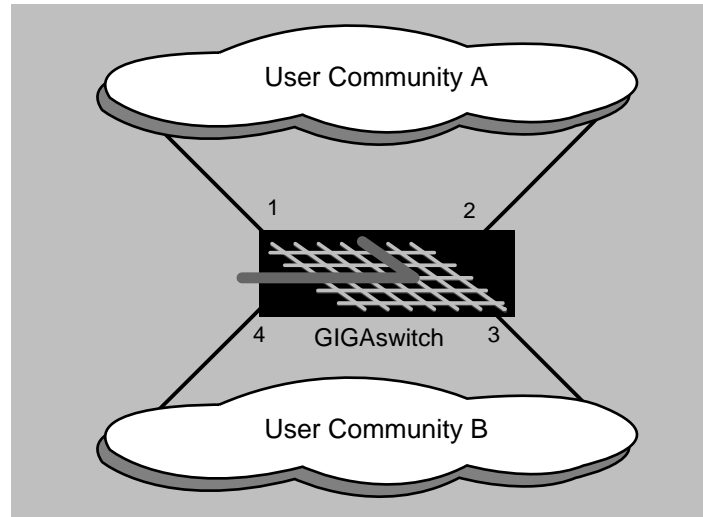
Note that once an I/O port pattern matrix is created there are further steps to take in order to apply the matrix to a given SA, DA, or PID. Actual blocking or forwarding of the packet depends on what I/O port patterns apply to the packet and the dispositions set for each. These steps are in the section titled Creating a Filter Based on SA, DA, or PID in this chapter.

### Matrix Example

Imagine users on separate rings that connect to separate ports on the GIGAswitch/FDDI System. The users connected to bridge ports 1 and 2 form one user community, and the users connected to bridge ports 3 and 4 form a second user community, as shown in Figure 4-1.

One user community may be development and the other administration. There may be a desire to restrict the flow of packets between user communities, perhaps for security reasons. So, it is best to ensure the packets entering the system on ports 1 or 2 can only leave the GIGAswitch/FDDI System on ports 1 or 2, and to ensure the packets entering the system on ports 3 or 4 can only leave the GIGAswitch/FDDI System on ports 3 or 4.

Figure 4–1 Four-Port, Two User Community Configuration



MR-6382-AD

For our example, we would need to create the matrix shown in Table 4–2 to meet our traffic filtering needs. A **1** indicates where we want the packet to travel from the input port (row) to the output port (column); **0** indicates where we want to block it.

Table 4–2 Port Matrix Table

Output Port		1	2	3	4
	<b>1</b>	1	1	0	0
<b>Input</b>	<b>2</b>	1	1	0	0
<b>Port</b>	<b>3</b>	0	0	1	1
	<b>4</b>	0	0	1	1

### Specifying the Matrix

Setting the **ebrNportMatrixValue** object employs sequential port numbers (SPN), and a convenient syntax to specify the rows of the desired matrix. Semicolons separate expressions. Within each expression, the information to the left of the colon describes the inputs; the information to the right of the colon describes the outputs. Bridge ports on the left side can send packets to bridge ports on the right side. Commas separate items in a list of bridge ports. Hyphens specify a range of numbers.

In the case above, indicate the desired reachability matrix or port pattern in either of these ways:

```
(1,2:1,2;3,4:3,4)
(1-2:1-2;3-4:3-4)
```

The commas separate different bridge port numbers, a dash shows a range of ports. Although they are listed here in numeric order, they need not be.

Alternatively front panel port numbers (FPPN) may be used to specify a matrix by using the **ebrNportMatrixFppnValue** objects. Simply replace the SPNs in the above syntax with FPPNs.

## Examples

If traffic is to go both ways through a port set, both directions must be specified, as shown in the first line of Table 4–3.

**Table 4–3 Sample Port Filter Entries**

Filter Entry	Explanation
(1:4;4:1)	Traffic can flow from port 1 to port 4, and port 4 to port 1.
(1,2,5:8)	Traffic can flow from ports 1, 2, and 5 to port 8.
(1,3:8,10)	Traffic can flow from ports 1 and 3 to ports 8 and 10.
(1-5:9-10)	Traffic can flow from ports 1, 2, 3, 4, and 5 to ports 9 and 10.
(1-3:5;5:3)	Traffic can flow from ports 1, 2, and 3 to port 5, and from port 5 to port 3.

If the **ebrNportMatrixValue** (or **ebrNportMatrixFppnValue**) is changed, all filters using the old port pattern are immediately updated to use the new one.

## The Default Filter Matrix

One filter matrix is applied to every packet. The default filter matrix defines a port pattern in the same way as other filter matrices. In the absence of other applicable filters, the default filter matrix alone determines whether a packet will be forwarded or blocked. When other filters are applicable to a packet, the default filter matrix is combined with the other filter matrices to determine how that packet is treated.

## Changing the Default Filter Pattern

When a GIGAswitch/FDDI System is booted for the very first time the default filter matrix is all 1s; it allows packets to be forwarded between any input and output ports. The default filter matrix can be altered by using the MIB objects **erbNportDefaultMatrixValue** or **ebrNportDefaultMatrixFppnValue**, using the same syntax employed in setting other matrix values.

---

## Creating a Filter Based on SA, DA, or PID

After creating a reachability matrix, or I/O port pattern, call it into use by assigning values to MIB objects in one of four identically designed tables, for SA, DA, *service access point (SAP)* and *subnet access protocol (SNAP) filters*.

For example, to create a filter based on SAP, the **ebrNportSapNameTable** must be modified. Each entry is an **ebrNportSapNameEntry** and corresponds to a SAP filter. Each entry contains five items, as listed in Table 4–4.

Table 4–4 SAP Filter Entry Objects

Object	Description
<b>ebrNportSapName</b>	The name used to refer to this filter entry. A “handle” that lets you “grasp” this combination of filter objects as a unit.
<b>ebrNportSapNameSap</b>	The octet string that represents the SAP that, when detected, calls this filter into use so it is applied to the desired packets.
<b>ebrNportSapMatrixName</b>	The name of the I/O port pattern this entry will use.
<b>ebrNportSapNameStatus</b> <sup>1</sup>	The status for a filter entry has value <b>1</b> meaning this entry is invalid, or <b>2</b> meaning this entry is valid. Only valid entries will be applied. This is the mechanism for deleting filters. Once the status of a filter is set to 1 (invalid) it can never be set back to 2 (valid).
<b>ebrNportSapNameDisp</b>	The disposition can be one of three integers. 1 indicates the lowest precedence <b>filter</b> . 2 indicates the middle precedence <b>alwaysForward</b> . 3 indicates the highest precedence <b>alwaysFilter</b> .

---

<sup>1</sup>When creating an entry, the status will always be 2 (permanent).

---



**Filter Matrix**

The filter matrix determines which input-output paths are allowed by that filter. The matrix entry along with the disposition helps determine whether to forward or block a packet. Every filter has an associated filter matrix which governs whether that filter directs packets to be forwarded or blocked.

**Disposition**

The filter disposition determines how that filter should interact with other applicable filters. Since a filter may be triggered by either SA, DA, or PID, it's possible that a given packet is governed by as many as three filters. These filter matrices (and the default filter matrix) may give conflicting indications of whether to forward or block (filter) the packet. The dispositions and values of the applicable filter matrices (SA, DA, PID and default) determine whether the packet is actually forwarded or blocked (filtered).

The default filter matrix applies to every packet and is treated as a matrix with disposition **filter**. Other filters can have disposition **filter**, **alwaysForward**, or **alwaysFilter**. The filters work together this way:

In each applicable matrix look at the position whose row corresponds to the input port number and whose column corresponds to the output port number. Use these rules to combine the filter matrices:

- Rule 1:  
If one of the matrices has disposition **alwaysFilter** and has a 0 in that position, then block the packet. If not, use rule 2.
- Rule 2:  
If one of the matrices has disposition **alwaysForward** and has a 1 in that position, then forward the packet. If not, use rule 3.
- Rule 3:  
If one of the matrices has disposition **filter** and has a 0 in that position, then block the packet. If not, forward the packet.

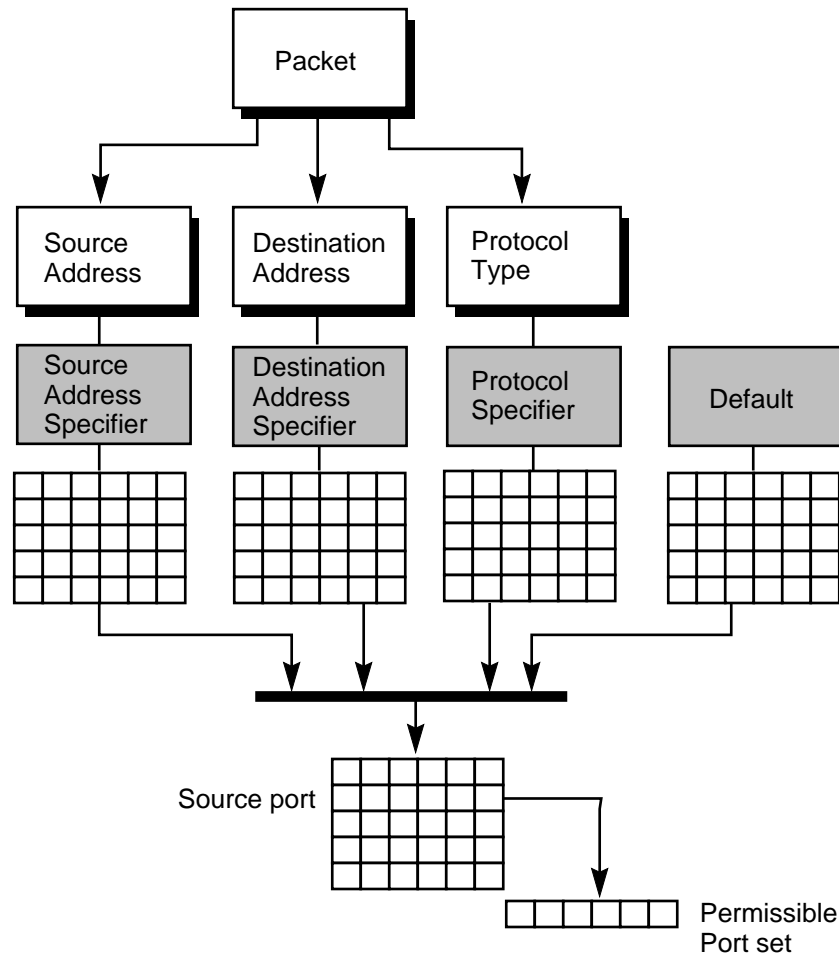
In summary, an **alwaysFilter** disposition matrix that says to block takes precedence. If none exists, an **alwaysForward** disposition matrix that says to forward is next in priority order. In the absence of these, a matrix with **filter** disposition that says to block takes precedence over a matrix with **filter** disposition that says to forward.

