

DEChub Network Modules

900-Series Switch Reference

Order Number: EK-SWTCH-HR. A01

February 1996

This manual describes the functions and features of Digital's HUB-based 900-Series switching products.

The switch products include the following network modules: the DECswitch 900EE, the DECswitch 900EF, and the PEswitch 900TX.

February 1996

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

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

© Digital Equipment Corporation 1996. All rights reserved.

The following are trademarks of Digital Equipment Corporation: DECconcentrator, DEChub, DECndu, DECswitch, Digital, HUBwatch, PEswitch, and the DIGITAL logo.

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

Contents

Preface

1 LAN Switches

Overview	1-1
What is a LAN Switch?.....	1-2
Switching at Different Levels in the Organization.....	1-3
LAN Switching Technology	1-5

2 900-Series Switches

Overview	2-1
900-Series Switch Products	2-2
DECswitch 900EE Module	2-5
DECswitch 900EF Module.....	2-10
PEswitch 900TX Module.....	2-16

3 Features and Functionality

Overview	3-1
Frame Formats	3-2
AppleTalk Translation.....	3-10
Rate Limiting.....	3-14
Frame Filtering/Forwarding	3-15

Managing Switches with HUBwatch.....	3-19
Out-of-Band Management (OBM)	3-23

4 Managing the 900-Series Switches

Overview	4-1
Switch-Specific HUBwatch Windows	4-3
Switch Summary Window.....	4-7
Enabling and Disabling Forwarding on Ports.....	4-9
Enabling and Disabling the Spanning Tree Algorithm on Ports	4-10
Setting LB100 Compatibility	4-12
Enabling and Disabling Raw 802.3 IPX Translation	4-14
Enabling and Disabling IP Fragmentation	4-16
Enabling and Disabling Rate Limiting.....	4-18
Setting the Rate Limit	4-21
Setting the Bridge Hello Time	4-24
Setting the Bridge Max Age.....	4-27
Setting the Bridge Forward Delay.....	4-30
Setting the No Frame Interval	4-33
Setting the Aging Time.....	4-34
Setting the Short Aging Time.....	4-36
Setting the Gateway Address	4-38
Adding and Deleting Trap Addresses.....	4-40
Creating Address Filters.....	4-43
Modifying Address Filters.....	4-47
Creating a Default Filter for All Unspecified Addresses.....	4-53
Creating Protocol Filters.....	4-55
Modifying Protocol Filters	4-58
Specifying Default Protocol Filters.....	4-64
Adding Protocols not in the Available Protocols List	4-66

Deleting Address and Protocol Filters.....	4-69
Writing Contents of Forwarding and Filter Databases to Files.....	4-72

5 FDDI Configuration Capabilities

Overview	5-1
Dual Ring Configurations.....	5-3
Tree Configurations.....	5-4
DECconcentrator 900MX.....	5-6
DECconcentrator 900TH	5-7
DECconcentrator 900FH	5-8
DECswitch 900EF.....	5-9
PEswitch 900TX.....	5-10
Configuration Guidelines and Rules	5-11
FDDI in the Hub Backplane.....	5-13
Default Configurations	5-16
FDDI Tree Configuration Examples	5-19
Dual Ring Configuration Examples.....	5-30
Fault Tolerance in Dual Rings	5-37
Fault Tolerance in Trees.....	5-39
Token Ordering of Trees or Dual Rings	5-41
Quick PC Trace Option for Concentrators	5-46
Summary of Important Configuration Features	5-47

A FDDI Overview

Overview	A-1
The Dual Ring.....	A-3
Station Types	A-4
Media Types and Maximum Distances	A-6
Station Configurations.....	A-7

Physical Topologies	A-9
Station States	A-12
FDDI Connection Rules	A-14
Ring Operation.....	A-18

B Accessing MIBs and RFCs

Overview	B-1
Accessing Online Information.....	B-2

C The Spanning Tree

Overview	C-1
The Spanning Tree Algorithm	C-2
The Spanning Tree Computation Process	C-4
Bridge Spanning Tree Parameters	C-7
Port Spanning Tree Parameters.....	C-13

D Repairing Nonvolatile Flash Memory

Overview	D-1
Power Interrupts During Upgrades	D-2
Symptoms of Corrupted Nonvolatile Flash Memory	D-3
The Recovery Process.....	D-5

Glossary

Index

Figures

Figure 1-1	Store and Forward Technology.....	1-6
Figure 1-2	Cut-Through Technology.....	1-7
Figure 1-3	Redundant Path for Network Availability.....	1-8
Figure 2-1	DECswitch 900EE Network Module.....	2-5
Figure 2-2	DECswitch 900EE Departmental Backbone.....	2-8
Figure 2-3	DECswitch 900EF Network Module.....	2-10
Figure 2-4	DECswitch 900EF Departmental Backbone.....	2-13
Figure 2-5	PEswitch 900TX Network Module.....	2-16
Figure 2-6	PEswitch 900TX for High-Performance Desktops.....	2-19
Figure 3-1	Frame Formats.....	3-2
Figure 3-2	Ethernet V2/FDDI Translation Example.....	3-4
Figure 3-3	IP Fragmentation Example.....	3-6
Figure 3-4	Novell IPX: Ethernet V2 Frame Format.....	3-7
Figure 3-5	Novell IPX: Raw 802.3 Frame Format.....	3-8
Figure 3-6	Frame Formats when IPX Translation is Enabled.....	3-8
Figure 3-7	Frame Formats when IPX Translation is Disabled.....	3-9
Figure 3-8	Standard Translation.....	3-11
Figure 3-9	Apple ARP V2 Translation.....	3-13
Figure 3-10	Apple ARP V1 Translation.....	3-13
Figure 4-1	Switch Summary Window.....	4-7
Figure 5-1	Dual Ring Port Configurations.....	5-3
Figure 5-2	Tree Port Configurations.....	5-5
Figure 5-3	DECconcentrator 900MX Port Configuration Capabilities.....	5-6
Figure 5-4	DECconcentrator 900TH Port Configuration Capabilities.....	5-7
Figure 5-5	DECconcentrator 900FH Port Configuration Capabilities.....	5-8
Figure 5-6	DECswitch 900EF Port Configuration Capabilities.....	5-9
Figure 5-7	PEswitch 900TX Port Configuration Capabilities.....	5-10
Figure 5-8	Ring Building Blocks.....	5-14
Figure 5-9	Tree Building Blocks.....	5-15

Figure 5-10	DECconcentrator Tree Connections in Hub Backplane.....	5-21
Figure 5-11	Building Block Representation of Example 1.....	5-21
Figure 5-12	Tree Connections with Switches and Concentrators	5-23
Figure 5-13	Building Block Representation of Example 2.....	5-23
Figure 5-14	Tree Connections to an External FDDI Network	5-25
Figure 5-15	Building Block Representation of Example 3.....	5-25
Figure 5-16	Dual Homed Connections to an FDDI Network.....	5-27
Figure 5-17	Building Block Representation of Example 4.....	5-27
Figure 5-18	Hub-Based Tree Connections to an External FDDI Network	5-29
Figure 5-19	Building Block Representation of Example 5.....	5-29
Figure 5-20	DECconcentrator Dual Ring Connections to an FDDI Network ...	5-31
Figure 5-21	Building Block Representation of Example 1.....	5-31
Figure 5-22	Dual Ring Connections for DECswitch 900EF.....	5-33
Figure 5-23	Building Block Representation of Example 2.....	5-33
Figure 5-24	Dual Ring Connections for PESwitch 900TX	5-35
Figure 5-25	Building Block Representation of Example 3.....	5-35
Figure 5-26	Self-Contained Dual Ring in the Backplane	5-36
Figure 5-27	Ring Configuration.....	5-38
Figure 5-28	Tree Configuration	5-40
Figure 5-29	Token Flow through Dual Ringed DEChub 900 Modules	5-43
Figure 5-30	Token Flow through Treed DEChub 900 Modules	5-45
Figure 5-31	Legal Dual Ring of Trees Topology	5-48
Figure 5-32	Illegal Dual Ring of Trees Topology	5-49
Figure 5-33	Valid FDDI Configurations for DEChub FDDI Modules.....	5-51
Figure A-1	FDDI Dual Ring.....	A-3
Figure A-2	FDDI Station Types.....	A-4
Figure A-3	FDDI Port Types.....	A-7
Figure A-4	FDDI Topologies	A-11
Figure A-5	Wrapped FDDI Ring.....	A-13