**Combining  
Several  
Matrices**

Knowing how dispositions combine can help in creating a filter structure that meets the needs of your network. Figure 4-2 shows how a packet's arrival triggers the SA, DA, and PID specifiers which in turn trigger the application of port pattern matrices as appropriate, in combination with the default matrix.

The entries in the applicable filter matrices are combined according to the above rules, resulting in a final matrix that governs the forwarding of a particular packet.

**Figure 4-2 Port Pattern Combinations**



MR-6381-AD

The row in the final matrix that corresponds to the source port of the incoming packet is read by the GIGAswitch/FDDI System. This row specifies the permissible outbound port set for packets coming from the given source port. The bit that fills the column slot for the desired output port of that packet determines what happens to the packet (1=forward, 0=block).

## **Filtering and Broadcast Packets**

Filtering works with broadcast and multicast packets to minimize the traffic passing through the GIGAswitch/FDDI System. Normally, packets that are broadcast or multicast frames are forwarded to all active ports. If one or more filters applies to the broadcast packet entering the GIGAswitch/FDDI System, a set of permissible output ports is computed as usual. The broadcast packet is only forwarded to ports in the permissible output port set, as found in the matrix resulting from the applicable filter combinations.

This optimization ensures that broadcast and multicast packets are not forwarded to unnecessary ports, reducing system traffic where possible.

---

## Filter Examples

### Blocking Traffic

By default, the GIGAswitch/FDDI System performs dynamic learning. As it learns the addresses each port connects to, it ensures that frames sent between nodes on the same port are blocked (filtered), since they need not pass through the switch to reach their destination.

You may want to block certain traffic from traveling through the GIGAswitch/FDDI System, or to constrain certain internode messages to specific parts of a network configuration. For example, imagine a four-port GIGAswitch/FDDI System configuration. Each port has a DECnet area attached to it, and the packets are all, by default, passed through the GIGAswitch/FDDI System.

For example, to constrain multicast level 1 routing messages to their own areas, create management-specified static filters to supplement the system's internal dynamic filtering.

To do this, create a filter matrix that describes what needs to happen. In this case, it is desired that *no* DECnet multicast routing messages pass through the GIGAswitch/FDDI System.

A filter matrix to perform this action is specified as:

(1:1, 2:2, 3:3, 4:4)

Table 4-5 shows the matrix.

**Table 4-5 Port Matrix Table**

Output Port		1	2	3	4
	1	1	0	0	0
Input	2	0	1	0	0
Port	3	0	0	1	0
	4	0	0	0	1

In this case, the filter setup would be as follows:

- Goal: No DECnet multicast through gigaswitch1.  
 Filter based on: multicast DECnet DA  
 Port pattern: (1:1, 2:2, 3:3, 4:4)  
 Disposition: **filter**

## Multiple Computer Site

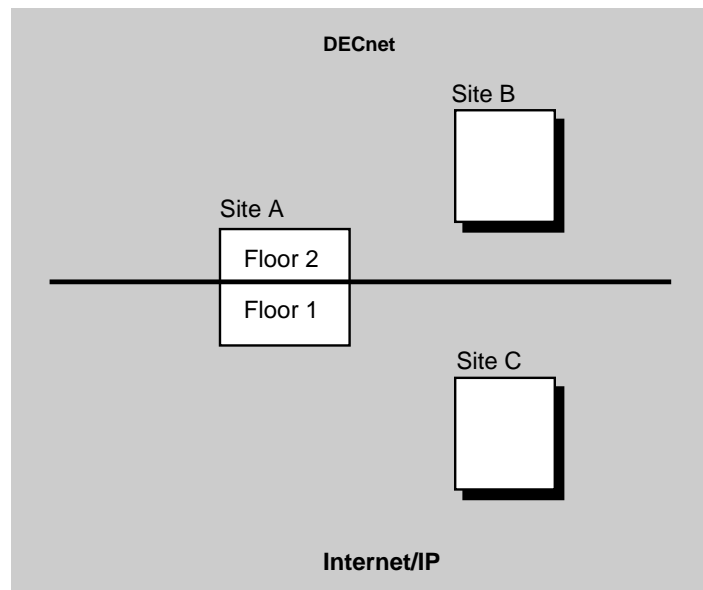
Figure 4–3 shows multiple computing sites that support different departments.

There are three sites, divided into two user communities:

- Users on the first floor of site A and all of site C do development and testing with outside researchers by using the Internet.
- Users on the second floor of site A and all of site B use an application layered on top of DECnet.

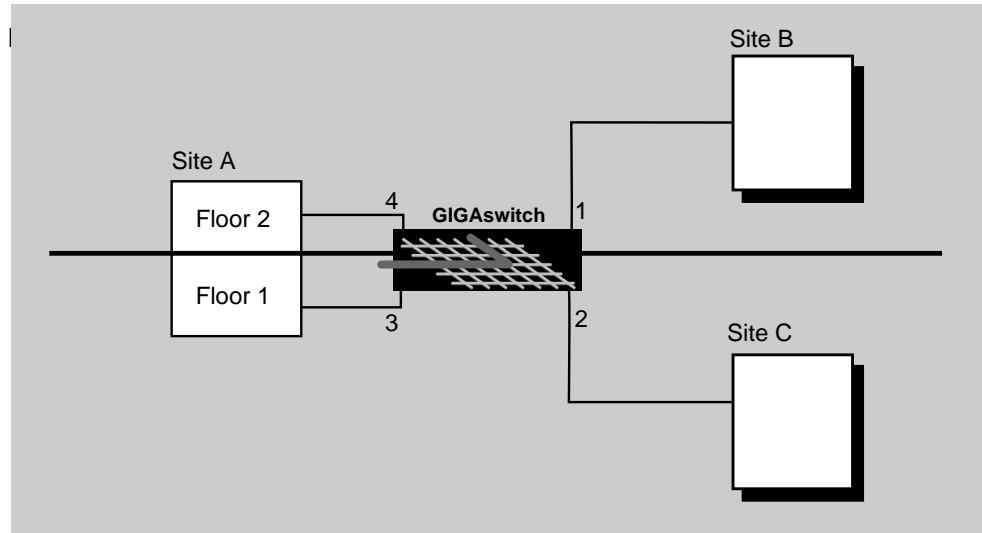
Since the communities use different protocols we can reduce traffic in both by restricting the flow of packets using those protocols to be within each community.

**Figure 4–3 Multiple Department Configuration**



TAY-0251-AD

The GIGAswitch/FDDI System shown in Figure 4-4 assists by isolating the DECnet and IP traffic to their respective environments, primarily the broadcast and multicast traffic. The system is physically located at site A, but services both network environments with the implemented filters.



TAY-0252-AD

In this case, the filter setup would be as follows:

- Goal: To pass IP packets only between ports 2 and 3.  
 Filter based on: IP SAP  
 Port pattern: (2,3:2,3)  
 Disposition: **filter**
- Goal: To pass DECnet packets only between ports 1 and 4.  
 Filter based on: DECnet SNAP  
 Port pattern: (1,4:1,4)  
 Disposition: **filter**

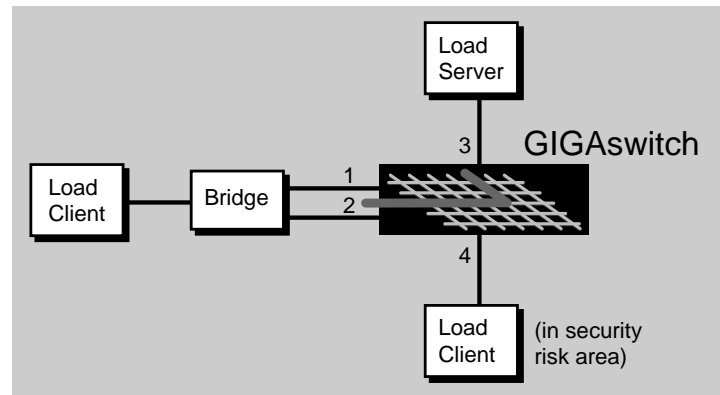
Note that in this case a single port pattern could be created that would serve for both filters:

(1,4:1,4 ; 2,3:2,3)

## Securing a Load Server

Figure 4–5 shows a college campus configuration.

Figure 4–5 College Campus Configuration



TAY-0248-AD

In this example, the load server for the campus resides on port 3 of the GIGAswitch/FDDI System. There are several load clients connected to this load server, one of them located in an undergraduate dormitory.

To ensure security, set up filtering so that load responses are allowed only from the source address of the load server, and load requests are allowed to go only to the destination address of the load server. This prevents another source address from masquerading as the load server. In this case, set up the following filter:

- Goal: To ensure load requests only go to the load server.  
 Filter based on: DA of server  
 Port pattern: (1,2,4:3)  
 Disposition: **filter**
- Goal: To ensure load responses only come from the load server.  
 Filter based on: SA of server  
 Port pattern: (3:1,2,4)  
 Disposition: **filter**

---

## Additional Means of Controlling Packet Flow

The previous sections described how filters can be used to control the flow of packets through the GIGAswitch/FDDI System. Another way of controlling packet flow is to control the contents of the forwarding database itself. Ordinarily the forwarding database is built up automatically by observation of the source address (SA) of each incoming packet. The techniques described in this section provide for management control over the contents of the forwarding database. In one case certain entries are specifically added to the database. In the second case automatic learning and forwarding is inhibited.

### Locking Down an Address

In addition to learning addresses dynamically, the address database can also receive entries from an NMS. By specifying a station address and the bridge port where that station is located, a manager can lock that station to that port. This creates a permanent entry for that address node and causes the bridge to ignore any learned information that differs from this permanent entry.