Figure A-6 FDDI Connection Rules.....	A-14
Figure A-7 Connecting to Similar Ports	A-16

Tables

Table 2-1 900-Series Switches Product Comparisons.....	2-3
Table 3-1 Field Descriptions	3-3
Table 3-2 Rules: Standard Ethernet to FDDI Translation.....	3-11
Table 3-3 Rules: Ethernet to FDDI Translation.....	3-12
Table 3-4 Rules: FDDI to Ethernet Translation.....	3-12
Table 4-1 Switch Summary Window Buttons.....	4-8
Table A-1 FDDI Connection Rules and Station States.....	A-17
Table B-1 Directory Names Available.....	B-3

Preface

About this Guide

Introduction

This guide describes Digital's hub-based datalink switching products that are targeted at the workgroup and departmental levels of computing. These products, for shared and switched Ethernet, integrate easily into Digital's switching products to build high-performance enterprise networks.

Intended Audience

This manual has two major audiences:

- Pre-sales technical support — includes Digital's technical sales force and Value Added Resellers (VARs).
- Post-sales support — includes Digital's Multivendor Customer Service personnel and Digital's customers.

Other Books in This Series

Following is a list of associated documents:

Title	Order Number
<i>DEChub Network Configuration</i>	EK-CONFIG-CG. A01
<i>DEChub Network Modules 900-Series Concentrator Reference</i>	EK-CONTR-HR. A01
<i>DEChub Network Modules Repeater Reference</i>	EK-REPTR-HR. A01
<i>DEChub Network Products Problem Solving</i>	EK-PRBSV-HR. A01
<i>DECswitch 900EE Installation</i>	EK-DEBMP-IN. A01
<i>DECswitch 900EF Installation</i>	EK-DEFBA-IN. A01
<i>PEswitch 900TX Installation</i>	EK-DESBF-IN. A01

What is in this manual

This manual contains the following information:

- Conceptual information common to Digital Equipment Corporation's 900-series switches.
- Description and comparison of Digital's 900-series switch products.
- A brief overview of how to use the HUBwatch graphical user interface (GUI) to manage Digital's 900-series switches.
- An overview of common switch management tasks, the windows you use to perform the tasks, and how to perform the task.
- An overview of Digital's 900-series switches and a description of the features and functionality common to Digital's 900-series switches.

- Conceptual information related to FDDI configuration capabilities that are supported in Digital's 900-series switches.
- A conceptual overview of the spanning tree algorithm and operation.
- What to do if your module's nonvolatile flash memory becomes corrupted.
- How to electronically access product information through Digital's Internet ftp server.

What is not In This Manual

This manual does not contain detailed procedural instructions for performing HUBwatch device configuration and network management tasks. You can find such information in the HUBwatch online help. The online help complements this manual and provides the step-by-step instructions necessary for using HUBwatch and associated network modules.

Structure of this manual

This manual is structured as follows:

- Chapter 1 introduces the concept of a LAN Switch. The chapter provides an overview of switches and how they fit into various network topologies.
- Chapter 2 introduces Digital's 900-Series switches and compares features and functionality of the various models.
- Chapter 3 lists and describes the technical features and functionality common to Digital's 900-Series switches.
- Chapter 4 lists some of the most common management tasks required by network managers and, using example HUBwatch window displays, explains how to quickly perform the tasks. Also included in the task examples are the relevant SNMP MIB object names for the convenience of non-HUBwatch users.
- Chapter 5 describes FDDI configuration capabilities that are supported in the DEChub 900 FDDI network modules.
- Appendix A provides an overview of FDDI concepts.

- Appendix B explains how to access the DEChub 900 product's online release notes, public MIBs, Digital's private MIBs, firmware images, and requests for comments (RFCs).
- Appendix C provides a conceptual overview of the spanning tree algorithm and operation.
- Appendix D describes how to repair a corrupted Flash memory.
- A Glossary provides definitions of terms common to the DEChub 900 family of products.
- Index

Conventions

The following conventions are used in this manual:

Convention	Meaning
Special Type	Indicates a literal example of system output or user input.
<i>lowercase italics</i>	Indicates a variable.

Firmware Updates

Digital continuously improves the quality of DEChub products through periodic firmware releases. To ensure the high quality and interoperability of HUBwatch products, you should always use the latest available versions of DEChub firmware.

FTP Location

You can get information about the latest firmware releases from your local Digital reseller or your local Digital Sales Office. You can also get this information by reading the README file found in the

`/pub/DEC/hub900` directory at `ftp.digital.com`.

How to Register for Release Notification

Firmware updates are customer installable. To register for automatic notification of new firmware releases, return the Business Reply Card supplied with the switch product. Alternatively, you can use the Internet by sending your Name, Title, and Mailing Address to `dechub_notice@lkg.dec.com`.

How To Load New Firmware

New Firmware can be loaded using the following tools:

Tool	Where To Get More Information
HUBloader	<i>HUBwatch USE</i> HUBwatch Online Help
DECndu Plus	<i>Using DECndu Plus (MS-DOS)</i>

Correspondence

Documentation Comments

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

Attn: Documentation Project Manager
FAX: (508) 486-6093
E-MAIL: doc_quality@lkg.mts.dec.com

Online Services

To locate product specific information, refer to the following online services:

BBS

To read the Bulletin Board System, set your modem to 8 bits, no parity, 1 stop bit and dial 508-486-5766 (U.S.)

WWW

The Digital Equipment Corporation Network Products Business Home Page on the World Wide Web is at the following addresses:

North America: <http://www.networks.digital.com>
Europe: <http://www.networks.europe.digital.com>
Australia <http://www.digital.com.au/networks>

How to Order Additional Documentation

Type of Order	How to Order
Direct Telephone Orders	In continental USA call:1-800-DIGITAL (1-800-344-4825) <ul style="list-style-type: none">• In Canada call: 1-800-267-6215• In New Hampshire, Alaska, or Hawaii call: 1-603-884-6660
Electronic Orders (U.S. Only)	Dial 1-800-dec-demo with any VT100 or VT200 compatible terminal and a 1200 baud modem. If you need assistance, call: 1-800-DIGITAL (1-800-344-4825)
Direct Mail Orders from the United States and Puerto Rico	Mail your order to: DIGITAL EQUIPMENT CORPORATION P.O. Box CS2008 Nashua, New Hampshire 03061 (Any prepaid order from Puerto Rico must be placed with the Local Digital Subsidiary. For further information call 809-754-7575.)
Direct Mail Orders from Canada	Mail your order to: DIGITAL EQUIPMENT OF CANADA LTD. 940 Belfast Road Ottawa, Ontario, Canada K1G 4C2 Attn: A&SG Business Manager
International	Mail your order to: DIGITAL EQUIPMENT CORPORATION A&SG Business Manager c/o Digital's local subsidiary or approved distributor
Internal (Digital)	Internal orders should be placed through U.S. Software Supply Business (SSB), Digital Equipment Corporation, 10 Cotton Rd. Nashua, NH. 03063-1260

Chapter 1

LAN Switches

Overview

Introduction

High-performance client server applications and interactive multimedia services are placing new demands on the networks that support them. This chapter describes how local area network (LAN) switches meet these challenges.

In This Chapter

The following topics are covered in this chapter:

Topic	See Page
What is a LAN Switch?	1-2
Switching at Different Levels in the Organization	1-3
LAN Switching Technology	1-5

What is a LAN Switch?

Introduction

The LAN switch is a relatively new class of internetworking product that circumvents the shortcomings of conventional bridge/routers in the microsegmentation of LAN environments. LAN switches can allow the process of microsegmentation to be extended to its ultimate limit of a single end station per LAN segment — a dedicated or *private* LAN connection for each user and server.

Because the LAN switch is a new type of bridge or bridge/router, switching is not restricted to a particular LAN technology.

LAN switches are sometimes called *frame switches* in order to stress the fact that they process and forward variable length LAN packets (or frames) and to distinguish them from *cell switches*, such as asynchronous transfer mode (ATM) switches, which process and forward fixed-length (53 byte) cells.

Properties Associated With LAN Switches

Properties normally associated with LAN switches are:

- Low cost per port
- High throughput
- Low latency

Switching at Different Levels in the Organization

Introduction

Switching permits organizations to meet the network performance demands of their users and applications. By incorporating switches into an existing LAN, network managers can increase network throughput without altering the network cabling infrastructure. In this way, switches help preserve network investments as needs change.

As discussed in the following sections, requirements for switches depend on the network level (desktop, departmental, or enterprise) where they are used.

Desktop Switching

At the desktop level, the goals are to maximize performance at minimal cost.

For users involved in data-intensive activities, such as database queries that result in large file transfers to the desktop, a network manager can personalize the bandwidth available to individual users.

Desktop switching enables data-intensive applications to utilize a dedicated high-speed line so they are not contending with other applications for bandwidth and, effectively, slowing down the entire network.

Departmental Switching

At the departmental level, the issues turn to traffic control and security, or *firewalling*.

Bandwidth-intensive desktops are segmented into manageable entities to ensure that they have access to required information and resources — but nothing extraneous or classified.

As an example, consider a medical imaging application, which places a very high load on a network and requires full protection of patient information. By grouping users according to needs and implementing

switches between the groups, a network manager can deliver the necessary bandwidth, while protecting privileged data.

To achieve firewalling and to gain greater control over the traffic, the switch can provide protocol or address filtering. In this respect, a switch can combine the security and functionality of a router, while retaining the performance capabilities originally sought from a switching solution.

Enterprise Switching

In an enterprise network, departmental workgroups must be interconnected to ensure quick access to information, communications, and resources.

Bandwidth becomes a primary concern, along with performance and availability. Financial services provide a good example, where users of a campus backbone share common databases, real-time applications and servers.

Enterprise switching provides the essential high-speed link between department LANs for optimal network responsiveness and high availability that is required in this transaction-intensive environment.

Here, at the heart of the network, the network manager must consider network expansion and provide appropriate redundancy to permit growth and ensure availability.

LAN Switching Technology

Introduction

LAN switching provides the physical connections (between users and independent LANs) that allows data packets to be switched from one LAN to another.

Packet switching is achieved through the use of either *store-and-forward* or *cut-through* technology.

Store-and-Forward Switches

Based on bridging algorithms, store-and-forward switches process the data packets passing through them, validating that the packets have been received without error.

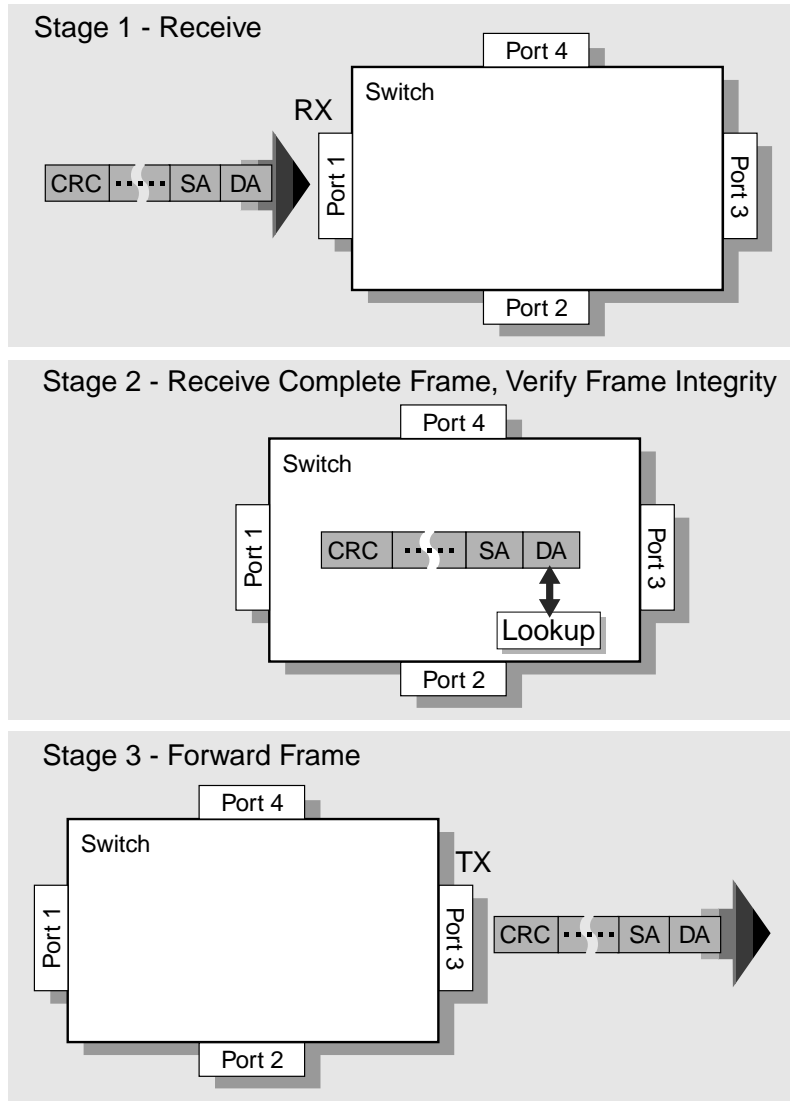
As shown in Figure 1-1, a store-and-forward switch waits to receive an entire packet from the network link, verifies packet integrity by examining the frame check sequence (CRC) field, processes its destination address (and, optionally, other fields) and, only then, forwards the packet to the appropriate network.

Cut-Through Switches

As shown in Figure 1-2, cut-through switches, unlike store-and-forward switches, do not attempt to validate the data in the packets passing through them. A cut-through switch begins retransmitting a packet as soon as it reads its destination address — even before it has received the entire packet.