Use the GIGAswitch/FDDI System MIB object **ebrNportPortNumTable** to lock down an address. An example DECmcc command to lock down a physical address to a port follows:

```
set snmp giga1 dec ema gigaswitch gigaverstion1 gigabridge ebrNportPortNumTable -
  ebrNportPortNumAddress %x 08002b02f070 ebrNportPortNum 10
by password 08002b01ac20
```

Where:

- *08002b02f070* is the physical address that will be locked to the port.
- *10* is the bridge port number to which the address is locked.
- The variable *08002b01ac20* is the read-write community string password.

The command causes the address to be mapped to port 10. By additionally specifying an SA filter, one can be assured that packets with SA = the locked down address will only be forwarded through the switch when received on the locked down port.

### Manual Mode

Place a specified bridge port into manual mode to prevent forwarding of any packet destined to, or originate from an unknown or dynamically learned address.

Manual mode is used on ports when the traffic must be carefully controlled. It is often used for a bridge port on the periphery of an extended LAN to ensure that only a predefined set of addresses has access to the rest of the extended LAN. This also enhances



security by preventing a user on the manual mode port from masquerading as another user on a different port.

The GIGAswitch/FDDI System MIB objects **ebrNportManualFilter** and **ebrNportFppnManualFilter** contain the list of ports in manual mode. Only packets with the DA and SA specified by **ebrNportPortNumTable** (SA and DA are both locked down) can be forwarded to a manual mode port.

For example, if port 7 is in manual mode the only packets that will pass out of the GIGAswitch/FDDI system through port 7 are those whose SA and DA are both locked down.



---

## Additional Filter Examples

### Introduction

This appendix contains two examples of GIGAswitch/FDDI System filters set up to control traffic in multi-site OpenVMS cluster environments. An OpenVMS cluster is a collection of OpenVMS hosts working together as a single distributed System. A distributed file system allows the individual hosts of the cluster to easily share files and other resources.

Both examples depict an OpenVMS cluster that spans several buildings and floors, with several FDDI rings serving as the cluster interconnect. The FDDI rings are themselves bridged together through a GIGAswitch/FDDI System.

The filters described in these examples are created using the **FilterByReferencedExpression** object group from the GIGAswitch/FDDI MIB. For consistency we will always refer to ports using sequential port numbers (SPN). Hence we will set the object **ebrNportMatrixValue**. Alternatively we could refer to ports using front panel port numbers (FPPN), using instead the object **ebrNportMatrixFppnValue**. Either numbering system can be used to create a filter matrix. Chapter 1 describes these two port numbering systems.

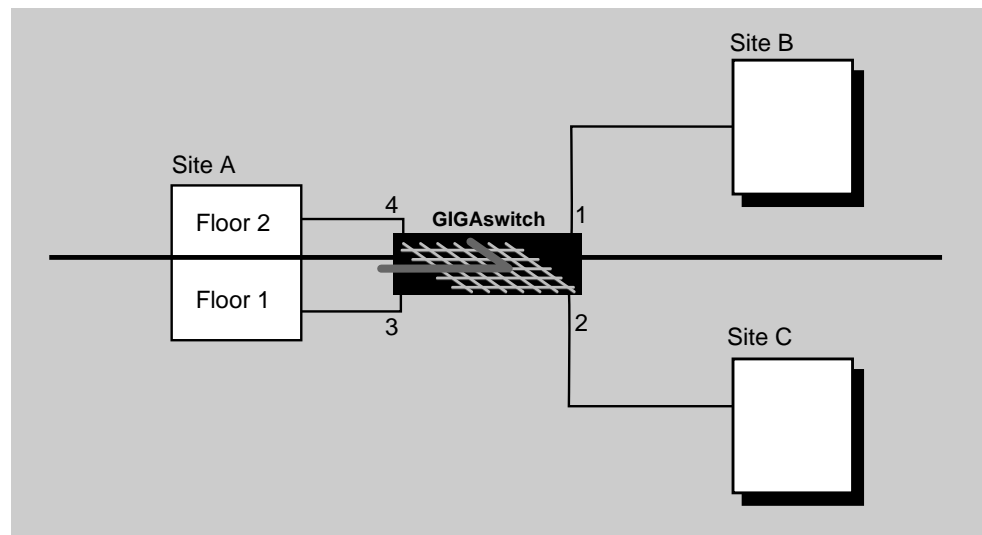
---

## Example 1: Filter for MOP Downline Load Requests

### Network Configuration

Figure A-1 shows a GIGAswitch/FDDI System connecting four rings located in three buildings; site A, site B, and site C. Site A is further divided between floor 1 and floor 2. Each of these four rings is connected to a single GIGAswitch/FDDI System port. Floor 1 of site A has a "server ring," made up of systems that act as servers for disks containing boot files required by other systems in the network.

Figure A-1 Three-Building Example



TAY-0252-AD

### MOP

The clustered systems and devices boot over the network by sending maintenance operations protocol (MOP) downline load requests to the MOP downline load multicast destination address (%xAB0000010000). In the given configuration these requests are serviced by systems on the server ring, located on floor 1 of site A.

### Desired Filter

It is required that MOP requests reach the server ring (port 3), but they should be kept from being forwarded onto other rings (except, of course, the ring of origin). A filter will be created to achieve this. It will be activated by the MOP multicast destination address, so it will be a DA filter.

## Creating the Reachability Matrix

The reachability matrix for this filter should allow the specified packets to be forwarded from any input port to port 3, but to no other port. Hence it will be specified as follows: (1,2,4:3). The following command will define the desired matrix:

```
set snmp myriad dec ema sysobjid bridges gigaswitch gigaversion1 gigaBridge -
  filterByReferenced Expression -
  ebrNportMatrixNameTable mop_site_matrix -
  ebrNportMatrixValue (1,2,4:3) -
  ebrNportMatrixStatus permanent
```

Where:

- *myriad* is the name of the GIGAswitch/FDDI System.
- *dec ema sysobjid bridges gigaswitch gigaversion1 gigaBridge filterByReferencedExpression* refers to the branch of the MIB object tree from which objects will be used.
- *ebrNportMatrixNameTable* is the table in which we are creating an entry.
- *mop\_site\_matrix* is the name of the filter matrix being created.
- *1,2,4:3* is the specification of the matrix value desired— which allows packets entering ports 1, 2, and 4 to be forwarded to port 3.
- *permanent* is the required status of any newly defined matrix.

## Creating the Filter

The next command will actually create the filter that uses the above matrix. Since it is a DA filter we create an entry in the DA Name Table. We use the following command:

```
set snmp myriad dec ema sysobjid bridges gigaswitch gigaversion1 gigaBridge -
  filterByReferenced Expression -
  ebrNportDANameTable mop_site_filter
  ebrNportDANameDA %Xab0000010000
  ebrNportDAMatrixName mop_site_matrix
```

Where:

- *myriad* is the name of the GIGAswitch/FDDI System.
- *dec ema sysobjid bridges gigaswitch gigaversion1 gigaBridge filterByReferencedExpression* refers to the branch of the MIB object tree from which objects will be used.
- *mop\_site\_filter* is the name used to refer to this filter.
- *ab0000010000* is the multicast address whose presence will trigger this filter.
- *mop\_site\_matrix* is the name of the matrix (defined above) which will determine which input/output ports a packet will be allowed to traverse if governed by this filter.

Note: if an explicit disposition is not specified the filter disposition defaults to "**filter.**"

## Example 1: Filter for MOP Downline Load Requests

### **Resulting Behavior**

With this filter in place, packets with the MOP downline load multicast destination address will be forwarded from ports 1, 2, and 4, to port 3 only.

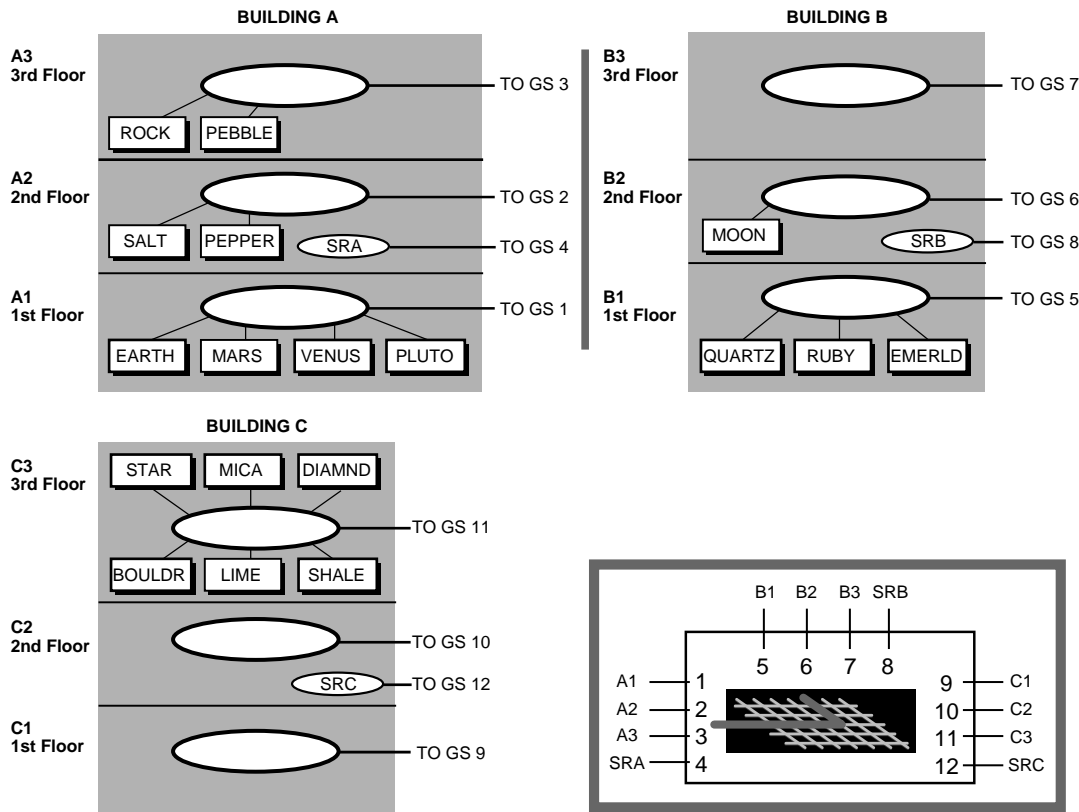
All MOP downline load requests from any ring in any building will be sent only to the server ring.