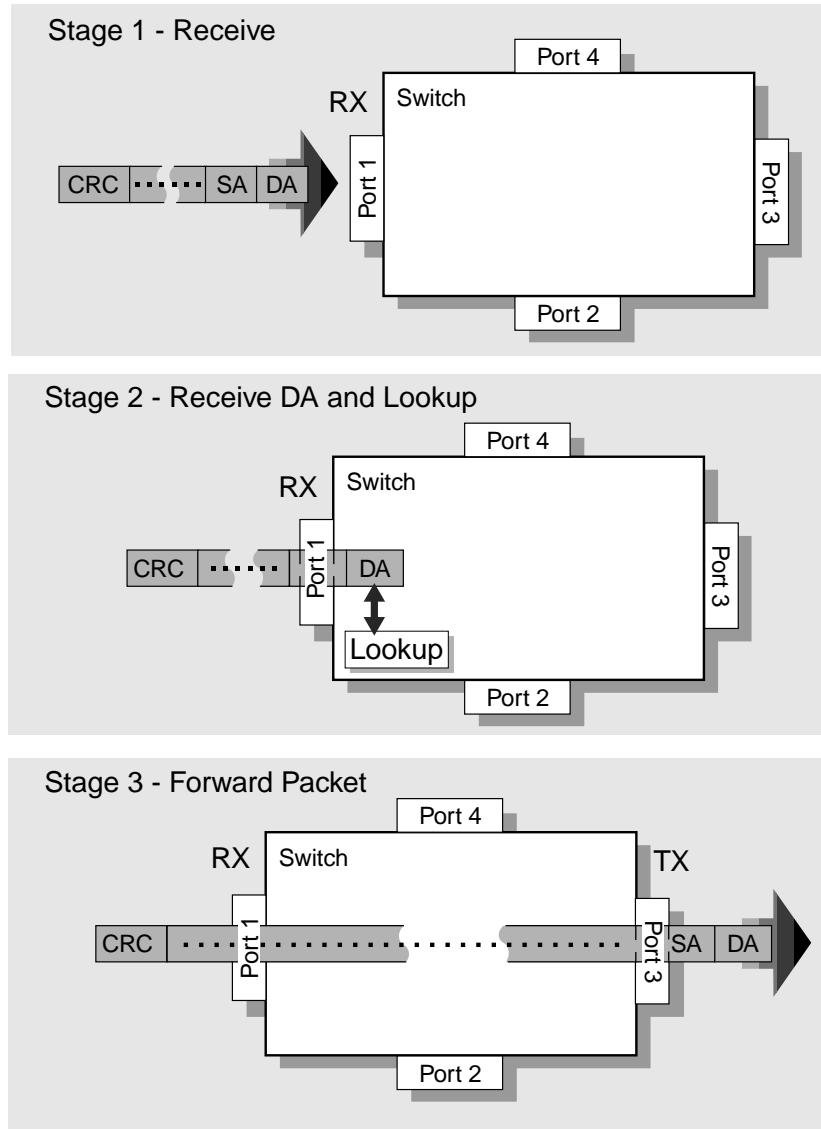
Because cut-through switches start transmitting the packet on the destination LAN before the packet has been entirely received, they typically have very low latency.

Figure 1–1 Store and Forward Technology



LKG-10105-951

Figure 1–2 Cut-Through Technology



LKG-10106-95I

Packet Integrity

The key advantage of store-and-forward switches is that their use guarantees the integrity of the packets passing through. The store-and-forward switch detects bad or incomplete fragments and does not propagate them through the extended LAN.

IEEE 802.1-compliant store-and-forward switches provide additional levels of functionality, such as support for redundant paths, to ensure network availability.

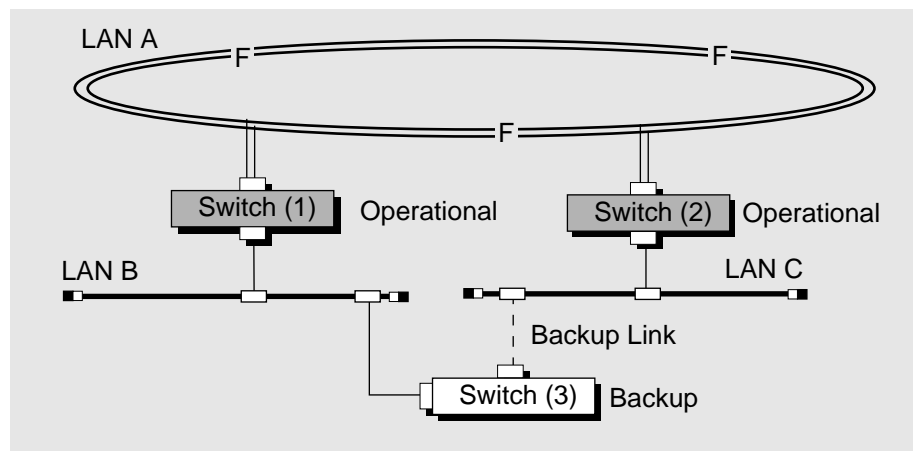
For example, as shown in Figure 1-3, there are two separate paths between LAN A and LAN C:

1. Through Switch 1 to LAN B and then through Switch 3
2. Through Switch 2

The first path (through Switches 1 and 3) is the redundant (backup) path that can be used if Switch 2 fails.

Path 1 is not available unless Path 2 becomes unavailable.

Figure 1-3 Redundant Path for Network Availability



LKG-10118-95F

Which Switching Method is More Effective?

The effectiveness of store-and-forward and cut-through switching methods depends on the network technologies on which they are deployed. This section compares the effectiveness of both switching methods when switches are used to interconnect the following network types:

- Ethernet
- FDDI
- Dissimilar Networks

Ethernet:

Ethernet is a collision-oriented approach to transmitting data on a network. If two stations on an Ethernet network attempt to transmit data at the same time, a collision occurs. Collisions can result in packet fragments (or “runt” packets) that do not contain any useful or complete user data.

When cut-through switches are used to switch Ethernet traffic, the network manager must consider both the integrity of data packets as well as the performance capabilities of the switch. Runt packets are filtered by store-and-forward switches but forwarded by cut-through switches. This is because cut-through switches only examine the destination address and then forward all packets immediately. Also, cut-through switches typically have less memory, which prevents them from providing adequate buffering on heavily loaded Ethernet networks.

In contrast, store-and-forward switches are often a better alternative for Ethernet networks because they can detect and reject runt packets, and because they typically carry more frame buffers.

FDDI:

FDDI networks are based on a timed token-passing, dual-ring scheme. Collisions do not occur with this type of network technology, therefore there are no runt packets. Cut-through switching can be used effectively to improve network performance when forwarding to other FDDI local area networks.

Dissimilar Networks:

When switching between different speeds or technologies is involved, cut-through switches are not very useful. For example, differences in speed between FDDI (100 Mbps) and Ethernet (10 Mbps), or between *fast* Ethernet (100 Mbps) and Ethernet (10 Mbps) makes buffering unavoidable. In addition, switching between FDDI and Ethernet involves translation of frame formats, fragmentation of large packets (if fragmentation is supported) and recalculation of checksums. This typically requires packets to be fully received and stored before forwarding them.

Store-and-forward switches are the only effective solutions when switching between dissimilar network technologies is involved.

Chapter 2

900-Series Switches

Overview

Introduction

This chapter lists the functions and features of Digital's 900-Series switches.

In This Chapter

The following topics are covered in this chapter:

Topic	See page...
900-Series Switch Products	2-2
DECswitch 900EE Module	2-5
DECswitch 900EF Module	2-10
PEswitch 900TX Module	2-16

900-Series Switch Products

Introduction

Switching is a cost-effective way for organizations to meet the network performance demands of their users and applications. Digital's 900-series switch products bring the benefits of high performance and 802.1d-compliant switching to a range of network applications for both desktop and department levels of computing.

Description

Digital's 900-series Switch products comprise the following modules:

Product Name	Part Number	Description
DECswitch 900EE	DEBMP-MA	Six-port Ethernet-to-Ethernet departmental switch.
DECswitch 900EF	DEFBA-MA	Six-port Ethernet-to-FDDI departmental switch.
PEswitch 900TX	DESBF-MA	Six port Ethernet-to-FDDI desktop switch.

These 802.1d-compliant switches combine data integrity with high performance. They are designed to connect multiple high-performance personal computers, workstations and servers on a single LAN, and can also interconnect multiple desktop and departmental LANs into a high-performance corporate backbone.

Table 2-1 provides a comparison of 900-series switch features:

Table 2-1 900-Series Switches Product Comparisons

Feature	DECswitch 900EE	DECswitch 900EF	PEswitch 900TX
Destination address filtering	Yes	Yes	Yes
Source address filtering	Yes	Yes	Yes
Protocol filtering	Yes	Yes	Yes
802.3/Ethernet ports	6	6	6
FDDI ports	None	1 DAS	1 DAS ¹
Front Panel Port connectors	2 AUI and 4 10BaseT connectors	2 AUI, 4 10BaseT, and 1 DAS MIC FDDI connector	6 10BaseT connectors
IEEE 802.1d compliant	Yes	Yes	Yes
SNMP manageable	Yes	Yes	Yes
HUBwatch manageable	Yes	Yes	Yes
Upgradeable Flash	Yes	Yes	Yes
User-settable rate limiting	Yes	Yes	Yes
Support for full translation of packets between FDDI and Ethernet	Not applicable	Yes	Yes
Specialized support for non-translating protocols (IEEE 802.1h)	Not applicable	Yes	Yes
Support for IP packet fragmentation (RFC 791 and RFC 1191)	Not Applicable	Yes	Yes
Out-of-band management (OBM)	Yes	Yes	Yes

(Continued on next page.)

Feature	DECswitch 900EE	DECswitch 900EF	PEswitch 900TX
Setup port	Yes	Yes	Yes
Routing upgrade via software load	Yes	Yes	No
Ethernet address table entries	8,000	8,000	Up to 96
Backplane connections in Hub	Up to 6 Ethernets	Up to 6 Ethernets and 1 DAS	Up to 6 Ethernets and 1 DAS
Standalone capability	Yes	Yes	Yes
Secure mode/manual mode	Yes	Yes	Yes
10BaseT port connector	Straight-thru (=)	Straight-thru (=)	Cross-over (X)

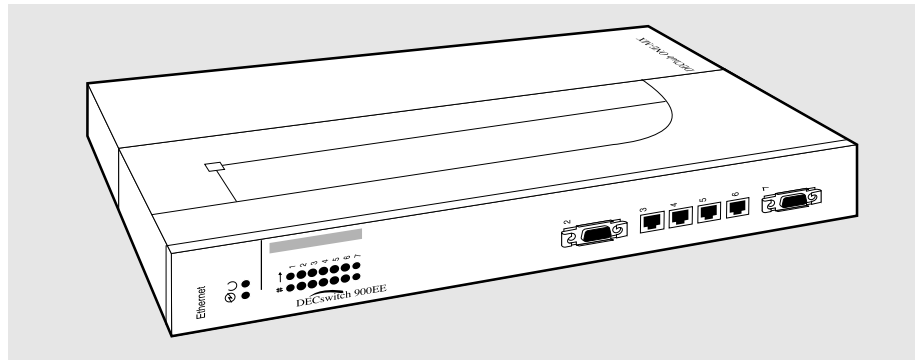
¹ No front panel port. The FDDI port is provided only through the DEChub 900 MultiSwitch enterprise hub or the DEF1H-xx docking station.

DECswitch 900EE Module

Introduction

The DECswitch 900EE module (see Figure 2-1), is a six port (two AUI ports and four 10BaseT ports) SNMP manageable Ethernet department backbone switch, providing full-speed switching capability between each of the six 802.3/Ethernet ports. It supports various filtering capabilities (source address, destination address, protocol type) as well as providing a large address table (8000 entries). The module is also fully IEEE 802.1d standards-compliant.

Figure 2-1 DECswitch 900EE Network Module



LKG-10107-95F

The module is provided with four front-panel 10BaseT 802.3/Ethernet ports and two front panel AUI ports. Each of these ports is configurable, via HUBwatch software, to connect to the front panel interface connectors, or alternatively, to a DEChub 900 backplane LAN segment. This feature offers maximum configuration flexibility whether the product is installed into a DEChub ONE docking station (DEF1H or DEHUA), or installed into the DEChub 900 MultiSwitch enterprise hub.

The DECswitch 900EE network module also offers nonvolatile flash memory for easy, non-disruptive upgrades of the device firmware using Trivial File Transfer Protocol (TFTP) load protocol. It is available on a wide variety of platforms including DOS, ULTRIX, UNIX, and OpenVMS VAX operating systems. This eliminates the need to replace or upgrade hardware in the future, and avoids the associated costs and disruption to network users.

Like all DEChub 900 network modules, the DECswitch 900EE network module also features integrated SNMP for easy, comprehensive management.

Highlights

The DECswitch 900EE Module:

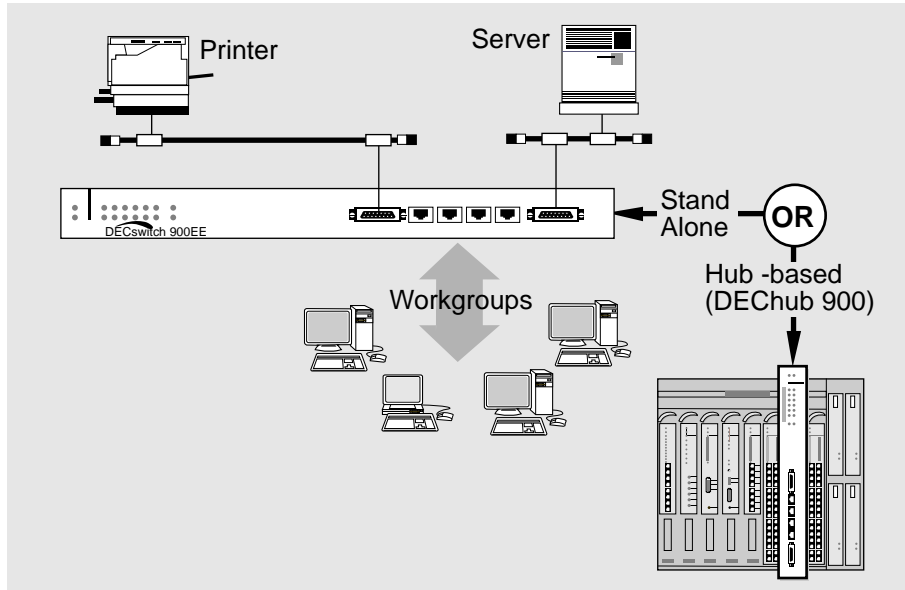
- Provides a low-cost, high-performance, six-port Ethernet switch.
- Offers standalone (DEF1H or DEHUA) or DEChub 900 MultiSwitch configuration options.
- Improves Ethernet LAN configuration flexibility and performance by dynamically switching multiple Ethernet LANs.
- Improves efficiency and utilization of current Ethernet networks.
- Features upgradeable device firmware (in nonvolatile flash memory) using Trivial File Transfer Protocol (TFTP) with HUBloader or through the setup port with any TFTP server.
- Offers user-configurable rate limiting for broadcast and multicast packets by address and specific protocol.
- Features a built-in SNMP management agent. It supports a comprehensive graphical user interface (GUI), via HUBwatch, that is identical for both in-band and out-of-band management.
- Supports a rich set of standard and private MIBs: MIB-II (RFC 1213), Bridge MIB (RFC 1493), Ethernet MIB (RFC 1398), and Digital enterprise MIBs for full management and configuration capability via SNMP

- Supports full-performance filtering between all of its six ports — at full Ethernet speeds (14,880 packets/second/Ethernet).
- Delivers an aggregate forwarding rate of 45,000 pps (with three ports forwarding and three ports receiving) which is the maximum rate at which six Ethernets can handle traffic.
- Provides spanning tree loop detection protocol
 - IEEE 802.1d (default)
 - Digital LB100 mode
- Provides ability to turn off spanning tree algorithm on individual switch ports on a per-port basis.