## Example 2: Filters for Multiple OpenVMS Clusters

### Network Configuration

Figure A-2 shows a cluster environment which spans three floors in each of the three buildings (sites A, B, and C). There are 12 FDDI rings in all, 1 each on floors 1 and 3 of each building, and 2 rings on the second floor of each. A MOP server ring on the second floor serves the nodes in each building. The MOP server rings are designated SRA, SRB, and SRC in sites A, B, and C, respectively.

Figure A-2 Filter Example Configuration



TAY-0174-AD

There are three OpenVMS clusters in this environment. Hosts names for each cluster are shown in Table A-1.

**Table A-1 OpenVMS Clusters**

Cluster Name	Site Floors	Systems
Cluster-1	A1, B2, C3	EARTH, MARS, VENUS, PLUTO, MOON, STAR
Cluster-2	A3, B1, C3	ROCK, PEBBLE, QUARTZ, RUBY, EMERLD, MICA, DIAMND, BOULDR, LIME, SHALE
Cluster-3	A2	SALT, PEPPER

### Desired Filters

Filters will be created to ensure that certain cluster traffic flows only between members of the same cluster. The traffic to be controlled is used by cluster members to ensure that all members are available and on line. It consists of "keep-alive hello" messages, which are multicast packets sent at regular intervals by each cluster member. The multicast address identifies the cluster for which it is intended. It is critical that these messages reach every node in the cluster. We will use filters to ensure they do not go to rings containing no cluster members.

### Two Strategies

To allow the hello messages to travel between some systems and not others, the filters can be set up in either of two ways:

- **Filter using multicast address:** Limit allowed forwarding of known multicast addresses for existing clusters. This requires only one filter per OpenVMS cluster and is easy to manage. If new OpenVMS clusters join the network, the network manager need to add a new filter for each new OpenVMS cluster's broadcast address. Using this method, you can add additional nodes to an OpenVMS cluster on rings that already contain members of that OpenVMS cluster without requiring new filter definitions. However, this method is not highly secure.
- **Filter using SCS protocol type and SA:** Block all cluster traffic, then allow exceptions to be forwarded. One benefit of this setup is that network administration has more control over OpenVMS cluster connections. It also yields a more secure filtering mechanism. However, over time, you would need to add a new filter whenever a new node is added to an OpenVMS cluster that spans multiple floors. Using this method, you cannot move OpenVMS cluster nodes between GIGAswitch/FDDI System ports without requiring new filter



definitions. Over all, more filters must be created and more network management could result.

### Multicast Address Filter

First, limit Multicast traffic for clusters with all nodes on one GIGAswitch/FDDI port (on one ring). Cluster-3 is used in this example.

---

#### Note

---

When specifying a filter for the first time, all fields in the filter entry must have values assigned.

---

### Set Up I/O Port Pattern

This command sequence sets up a port pattern, or reachability matrix, that restricts all traffic to its own ring:

```
set snmp myriad dec ema sysobjid bridges gigaswitch gigaversion1 gigabridge -
  filterByReferencedExpression -
  ebrNportMatrixNameTable lavc_def_matrix -
  ebrNportMatrixValue (1-12:), -
  ebrNportMatrixStatus permanent
```

Where:

- *myriad* is the GIGAswitch FDDI System name.
- *dec ema sysobjid bridges gigaswitch gigaversion1 gigabridge filterByReferencedExpression* specifies the location of the MIB objects that will be used in the object tree.
- *lavc\_def\_matrix* is the matrix name.
- *(1-12:)* defines a matrix that prevents ports from sending any traffic to other ports.
- *permanent* is the matrix status.

### Limit Multicast Messages for Cluster-3

The following commands limit the OpenVMS cluster multicast messages for a cluster (for example cluster-3) that only has members on a single floor.

```
set snmp myriad dec ema sysobjid bridges gigaswitch gigaversion1 gigabridge -
  filterByReferencedExpression -
  ebrNportDANameTable lavc3_filter -
  ebrNportDANameDA %Xab0004012103, -
  ebrNportDAMatrixName lavc_def_matrix, -
  ebrNportDANameDisp filter, -
  ebrNportDaNameStatus permanent
```

Where:

- *ebrNportDANameTable* refers to the destination address name table. An entry is created in this table.
- *lavc3\_filter* is the name of the filter.
- *ebrNportDANameDA* is the object that refers to a destination address being filtered.

## Example 2: Filters for Multiple OpenVMS Clusters

- *%Xab0004012103* is the multicast address for the hello messages for OpenVMS cluster members of cluster-3.
- *lavc\_def\_matrix* is the matrix created in the previous command sequence. This matrix will be applied to all messages that have the above DA.
- *filter* is the disposition.
- *permanent* is the status.

### Limit Multiple Port Messages

Next, limit multicast messages for LAVCs with nodes across multiple GIGAswitch FDDI ports (multiple rings). The following commands define the reachability matrix for cluster-1 and set the multicast (DA) filter:

```
set snmp myriad dec ema sysobjid bridges gigaswitch gigaversion1 gigabridge -
  filterByReferencedExpression -
  ebrNportMatrixNameTable lavc1_matrix -
  ebrNportMatrixValue (1,6,11:1,6,11), -
  ebrNportMatrixStatus permanent

set snmp myriad dec ema sysobjid bridges gigaswitch gigaversion1 gigabridge -
  filterByReferencedExpression -
  ebrNportDANameTable lavc3_filter -
  ebrNportDANameDA %xab0004012101, -
  ebrNportDAMatrixName lavc1_matrix, -
  ebrNportDANameDisp filter, -
  ebrNportDANameStatus permanent
```

#### Where:

- *lavc1\_filter* is the name of the filter.
- *(1,6,11:1,6,11)* allows all members of cluster-1 to connect with one another across rings and GIGAswitch FDDI ports.
- *%Xab0004012101* is the multicast address for LAVC1.
- *lavc1\_matrix* is the newly created filter matrix that will be applied to packets with the DA specified.
- *filter* is the matrix disposition.
- *permanent* is the matrix status.

These commands define a similar reachability matrix for cluster-2 and set the multicast (DA) filter:

```
set snmp myriad dec ema sysobjid bridges gigaswitch gigaversion1 gigabridge -
  filterByReferencedExpression -
  ebrNportMatrixNameTable lavc2_matrix -
  ebrNportMatrixValue (3,5:3,5), -
  ebrNportMatrixStatus permanent
```

```
set snmp myriad dec ema sysobjid bridges gigaswitch gigaversion1 gigabridge -
  filterByReferencedExpression -
  ebrNportDANameTable lavc3_filter -
  ebrNportDANameDA %xab0004012102, -
  ebrNportDAMatrixName lavc2_matrix, -
  ebrNportDANameDisp filter, -
  ebrNportDANameStatus permanent
```

## Protocol Type and SA Filters

The following filter specifications set up the reachability matrix for SCS protocol (the protocol used by OpenVMS clusters) packets so they remain local to each LAN. Create a filter that will block (or wall off) traffic between GIGAswitch FDDI ports, and then create exceptions to allow intracluster traffic to pass. This filter setup prevents the LAVC protocol from being transmitted out of the ring unless overridden.

This filter setup requires additional filters if you add new clusters that span multiple rings. Also, many filter commands are needed for the 16 nodes in cluster-1 and cluster-2. However, if nodes move from one port to another, you need only change the reachability matrix once to alter the filter setup to reflect the change.

## Set Up Filter Matrix

The first command sequence sets up a filter matrix that restricts all traffic to its own ring. The second command applies this filter matrix to all packets with the specified SNAP.

```
use default qualifier by password "08002b080666"

set snmp myriad dec ema sysobjid bridges gigaswitch gigaversion1 gigaBridge -
  filterByReferencedExpression -
  ebrNportMatrixNameTable lavc_def_matrix -
  ebrNportMatrixValue (1-12:), -
  ebrNportMatrixStatus permanent

set snmp myriad dec ema sysobjid bridges gigaswitch gigaversion1 gigaBridge -
  filterByReferencedExpression -
  ebrNportSnapNameTable lavc_protocol -
  ebrNportSnapNameSnap %0000006007, -
  ebrNportSnapMatrixName lavc_def_matrix, -
  ebrNportSnapNameDisp filter, -
  ebrNportSnapNameStatus permanent
```

### Where:

- *myriad* is the GIGAswitch FDDI System name.
- *dec ema sysobjid bridges gigaswitch gigaversion1 gigaBridge filterByReferencedExpression* specifies where the MIB objects are that will be used in the object tree.
- *lavc\_def\_matrix* is the matrix name.
- *(1-12:)* defines a matrix that prevents ports from sending any traffic to other ports.
- *lavc\_protocol* is the name of the SNAP table entry.

## Example 2: Filters for Multiple OpenVMS Clusters

- *%0000006007* defines the SNAP whose packets will be filtered using the *lavc\_def\_matrix* (this is the SCA SNAP).
- *filter* is the matrix disposition.
- *permanent* is the matrix status.

The following commands create SA alwaysForward filters that override the protocol type filters just created for cluster-1 and cluster-2. The port matrix, specified as the *ebrNportSAMatrixName*, has been previously set. One filter command needs to be entered for each of the 16 nodes.

```
set snmp myriad dec ema sysobjid bridges gigaswitch gigaversion1 gigaBridge -
  filterByReferencedExpression -
  ebrNportSANameTable ROCK_hw -
  ebrNportSANameSA %0800ab083163, -
  ebrNportSAMatrixName lavc1_matrix, -
  ebrNportSANameDisp alwaysForward, -
  ebrNportSANameStatus permanent
.
.
.
```

Where:

- *ROCK\_hw* is the table entry for node ROCK's hardware address filter.
- *%0800ab083163* is the hardware address (SA) where the filter will be applied.
- *lavc1\_matrix* is the matrix created earlier that allows ports 1, 6, and 11 (ports that have members of cluster-1 connected to them) to communicate with one another.

### Filter Specifications

You must create a filter for each node based on the hardware address. Filter specifications for cluster-1 specify all nodes in cluster-1 and their addresses. Filter specifications for cluster-2 specify all nodes in cluster-2 and their addresses. Use the *lavc2\_matrix* that was created earlier, allowing ports 3, 5, and 12 to communicate with one another, permitting the cluster-2 nodes on separate rings to communicate.