Department Backbone with the DECswitch 900EE

Figure 2-2 shows the DECswitch 900EE module used as a high-performance Ethernet switch for a department backbone:

Figure 2-2 DECswitch 900EE Departmental Backbone



LKG-10108-95F

DECswitch 900EE Ordering Information

Description	Order Number
DECswitch 900EE network module	DEBMP-MA
DEChub ONE-MX docking station for DEChub 900 modules (for standalone use). Includes AUI network connector, power supply, setup port, OBM port, and 2 optional FDDI ModPMDs (A/M and B/S) ports.	DEF1H-##
DEChub ONE docking station for DEChub 900 modules (for standalone use). Includes AUI network connector, power supply, setup port, and OBM Port.	DEHUA-##

Note: ## = Country kit code. Order the following as needed. CA = United States, Canada, and Japan; CD = Denmark; CE = United Kingdom; CI = Italy; CK = Switzerland; CT = Israel; CX = Central Europe; CZ = Australia; DJ = India and South Africa

DECswitch 900EE Specifications

Parameter	Specification																
Height	44.45 cm (17.5 in)																
Width	4.45 cm (1.75 in)																
Depth	15.25 cm (6 in) ¹																
Weight	1.8 kg (4 lb) ²																
Operating Temperature	5° C to 50° C (41°F to 122°F)																
Relative Humidity	10% to 95% non-condensing																
Altitude	Sea level to 4900 m (16,000 ft)																
Power	62.5 W total power 8.0 A, 5 Vdc 0.1 A, 12 Vdc — derived from 15 Vdc 1.5 A, 15 Vdc																
Connectors	4 shielded 10BaseT (MJ-8 RJ45 type) -- straight-thru wiring 2 15-pin D-Subminiature (AUI) sockets																
Certification	CE, CSA, FCC, TUV, UL, VCCI																
Standards Compliancy	IEEE 802.1d, IEEE 802.3, Ethernet V1 & V2																
Cooling	Three fans																
Acoustics	<table border="1"> <thead> <tr> <th>Product</th> <th>Operating Mode</th> <th>LwAD³</th> <th>LPAm⁴</th> </tr> </thead> <tbody> <tr> <td>DEBMP-MA</td> <td>Idle/Operate</td> <td>5.0 Bels</td> <td>36 dBA</td> </tr> <tr> <td>DEBMP-MA with DEHUA-C</td> <td>Idle/Operate</td> <td>5.3 Bels</td> <td>40 dBA</td> </tr> <tr> <td>DEBMP-MA with DEF1H-C</td> <td>Idle/Operate</td> <td>5.4 Bels</td> <td>39 dBA</td> </tr> </tbody> </table>	Product	Operating Mode	LwAD ³	LPAm ⁴	DEBMP-MA	Idle/Operate	5.0 Bels	36 dBA	DEBMP-MA with DEHUA-C	Idle/Operate	5.3 Bels	40 dBA	DEBMP-MA with DEF1H-C	Idle/Operate	5.4 Bels	39 dBA
Product	Operating Mode	LwAD ³	LPAm ⁴														
DEBMP-MA	Idle/Operate	5.0 Bels	36 dBA														
DEBMP-MA with DEHUA-C	Idle/Operate	5.3 Bels	40 dBA														
DEBMP-MA with DEF1H-C	Idle/Operate	5.4 Bels	39 dBA														

¹ Include an additional 14.99 cm (5.9 in) when attached to a DEChub ONE-MX; when attached to a DEChub ONE, include an additional 10.16 cm (4.0 in).

² Include an additional 2.10 kg (4.63 lb) when attached to a DEChub ONE-MX; when attached to a DEChub ONE, include an additional 1.59 kg (3.5 lb).

³ LwAd = Declared A-weighted sound power level measured in bels re 1 pW. 1 bel = 10 dB.

⁴ LPAm = Declared Average A-weighted sound pressure level measured in dB (re 20 uPa) at the four bystander positions: 1.0 meter from the front, rear, and side edges of the standard test table, and 1.5 meters above the floor.

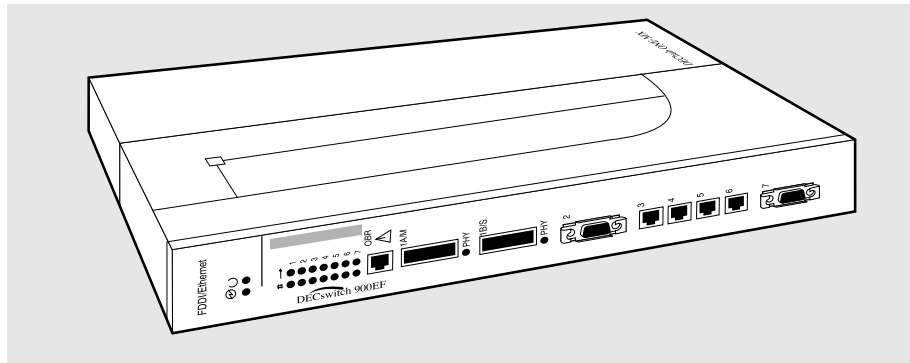
All data is measured in accordance with ANSI S12.10, ISO 9296 and ISO 7779.

DECswitch 900EF Module

Introduction

The DECswitch 900EF module (see Figure 2-3), is a high-throughput, SNMP manageable, multiport network switch solution for linking Ethernet LANs with FDDI. The module improves the configuration flexibility of your network by easily integrating Ethernet and FDDI LANs within a single standalone or hub-based architecture. It provides switching for up to 6 Ethernet LANs and 1 high-speed FDDI network.

Figure 2-3 DECswitch 900EF Network Module



LKG-10104-95F

The DECswitch 900EF module has 6 Ethernet switched ports on the front panel (two AUI and four 10BaseT), 1 DAS FDDI port, and 1 shielded MJ-6 OBR port for connecton of an (optional) OBR device.

With HUBwatch management, each port (including FDDI PHY ports 1A/M and 1B/S) can be individually switched to a DEChub 900 backplane LAN. Also, Port 3 can be redirected to the DEChub 900 backplane ThinWire LAN segment or to other backplane LANs.

When connected to a DEChub ONE docking station (DEF1H or DEHUA), a user can configure either the docking station's AUI port or the module's (front panel) port 4 as an active Ethernet interface.

When connected to a DEChub ONE-MX docking station (DEF1H), each of the FDDI PHY ports (1A/M and 1B/S) is individually switchable to the corresponding ModPMD PHY ports on the DEChub ONE-MX.

The DECswitch 900EF network module is a true backbone network switch that supports complete filtering capabilities (source address, destination address, protocol type). It includes a large address table (8K entries) and is fully IEEE 802.1d standards-compliant — ensuring high performance and packet integrity required in large networks.

The DECswitch 900EF network module also offers nonvolatile flash memory for easy, non-disruptive upgrades of the device firmware using Trivial File Transfer Protocol (TFTP) load protocol. It is available on a wide variety of platforms including DOS, ULTRIX, UNIX, and OpenVMS VAX operating systems. This eliminates the need to replace or upgrade hardware in the future, and avoids the associated costs and disruption to network users.

Like all DEChub 900 network modules, the DECswitch 900EF network module features integrated SNMP for easy, comprehensive management.

Highlights

The DECswitch 900EF module:

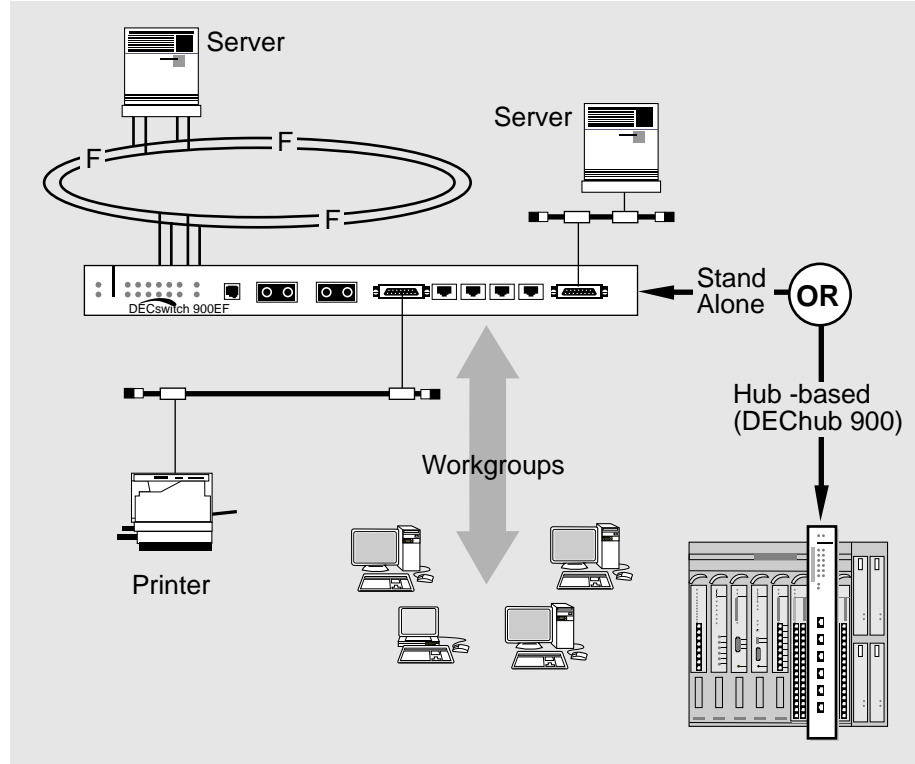
- Supplies a seven-port switch, providing six Ethernet ports (2 AUI and 4 RJ45 MJ-8), plus one DAS (ANSI MIC) FDDI port.
- Provides a front panel Optical Bypass Relay (OBR) connector (6-pin MJ) that allows connection of an (optional) OBR device to maintain connectivity of the FDDI ring in the absence of power or during fault conditions in a station.
- Features a built-in SNMP agent for in-band and out-of-band management — whether configured in a single-slot standalone DEChub ONE chassis or installed in a DEChub 900 MultiSwitch enterprise hub
- Features upgradeable device firmware (in nonvolatile flash memory) using Trivial File Transfer Protocol (TFTP) with HUBloader or through the setup port with any TFTP server.
- Offers multiple filtering options, including source and destination address and protocol
- Supports high filtering rates — 14,880 pps on each Ethernet port, and a filtering rate of more than 440,000 pps on the FDDI port

- Provides high-performance forwarding rates with an aggregate throughput in excess of 62,000 packets per second
- Supports 8K network addresses
- Handles IP fragmentation of large packets from FDDI per RFC 791 (Internet Protocol) and RFC 1191 (Path MTU Discovery)
- Provides translation between FDDI and 802.3/Ethernet frame formats for direct transparent connections, translation of AppleTalk 1 and 2 AARP packets, and handling of raw 802.3 Novell IPX packets
- Supports a rich set of standard and private MIBs: MIB-II (RFC 1213), Bridge MIB (RFC 1493), FDDI MIB (RFC 1512), Ethernet MIB (RFC 1398), and Digital enterprise MIBs for full management and configuration capability via SNMP
- Features out-of-band management using SNMP over SLIP through the OBM connector as an alternative to normal in-band management
- Provides user-configured rate limiting for broadcast and multicast packets by address and specific protocol
- Supports operation in either an FDDI tree or dual ring configuration. FDDI port 1A/M can be switched to emulate an M port of a concentrator. This action causes FDDI port 1B/S to automatically switch to emulate an S port.
- Provides spanning tree loop detection protocol
 - IEEE 802.1d (default)
 - Digital LB100 mode
- Provides ability to turn off spanning tree algorithm on individual switch ports on a per-port basis.

Department Backbone with the DECswitch 900EF

Figure 2-4 shows the DECswitch 900EF module used as a high-performance Ethernet switch for a department backbone:

Figure 2-4 DECswitch 900EF Departmental Backbone



DECswitch 900EF Ordering Information

Description	Order Number
DECswitch 900EF network module.	DEFBA-MA
DEChub ONE-MX docking station for DEChub 900 network modules (for standalone use). Includes AUI network connector, power supply, setup port, OBM port, and 2 optional FDDI ModPMDs (A/M and B/S) ports. (See following table for optional ModPMDs that are available to support your configuration.)	DEF1H-##
DEChub ONE docking station for DEChub 900 network modules (for standalone use). Includes AUI network connector, power supply, setup port, and OBM port.	DEHUA-##

Note: ## = Country kit code. Order the following as needed. CA = United States, Canada, and Japan; CD = Denmark; CE = United Kingdom; CI = Italy; CK = Switzerland; CT = Israel; CX = Central Europe; CZ = Australia; DJ = India and South Africa

Optional ModPMDs

Media	Order Number
Multi Mode Optics (ANSI MIC connector)	DEFXM-AA
Multi Mode Optics (SC connector)	DEFXM-SC
Single Mode Optics (SC connector)	DEFXS-SC
Single Mode Optics (ST connector)	DEFXS-BA
Unshielded Twisted Pair (RJ45 connector)	DEFXU-BA

DECswitch 900EF Specifications

Parameter	Specification			
Height	44.45 cm (17.5 in)			
Width	4.45 cm (1.75 in)			
Depth	15.25 cm (6 in) ¹			
Weight	1.8 kg (4 lb) ²			
Operating Temperature	5° C to 50° C (41° F to 122° F)			
Relative Humidity	10% to 95% non-condensing			
Altitude	Sea level to 4900 m (16, 000 ft)			
Power	67.5 W total power 9.0 A, 5 Vdc 0.1 A, 12 Vdc — derived from 15 Vdc 1.5 A, 15 Vdc			
Connectors	4 shielded 10BaseT (RJ45), 2 15 pin D-Subminiature (AUI) sockets, 1 FDDI DAS port, 1 shielded MJ-6 OBR connector			
Certification	CE, CSA, FCC, TUV, UL, VCCI			
Standards Compliancy	IEEE 802.1d, IEEE 802.1h, IEEE 802.1i, IEEE 802.3, Ethernet V1 & V2, ANSI X3/ISO 9314-*			
Cooling	Three fans			
Acoustics	Product	Operating Mode	LwAD³	LPAm⁴
	DEFBA-MA	Idle/Operate	5.0 Bels	36 dBA
	DEFBA-MA with DEHUA-C	Idle/Operate	5.4 Bels	40 dBA
	DEFBA-MA with DEF1H-C	Idle/Operate	5.4 Bels	39 dBA

¹. Add 14.99 cm (5.9 in) when attached to a DEChub ONE-MX; for a DEChub ONE, include an additional 10.16 cm (4.0 in).

². Include an additional 2.10 kg (4.63 lb) when attached to a DEChub ONE-MX; when attached to a DEChub ONE, include an additional 1.59 kg (3.5 lb).

³. LwAd = Declared A-weighted sound power level measured in bels re 1 pW. 1 bel = 10 dB.

⁴. LPAm = Declared Average A-weighted sound pressure level measured in dB (re 20 uPa) at the four bystander positions:
1.0 meter from the front, rear, and side edges of the standard test table, and 1.5 meters above the floor.