### DECnet Phase IV Filters

If a network is running DECnet Phase IV, or DECnet Phase V with Phase IV routing, you must create two filters per node. Enter an additional 16 filter commands as shown in the following commands. When the node initially appears on the network, it uses its network interface card hardware address, and when the DECnet protocol is in use, it switches to its DECnet address. The additional entry specifies the previous information by using the DECnet address.

```

set snmp myriad dec ema sysobjid bridges gigaswitch gigaversion1 gigaBridge -
  filterByReferencedExpression -
  ebrNportSANNameTable ROCK_DECnet -
  ebrNportSANNameSA %aa00ab35d143, -
  ebrNportSAMatrixName lavc1_matrix, -
  ebrNportSANNameDisp alwaysForward, -
  ebrNportSANNameStatus permanent
.
.
.

```

**Where:**

- *ROCK\_DECnet* is the table entry for node ROCK's hardware address filter.
- *%aa00ab35d143* is the DECnet address (SA) where the filter will be applied.
- *lavc1\_matrix* is the matrix created earlier that allows ports 1, 6, and 11 (ports that have members of LAVC1 connected to them) to communicate with one another.
- *alwaysForward* is the matrix disposition.
- *permanent* is the matrix status.

You must create a filter for each node based on its DECnet address. Filter specifications for LAVC1 specify all nodes in LAVC1 and their addresses. Filter specifications for LAVC2 specify all nodes in LAVC2 and their addresses, and use the *lavc2\_matrix* that was created earlier. This permits ports 3, 5, and 11 to communicate with one another, permitting the LAVC2 nodes on separate rings to communicate.



---

## LEDs of Logic and Power Modules

This appendix describes the LEDs of the logic and power modules:

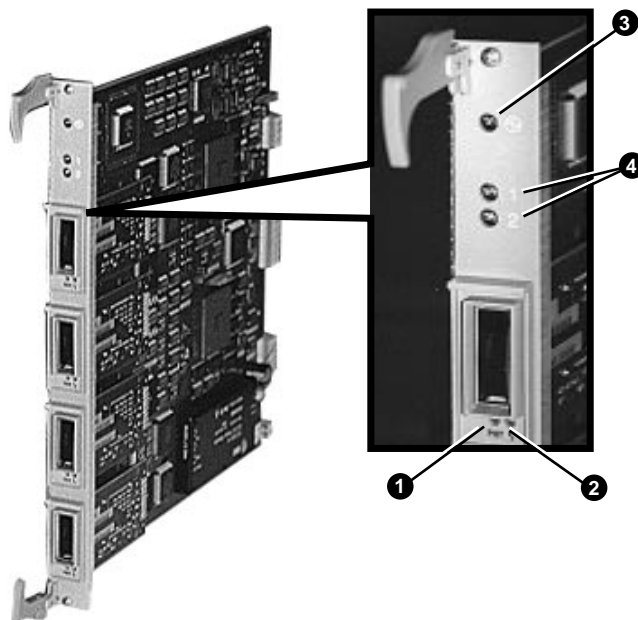
- Logic modules
  - Linecards
  - SCP card
  - Clock card
  - CBS card
- Power modules
  - Fan tray
  - ACFEU
  - DCFEU
  - PSA (security switch)

## Linecard LEDs

All GIGAswitch/FDDI System linecards have a module LED and two or four port LEDs. The following figure identifies the location of each LED. Table B-1 and Table B-2 describes the functions of each LED.

**Table B-1 Meaning of Module LEDs**

State	Module ③ LED	Port ④ LED
<b>Off</b>	No power	No power
<b>Green Steady</b>	Module self-test (MST) passed	Port active in forwarding state
<b>Green Flashing</b>	Firmware downline load in progress	Port not in forwarding state
<b>Amber Steady</b>	MST failed or fatal firmware error	MST failure on this port
<b>Amber Flashing</b>	MST in progress	MST in progress
<b>Alternate Green/Amber</b>	<u>Nonfatal</u> error logged within last 10 minutes	–



mk28108



**PMD LEDs** Each PMD on the FGL-2 and FGL-4 FDDI linecards has two LEDs. Table B-2 describes the functions of PMD LEDs.

**Table B-2 Meaning of PMD LEDs**

<b>State</b>	<b>PHY ① Status LED <sup>1</sup> (Left)</b>	<b>Port ② Type LED <sup>2</sup> (Right)</b>
<b>Off</b>	Ready to connect	M-Type
<b>Green Steady</b>	Connection accepted	S-Type
<b>Green Flashing</b>	Broken or disabled	A/B Type
<b>Amber Steady</b>	Link confidence test failure	PMD loop test failed
<b>Amber Flashing</b>	Topology reject	–
<b>Alternate Green/Amber</b>	Dual homing standby	–

<sup>1</sup>Formerly called PMD PHY LED

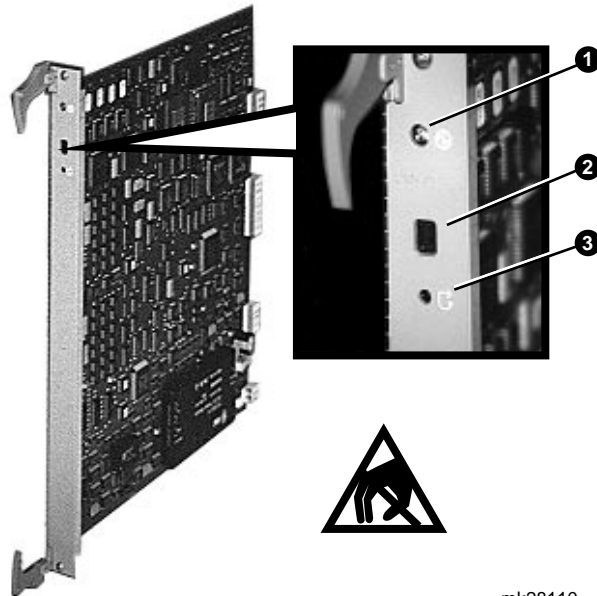
<sup>2</sup>Formerly called PMD FRU LED

**AGL-2 LEDs** The LEDs on the AGL-2 MOD PHY ports are described in the GIGAswitch/FDDI System AGL-2 Manager's Reference Guide.

---

## SCP Card LEDs

The switch control processor (SCP) has a single module LED near the top of the module and a HEX display below it. There is also a Reset push button on the SCP. Pressing it causes the SCP to reinitialize. In the case of the elected SCP it also causes all linecards to be reinitialized in turn.



mk28110

Number	Function
❶ Module LED (Amber/green)	Indicates power available and MST status
❷ Diagnostic Readout (Hexadecimal LED)	Indicates coded diagnostic results, and operational state
❸ Reset (push button)	Resets the SCP

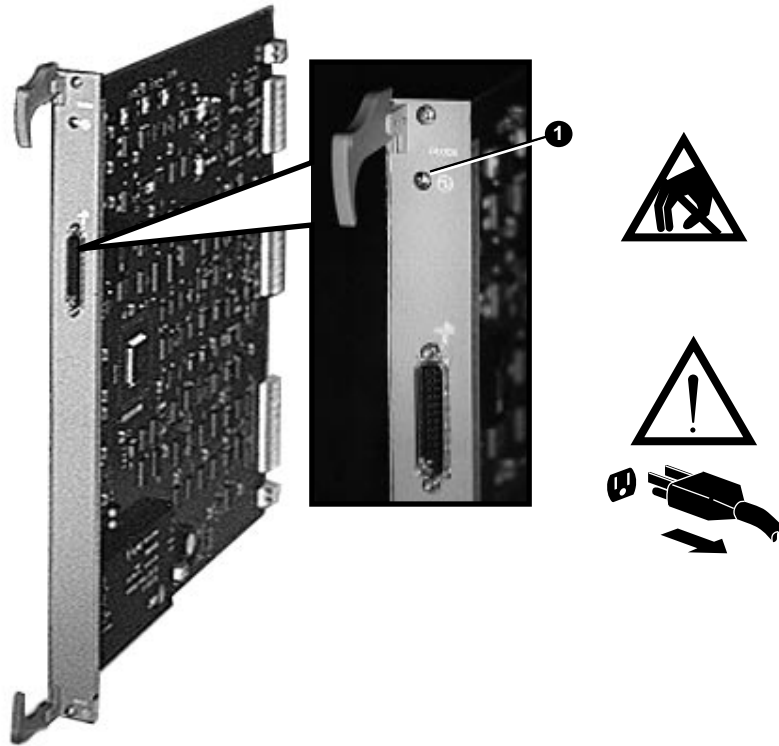
Table B-3 further identifies the purpose of the SCP LEDs and the HEX display.

**Table B-3 Meaning of SCP Indicators**

<b>SCP LED ① State</b>	<b>HEX ② Display</b>	<b>Meaning</b>
<b>Green</b>	E	Elected SCP—operational
	B	Backup SCP—operational
	D	Firmware copy in progress
	D/E (alternating)	Corrupted image found; performing emergency download, if possible
<b>Amber</b>	Out	Module self-test failed
	F	Startup complete
<b>Amber Flashing</b>		Module self-test in progress; HEX display indicates test in progress

## CLK Card LED

The Clock Card (CLK) has a single LED near the top of the module. It reflects the state of the module as described in the Table B-4.



MK28132

Table B-4 Meaning of CLK LED

CLK LED ① State	Meaning
<b>Amber</b>	Running bootblock diagnostics
<b>Amber Patterned Flashing</b>	Bootblock diagnostic or unexpected interrupt failure—identified by pattern of flashes
<b>Amber Flashing</b>	Module diagnostic failure
<b>Green</b>	Bootblock diagnostics passed; diagnostic or operational code is running

---

## CBS Card LED

The crossbar switch (CBS) has a single LED. Table B-5 describes this LED.

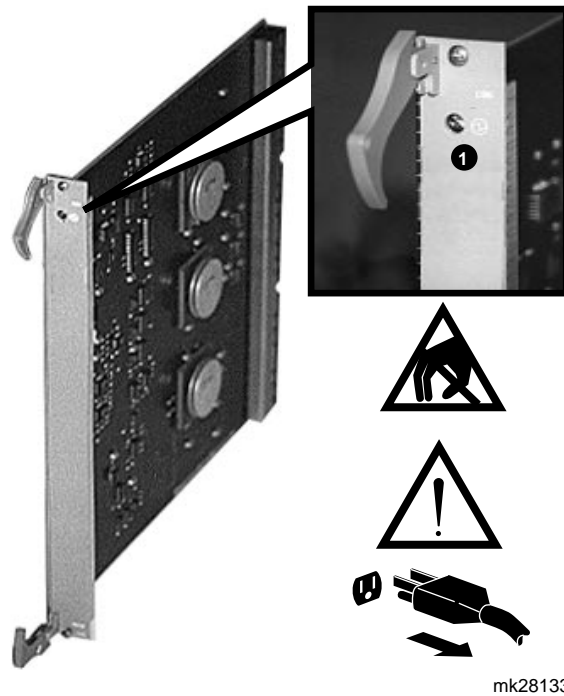


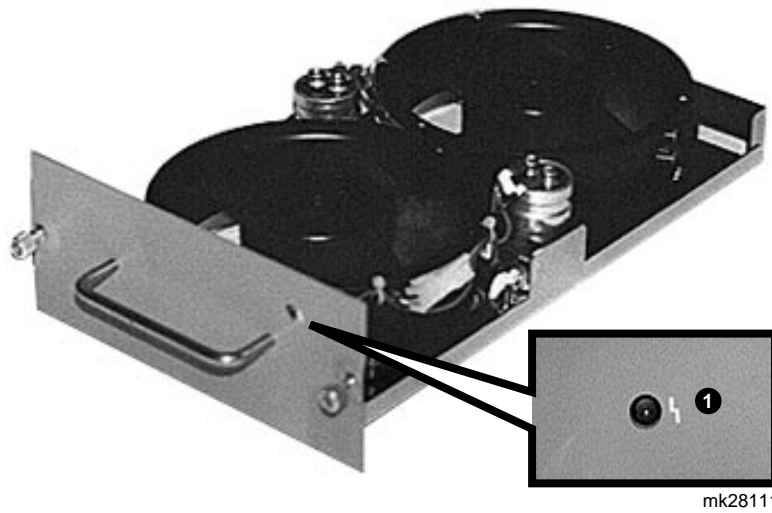
Table B-5 Meaning of CBS LED

CBS LED ① State	Meaning
Green	Test passed
Amber	Test failed

---

## Fan Tray Assembly LED

The fan tray assembly has a single LED. Table B-6 describes this LED.



**Table B-6** Meaning of Fan Tray Assembly LED

---

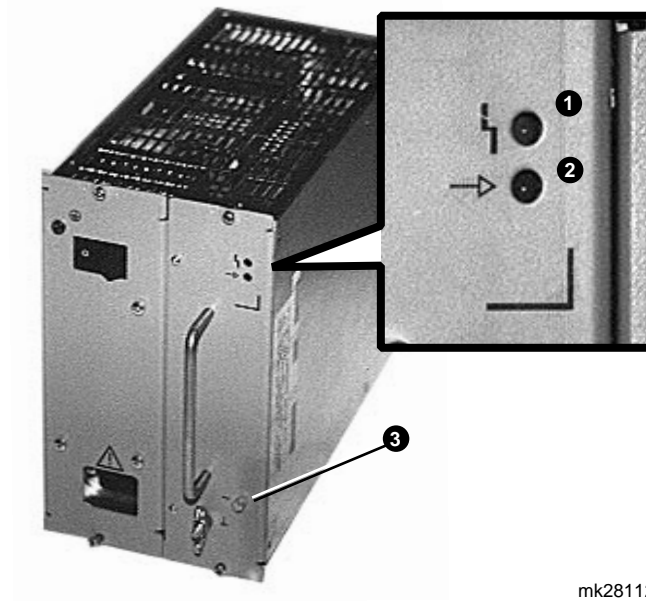
Fan Tray Fault ⓘ	
State	Meaning
Off	MST passed
Amber	MST failure

---

---

## ACFEU LEDs

The ACFEU has three LEDs. Table B-7 describes these LEDs.



mk28112

**Table B-7 Meaning of ACFEU LEDs**

Number/Name	Condition
①/ACFEU	Amber Steady—MST failure
②/ACFEU OK	Green On—MST passed
③/AC Power	Off—Power is NOT available for FEU circuit breaker On—Power is available for ACFEU circuit breaker

### 48V DCFEU LEDs

The 48 Vdc Power Interface Unit has three LEDs which are located in the same place as in the ACFEU above. Table B-8 describes each LED.

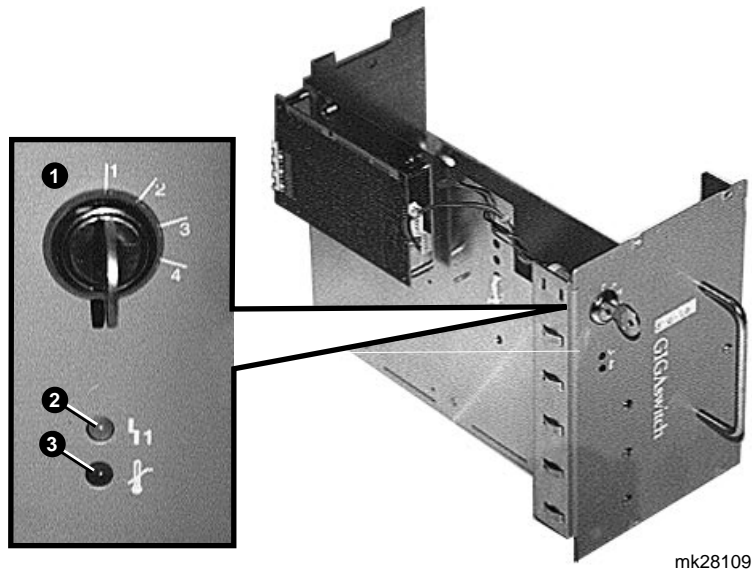
**Table B-8 Meaning of 48 Vdc LEDs**

Number/Name	Condition
①/DCFPU	Amber Steady—MST failure
②/DCFPU OK	Green On—MST passed
③/DC Power	Off—Power is NOT available for DCFPU circuit breaker On—Power is available for DCFPU circuit breaker

---

## PSA LEDs

The PSA has a keyswitch and two LEDs. Table B-9 describes these LEDs.



mk28109

**Table B-9 Meaning of Security Keyswitch LEDs**

Number/Name	Condition
②/PSC card Fault	Off—MST passed
	Amber Steady —MST failure
③/System temperature fault	Red Steady—System temperature fault
	Off—System temperature normal

Refer to Chapter 2, Table 2-2 for a description of the security keyswitch settings.



---

## **GIGAswitch/FDDI System Specifications**

This appendix provides the specifications for the GIGAswitch/FDDI System. These specifications include:

- Physical specifications for the GIGAswitch/FDDI System.
- Electrical specifications for the GIGAswitch/FDDI System.
- Environmental specifications for the GIGAswitch/FDDI System.

---

## Physical Dimensions of the GIGAswitch/FDDI System

The following table shows the physical specifications for the GIGAswitch/FDDI System. Allow 90.0 cm (35.4 in) contiguous vertical space for the installation of the GIGAswitch/FDDI System, the lower plenum, and the upper plenum. (Physical Specifications)

Parameter	Min	Typ	Max	Units	Symbol
Mounting type		Rack Mounted		–	–
Height	–	896.2	–	millimeters	mm
	–	35.25	–	inches	in
Width	–	507	–	millimeters	mm
	–	19.95	–	inches	in
Depth	–	495	–	millimeters	mm
	–	19.50	–	inches	in
Weight	–	87.1	–	kilograms	kg
	–	192	–	pounds	lb
Operation clearance (front)	51	–	–	millimeters	mm
	2.0	–	–	inches	in
Operation clearance (rear)	76	–	–	millimeters	mm
	3.0	–	–	inches	in
Operation clearance (side)	0	–	–	millimeters	mm
	0	–	–	inches	in
Service clearance (front)	914	–	–	millimeters	mm
	36.0	–	–	inches	in
Service clearance (rear)	914	–	–	millimeters	mm
	36.0	–	–	inches	in
Service clearance (side)	0	–	–	millimeters	mm
	0	–	–	inches	in
Service clearance (top)	0	–	–	millimeters	mm
	0	–	–	inches	in
Shipping height <sup>1</sup>	–	1283	–	millimeters	mm
	–	50.5	–	inches	in
Shipping width <sup>1</sup>	–	–	–	millimeters	mm
	–	26.0	–	inches	in
Shipping depth <sup>1</sup>	–	–	–	millimeters	mm
	–	32.0	–	inches	in
Shipping weight <sup>1</sup>	–	99.8	120	kilograms	kg
	–	220	264	pounds	lbs

---

<sup>1</sup>Shipping for standard shipping container

---

## Electrical Information

**AC Input Power Requirements**      The following table shows the ac input power requirements for the GIGAswitch/FDDI System.

Parameter	Min	Typ	Max	Units	Symbol
Nominal Voltage	–	120	–	volts	V
Operational Voltage Range	93	–	264	volts	V
Nominal Frequency	–	50/60	–	hertz	Hz
Frequency Range	47	–	63	hertz	Hz
Number of Phases	–	1	–	none	NA
120V Single Phase Input Current (Steady State)	–	8.0	15	amperes	A
120V Single Phase Input Current (Neutral N)	–	4.0	7.5	amperes	A
120V Single Phase Input Current (Ground G)	–	1.0	–	milliamperes	mA
240V Single Phase Input Current (Steady State)	–	4.0	7.5	amperes	A
240V Single Phase Input Current (Neutral N)	–	4.0	7.5	amperes	A
240V Single Phase Input Current (Ground G)	–	1.0	–	milliamperes	mA
Ride-Through Time	100	–	–	milliseconds	ms
Inrush Current	–	–	n/a	amperes peak	A
Start-Up Current	–	–	n/a	rms amperes	A
Start-Up Current Duration	–	–	n/a	seconds	s
Power Consumption	–	800	1250	watts	W
Apparent Power	–	1052	1316	volt amperes	VA
Power Factor	–	.95	–	none	PF
Crest Factor	–	1.37	–	none	CF

**Power Cord Types**      The following table lists the power cords used in the various country kits available with the GIGAswitch/FDDI System.

Country	Part Number	Country	Part Number
Denmark	BN16A-2E	Israel	BN18W-2E
UK/Ireland	BN12A-2E	Central Europe	BN13A-2E
Italy	BN17A-2E	Australia	BN22C-2E
Switzerland	BN14A-2E	New Zealand	BN22C-2E

Line cords are 2.5 meters in length. Use different outlets and services breakers for redundant power supplies.)

## Electrical Information

The following table shows the DC power requirements for the GIGAswitch/FDDI System.

Parameter	Min	Typ	Max	Units	Symbol
Power Consumption	–	640	1000	watts	W
Current at 48 Vdc	–	12	20	amperes	A
Current at 12-26 Vdc	—	3.6	5.0	amperes	A
DC voltage range (48 Vdc)	46.32	–	49.68	volts	Vdc
DC voltage range (12Vdc - 26 Vdc)	11.0	–	27.1	volts	Vdc
Output Watts Available	–	–	1000	watts	W
Current available at 48 Vdc	–	–	22.	amperes	A
Current available at 11-27.1 Vdc	—	–	1.5-5.0	amperes	A

## Environmental Information

Parameter	Min	Typ	Max	Units	Symbol
Temperature (Operating)	10	–	35	degrees Celsius	°C
	50	–	95	degrees Fahrenheit	°F
Altitude derating	–	1.8	–	degrees Celsius per kilometer	°C/km
	–	1.0	–	degrees Fahrenheit per 1000 feet	°F/1000 ft
Temperature (Nonoperating)	-40	–	66	degrees Celsius	°C
	-40	–	151	degrees Fahrenheit	°F
Temperature (Storage)	-40	–	66	degrees Celsius	°C
	-40	–	151	degrees Fahrenheit	°F
Relative Humidity (Operating)	10	–	90	percent relative humidity (noncondensing)	%RH
Relative Humidity (Nonoperating)	<50	–	95	percent relative humidity (noncondensing)	%RH
Relative Humidity (Storage)	<50	–	95	percent relative humidity (noncondensing)	%RH
Maximum Wet Bulb Temperature (Operating)	–	–	25	degrees Celsius	°C
	–	–	77	degrees Fahrenheit	°F
Maximum Wet Bulb Temperature (Storage)	–	–	146	degrees Celsius	°C
	–	–	115	degrees Fahrenheit	°F
Minimum Dew Point Temperature (Operating)	2	–	–	degrees Celsius	°C
	36	–	–	degrees Fahrenheit	°F
Heat Dissipation	–	800	1250	watts	W
	–	2730	4265	Btu/hr	Btu/hr
Altitude (Operating)	–	–	2400	meters above sea level	m
	–	–	8000	feet above sea level	ft
Altitude (Nonoperating)	–	–	4900	meters above sea level	m
	–	–	16000	feet above sea level	ft
Mechanical Shock (Operating)		Duration	10+3	milliseconds	ms
		Level	10g	gravities	G
Vibration Freq Range (Operating)	5	–	500	hertz	Hz
Vibration Level (Operating)	.010- in DB	.25g	peak		
Mechanical Shock (Nonoperating)		Duration	29.2	milliseconds	ms
		Level	13.67	gravities	G
Vibration Freq Range (Nonoperating)	10	–	300	hertz	Hz
Vibration Level (Nonoperating)	1.40g	–	.029	g <sup>2</sup> /hz	
Acoustic Emission (Operating)	–	–	–	Bels	B

Parameter	Min	Typ	Max	Units	Symbol
Acoustic Emission (LNPE)	–	5.9	–	decibels	dBA
Acoustic Emission (LPA)	–	46	–	decibels	dBA
Acoustic Emission (Idle /Standby)	–		–	Bels	B
Acoustic Emission (LNPE)	–	5.9	–	decibels	dBA
Acoustic Emission (LPA)	–	46	–	decibels	dBA
Airflow Intake Location			Top-Front		
Airflow Exhaust Location			Bottom Rear		

**Ventilation**

The GIGAswitch/FDDI System cooling system is designed to be tolerant of various rack installation configurations. However, to provide adequate ventilation:

- Do not block off the inlet air vents (upper grilles).
- Do not block off the outlet air vents (lower grilles).
- Do not allow the cooling air entering the GIGAswitch/FDDI System to rise above 32°C (90°F).

**EMI Susceptibility**

The following table shows the electromagnetic interference (EMI) susceptibility for the GIGAswitch/FDDI System.

Parameter		Maximum	Units	Symbol
Broadband Conducted EMI	Class A	Composite (FCC/VDE)	Volts dbuv	dbuv
Narrowband Conducted Transients	Frequency Range	10KHZ to 30MHZ	kilohertz, megahertz	kHz, MHz
	V rms into 50 ohms	3VRMS	Volts	V
Narrowband Radiated Susceptibility	Frequency Range	.01MHZ-1GHZ	kilohertz, megahertz	kHz, MHz
	Level	5 Volts/M	Volts per Meter	V/m
ESD Control		15KV	kilovolts	kV

---

# Glossary of GIGAswitch/FDDI System Terms

## **Address Resolution Protocol**

*See ARP.*

## **agent**

In the client-server model, the part of the system that prepares and exchanges information on behalf of a client or server application.

## **alarm**

A message sent to operator terminals that are enabled or defined by management software. Alarms are set using the network management station (NMS). *See also NMS.*

## **American National Standards Institute**

*See ANSI.*

## **ANSI**

American National Standards Institute. A national standards organization with members from computer manufacturers and users in the United States. It is the U.S. member body of ISO and is involved with the development of standards around the OSI Reference Model. ANSI proposes, compiles, and publishes standards for programming languages, databases, telecommunications, and other products.

## **ARP**

Address Resolution Protocol. A protocol that maps a high-level Internet address with a low-level physical hardware address. Limited to networks that support hardware broadcast.

## **backup**

A network device or circuit that is used if the primary device or circuit becomes unavailable. The spanning tree algorithm can put bridges or network branches in backup mode if they are redundant with others and might create loops in the network. *See also spanning tree.*

## **BOOTP**

Boot protocol. A protocol that determines a diskless host Internet address at startup, so that the host can operate in an Internet network. *See also protocol.*

**BPDU**

An IEEE 802.1d Bridge Protocol Data Unit.

**broadcast**

Simultaneous transmission of data to more than one destination in a network, so that all broadcast addresses receive the same message.

**CBS**

Crossbar switch. The switching module that forms the heart of the GIGAswitch/FDDI System.

**community string**

SNMP password for primitive security. *See also SNMP.*

**crossbar switch**

*See CBS.*

**cutthrough**

A process that enables the GIGAswitch/FDDI System to start forwarding a packet out of a port before the entire packet is received. Inbound cutthrough begins packet transmission through the crossbar switch before it is fully received from the inbound port. Outbound cutthrough begins packet transmission on the outbound port before it is fully received from the crossbar switch.

**DA**

Destination Address. A unique network address identifying a target system. For filter purposes, this is the 48-bit MAC address. Packets are filtered based on the destination address of the packet.

**destination address**

*See DA.*

**DAS**

Dual Attachment Station. An FDDI station that offers two connections to the dual counter-rotating ring. *See also FDDI.*

**dotted decimal notation**

The representation for a 32-bit integer that consists of four 8-bit numbers written in base 10 with decimals separating them. This is used to represent IP addresses on the Internet.

**dual attachment station**

*See DAS.*

**dual homing**

An FDDI method of cabling concentrators and stations that enables an alternate or backup path to the ring if the primary connection fails. *See also FDDI.*



**FEU**

Front-end unit. Power supply for the GIGAswitch/FDDI System.

**FDDI**

Fiber Distributed Data Interface. A set of ANSI/ISO standards that define a high-bandwidth (100 megabits per second) general-purpose LAN connection between computers and peripheral equipment in a timed-token passing, dual ring of trees configuration.

**Fiber Distributed Data Interface**

*See FDDI.*

**FGL-2**

Fiber GIGAswitch/FDDI System Linecard, 2-port.

**FGL-4**

Fiber GIGAswitch/FDDI System Linecard, 4-port. Can configure only as a single attachment station, it cannot be configured as a dual attachment station.

**filtering**

The process where a bridge evaluates incoming messages and selects those it needs to process and those it blocks from delivery. Filters can be set using management station commands.

**forwarding**

The ability of a bridge or router to accept messages from one local area network (LAN) segment and retransmit those messages to another LAN segment. *See also LAN.*

**frame**

A data transmission unit containing data or control information, address information, and a frame check sequence.

**front-end unit**

*See FEU.*

**full-duplex**

Pertaining to a type of data communications system capable of providing simultaneous, independent transmission and reception in both directions.

**get**

An SNMP request for data command. *See also SNMP.*

**get-next**

An SNMP command that gets the next data item in the MIB object tree. *See also SNMP, MIB.*

**hotswap**

The ability to remove and insert a component without powering down the GIGAswitch/FDDI System. This procedure does not interrupt normal operation.

**in-band management**

A technique for carrying control signals within the same bandwidth as data being carried. In-band management for the GIGAswitch/FDDI System is performed using a network management station (NMS). *See also NMS.*

**Internal Protocol**

*See IP.*

**IP**

Internet Protocol. The network layer protocol for the Internet protocol suite that provides the basis for the connectionless, best-effort packet delivery service. IP includes the Internet Control Message Protocol (ICMP) as an integral part. The Internet protocol suite is referred to as TCP/IP because IP is one of the two most fundamental protocols.

**LAN**

Local area network. A self-contained group of computers and communications devices (such as modems, routers, servers, and repeaters) that offer a high-speed, reliable communications channel. LANs span a limited distance, such as a building or cluster of buildings, but can be connected to wide area networks (WANs) with bridges or routers.

**learning**

The process by which a bridge discovers and remembers which ports network devices are connected to.

**local area network**

*See LAN.*

**Maintenance Operation Protocol**

*See MOP.*

**Management Information Base**

*See MIB.*

**Management Station for UNIX**

*See MSU.*

**MIB**

Management Information Base. A collection of objects that can be accessed with a network management protocol.

**MMF**

Multi mode fiber. Used in FDDI networks to support network station connections up to 2 kilometers

**MOP**

Maintenance Operations Protocol. A network management protocol within DECnet software that handles tasks such as downline loading, upline dumping, and circuit testing.

**multicast**

A special form of broadcast transmission where copies of the packet are only delivered to a subset of all destinations.

**network management station**

*See NMS.*

**NMS**

Network management station. The system responsible for managing a network. The NMS talks to network management agents, which reside in the managed nodes, using a network management protocol (such as SNMP). *See also SNMP.*

**OBM**

Out-of-band management. In network management, a technique for carrying control signals over a separate channel rather than within the main signal bandwidth. Out-of-band management for the GIGAswitch/FDDI System is performed with a local terminal connected directly to the system with an RS-232 cable.

**out-of-band management**

*See OBM.*

**PDU**

Protocol data unit. The data units (messages or blocks of data) passed between peer entities on different open systems. PDUs consist of both Protocol Control Information (PCI) and user data.

**Physical media device**

*See PMD.*

**PAID**

Process identification. A binary value that uniquely identifies a process. Each process has a process identification and a process name.

**PID**

Protocol ID (*not process ID*).

**PM**

Presentation module. An interaction method for use with DECmcc.

**PMD**

Physical layer media dependent. The GIGAswitch/FDDI System supports two types of PMDs: multimode fiber and single mode fiber.

**POLYCENTER**

POLYCENTER network management software monitors, controls, and tests entities in the DECnet, DECnet/OSI, and multivendor distributed environment. The GIGAswitch/FDDI System can be managed by the POLYCENTER Network Manager (formerly DECmcc) with the SNMP access module, or by the POLYCENTER SNMP Manager (formerly DECmcc Management Station for ULTRIX). *See also SNMP.*

**port**

An individual connector on the GIGAswitch/FDDI System that connects a LAN to the GIGAswitch/FDDI System. *See also LAN.*

**presentation Module**

*See PM.*

**privileged port**

A port that can perform SNMP set operations on a secure GIGAswitch/FDDI System. Privileged ports are defined by network management. *See also SNMP.*

**process identification**

*See PI.*

**protocol**

A set of rules for the implementation of a network communication system. Protocols cover options such as signaling methods, coding, packaging of messages, and methods of preventing and correcting errors.

**protocol data unit**

*See PDU.*

**PSA**

Power system assembly.

**PSC**

Power system controller.

**rate limiting**

Limits imposed on multicast traffic and traffic with unknown destination addresses (DAs). This reduces the risk of overloading ports with traffic. *See also DA.*

**SA**

Source address. The unique network address indicating the originator of a message.

**Simple Network Managing Protocol**

*See SNMP.*

**SAP**

Service access point. The point at which an entity provides a service to a user entity in the layer above it. The SAP is named according to the layer providing the services (transport services are provided at a transport SAP, or TSAP, at the top of the transport layer).

**SAS**

Single attachment station. An FDDI station that offers one S port for attachment to the FDDI ring, usually via a concentrator. *See also FDDI.*

**SCP**

Switch control processor.

**service access point**

*See SAP.*

**SET**

An SNMP command that can set (alter) an SNMP object. *See also SNMP.*

**single attachment station**

*See SAS.*

**slot**

A groove where a module or card can be installed.

**SMF**

Single Mode Fiber. Used in FDDI networks to support network station connections up to 40k.

**SNAP**

Subnetwork Access Protocol. Used in protocol ID PID filtering. *See also PID.*

**SNMP**

Simple network management protocol. A protocol for monitoring and controlling hosts, bridges, routers, and terminal servers on TCP/IP networks with network management applications, such as DECmcc.

**source address**

*See SA.*

**spanning tree**

The logical arrangement created by bridges in an extended LAN in which all LANs are connected and there are no loops. *See also LAN.*

**Subnet mask**

Address mask. A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the IP address and one or more bits of the local portion.

**TFTP**

Trivial file transfer protocol. An Internet facility for transferring electronic files in a TCP/IP environment. TFTP allows authorized users to transfer files over the network.

**transparent bridging**

The IEEE 802.1d bridging scheme used to interconnect LANs based upon a spanning tree algorithm. The bridge provides all necessary functionality, including address learning and address filtering. Transparent bridging is protocol independent, performs automatic learning and forwarding, and ensures a loop-free topology in a large network, as only one active bridge connects any two LANs. *See also LAN, learning, spanning tree.*

**trap**

An unsolicited SNMP message sent by an SNMP manageable device to one or more network management stations (NMS). *See also NMS, SNMP.*

**Trivial File Transfer Protocol**

*See TFTP.*

**WAN**

Wide area network. Two or more standard or extended LANs that are joined by routers, gateways, or packet-switched interface (PST) software.

**Wide Area Network**

*See WAN.*

**UTP**

Unshielded twisted pair. Used in networks to support network station connections up to 100 meters.

---

# Index

- 2-port FDDI line card (54-22122-01)
  - function of, 1-5
  - location of (*fig*), 1-5
- 2-port FDDI line card (54-22122-01) (*fig*), B-2

## B

---

- Backup Front end unit (FEU) (H7884-AB)
  - function of, 1-8
  - location of (*fig*), 1-7
- Bootptab
  - example of an /etc/bootptab file, 3-19
- Bootsrver
  - setup for DECnet-VAX MOP, 3-18
  - setup for BOOTP, 3-19
  - setup for ULTRIX MOP, 3-19
  - to assist with corrupt SCP code, 3-18

## C

---

- Cables
  - connecting to ports, 2-8
  - installing multimode cables, 2-9
  - installing single-mode cables, 2-8
  - installing unshielded twisted pair cables, 2-8
- Clock card (54-22120-01)
  - description of, B-6
  - evaluating LEDs on (*table*), B-6, B-7
  - function of, 1-5
  - location of (*fig*), 1-5
  - part number, B-6
- Clock card (54-22120-01) (*fig*), B-6
- Connector, terminal
  - See OBM port
- Console port
  - See OBM port
- Cooling and Power Modules, B-8
- Cooling modules
  - functions of, 1-8
- Cooling modules (*fig*), 1-7
- Crossbar switch (CBS) card (54-22116-01)
  - description of, B-7
  - evaluating LEDs on (*table*), B-6, B-7
  - function of, 1-5
  - location of (*fig*), 1-5

- Crossbar switch (CBS) card (54-22116-01)
  - (cont'd)
  - part number, B-7
- Crossbar switch (CBS) card (54-22116-01) (*fig*), B-7

## D

---

- DECndu Plus
  - description of, 3-11
  - ordering information, 3-11
- Dispositions
  - always filter, 4-9

## F

---

- Fan tray assembly (70-30578-01)
  - evaluating LEDs (*table*), B-8
  - function of, 1-8
  - location of (*fig*), 1-7
  - status LED, B-8
- Fan tray assembly (70-30578-01) (*fig*), B-8
- Filtering
  - and broadcast, 4-11
  - and multicast, 4-11
  - basics, 4-2
  - creating SA, DA and PID filters, 4-8
  - disposition, 4-9
  - for multiple sites, 4-13
  - lock down, 4-16
  - manual mode, 4-16
  - port pattern example, 4-5
  - port pattern matrices, 4-4
  - securing a load server, 4-15
  - setup procedures, 4-4
  - specifying the matrix, 4-6
  - to isolate traffic, 4-12
  - types of, 4-16
- Filters
  - downline loading example, A-2
  - examples of, A-1
  - local area VMS cluster example, A-5
  - multicast address example, A-7
  - protocol example, A-9
- Firmware upgrades
  - copying the file, 3-4
  - file extensions, 3-6
  - file loading indications, 3-2

Firmware upgrades (cont'd)  
file verification, 3-2  
image installation, 3-9  
image transfer, 3-6  
MOP transfer, 3-7  
strategy, 3-17  
TFTP firmware upgrade objects, 3-6  
TFTP transfer, 3-6  
Front end unit (FEU) (H7884-AB)  
function of, 1-8  
location of (*fig*), 1-7  
Function of  
security switch positions, B-10

---

## G

GIGAswitch/FDDI System  
electrical, C-3  
environment, C-5  
physical dimensions, C-2  
sections of, 1-4  
specifications, C-1  
temperature status LED, B-10  
ventilation, C-6

---

## H

Hotswap  
modules eligible for, 1-9

---

## I

Input power connector, 1-8  
Input power switch, 1-8

---

## K

Key operated switch  
*See* Security switch

---

## L

Lock down filtering, 4-16  
Logic module  
Clock card (54-22120-01), B-6  
crossbar switch (CBS) card (54-22116-01),  
B-7  
Logic modules, B-1  
functions of, 1-5  
slot restrictions, 1-5  
Logic modules (*fig*), 1-5  
Logic modules linecards  
types of, 1-5

---

## M

Manual mode filtering, 4-16  
Modules, logic (*fig*), 1-5  
Multicast traffic  
filtering and, 4-2

---

## N

Network troubleshooting  
filtering and, 4-2

---

## O

OBM  
guidelines, 2-3  
OBM port  
access control, B-10  
password requirements, B-10  
OBM terminal  
access control, 1-14  
connecting, 2-3  
connecting (*Fig*), 2-3  
Out-of-band management connector  
*See* OBM port  
Out-of-band terminal  
*see* OBM terminal

---

## P

Packets  
filtering and, 4-9  
Part number  
Clock card (54-22120-01), B-6  
crossbar switch (CBS) card (54-22116-01),  
B-7  
PMD  
types of PMDs, 2-8  
Ports  
connecting cables, 2-8  
filtering and, 4-9  
manual mode, 4-16  
Power modules, B-1  
functions of, 1-8  
Power Status Assembly (PSA) (70-30585-01)  
location of (*fig*), 1-7  
Power Status Assembly (PSA) (70-30585-01)  
(*fig*), B-10  
Power System Controller (PSC)  
evaluating LEDs (*table*), B-10  
LED interpretation (*fig*), B-10  
Power system controller (PSC) card  
(54-22132-01)  
function of, 1-5, 1-8  
PSC  
location of LEDs, B-10  
meaning of LEDs, B-10



## R

---

### Requirements

- electrical, C-3
- environmental, C-5
- physical dimensions, C-2

## S

---

### SCP

- loading, 3-17

### Security

- filtering and, 4-2

### Security keyswitch, 1-14

- (fig)*, 2-6
- OBM access and, 2-4
- positions, 2-7

### Security switch

- use of, B-10

### Serial port

- See* OBM port

## Specifications

- electrical, C-3
  - environmental, C-5
  - physical dimensions, C-2
- ### Switch control processor (SCP) card (54-22118-01)
- evaluating LEDs on *(table)*, B-4
  - function of, 1-5
  - location of *(fig)*, 1-5
- ### Switch control processor (SCP) card (54-22118-01) *(fig)*, B-4

## T

---

### Temperature, system

- status LED, B-10

### Terminal

- connecting, 2-3

### Traffic

- filtering of, 4-2

## V

---

- Ventilation, C-6