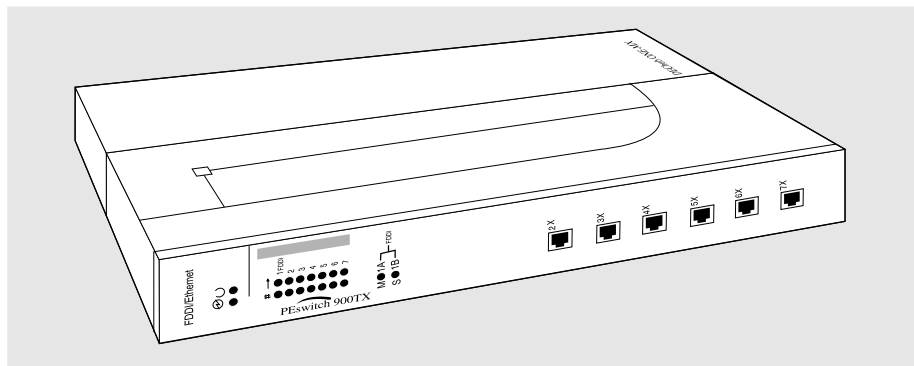
All data is measured in accordance with ANSI S12.10, ISO 9296 and ISO 7779.

PEswitch 900TX Module

Introduction

The PEs switch 900TX module (see Figure 2-5), is a full 802.1d-compliant, six-port switched (personal, 10 MB/s) Ethernet to FDDI switch. It combines high-performance switched Ethernet and packet integrity with high-performance FDDI server/network connectivity. It also delivers full IEEE-compliant 802.1d bridged Ethernet to FDDI translation and IP fragmentation.

Figure 2-5 PEs switch 900TX Network Module



LKG-10110-95F

The six front panel Ethernet ports of the PEs switch 900TX are all 10BaseT (MJ-8 RJ45) type (cross-over wired) connectors. The FDDI port connects through the DEChub 900 MultiSwitch enterprise hub backplane or, when used in a standalone, single-slot hub rack-and-stack configuration, through the DEChub ONE MX docking station (DEF1H) ModPMD ports.

The PEs switch 900TX is a IEEE 802.1d compliant bridge, and supports high-performance filtering and forwarding across all ports (i.e., Ethernet to Ethernet, and Ethernet to FDDI). Packet translation between Ethernet and FDDI, as well as IP packet fragmentation is supported. In addition, specialized support is offered for non-translated protocols (IEEE 802.1h) such as AppleTalk.

PEswitch 900TX functionality also allows you to selectively and cost-effectively upgrade the performance of desktop network connections by providing a switched Ethernet connection to each user.

When used in a DEChub 900 MultiSwitch enterprise hub, the PEs switch 900TX not only allows you to internetwork between switched Ethernet and FDDI across the DEChub 900 backplane, but it also makes switch management simple with the HUBwatch management tool.

The PEs switch 900TX network module also offers nonvolatile flash memory for easy, non-disruptive upgrades of the device firmware using Trivial File Transfer Protocol (TFTP) load protocol. It is available on a wide variety of platforms including DOS, ULTRIX, UNIX, and OpenVMS VAX operating systems. This eliminates the need to replace or upgrade hardware in the future, and avoids the associated costs and disruption to network users.

Like all DEChub 900 network modules, the PEs switch 900TX network module also features integrated SNMP for easy, comprehensive management.

Highlights

The PEs switch 900TX module:

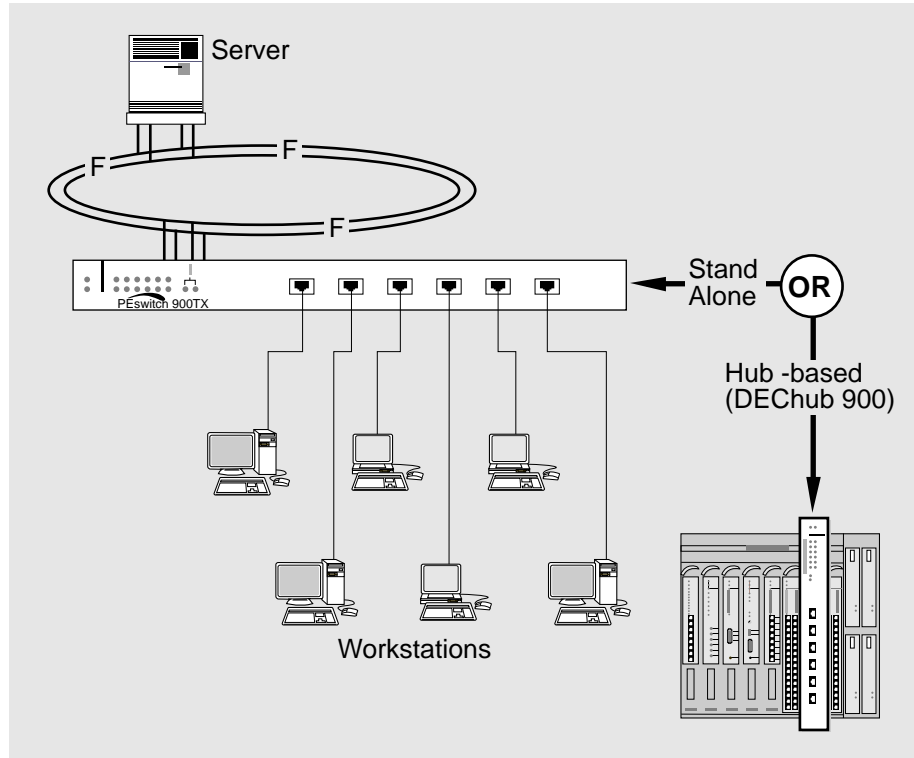
- Handles IP fragmentation of large packets from FDDI per RFC 791 (Internet Protocol) and RFC 1191 (Path MTU Discovery)
- Provides translation between FDDI and 802.3/Ethernet frame formats for direct transparent connections, translation of AppleTalk 1 and 2 ARP packets, and handling of raw 802.3 Novell IPX packets
- Supports a rich set of standard and private MIBs: MIB-II (RFC 1213), Bridge MIB (RFC 1493), FDDI MIB (RFC 1512), Ethernet MIB (RFC 1398), and Digital enterprise MIBs for full management and configuration capability via SNMP
- Provides a low-cost, dedicated, switched 10-Mb/s Ethernet solution for high-performance desktops, while maximizing a current investment in 10-Mb/s Ethernet

- Offers a dedicated 10-Mb channel per user with a connection to a high-speed link (FDDI) for more efficient access and improved response time to network-based servers and systems
- Features upgradeable device firmware (in nonvolatile flash memory) using Trivial File Transfer Protocol (TFTP) with HUBloader or through the setup port with any TFTP server.
- Supports up to 96 addresses across the 6 available Ethernet ports, and up to 8,000 on the FDDI port
- Delivers aggregate Ethernet forwarding rates in excess of 62,000 packets per second, combined with full-speed filtering for FDDI and all Ethernet ports
- Provides multiple filtering capabilities (source address, destination address, protocol type).
- 802.1d compliancy ensures packet integrity
- Allows selective performance upgrades of desktop network connections
- Provides for simplified GUI-based network management via the HUBwatch management application.
- Supports operation in either an FDDI tree or dual ring configuration. FDDI port 1A/M can be switched to emulate an M port of a concentrator. This action causes FDDI port 1B/S to automatically switch to emulate an S port.
- Provides spanning tree loop detection protocol
 - IEEE 802.1d (default)
 - Digital LB100 mode
- Provides ability to turn off spanning tree algorithm on individual switch ports on a per-port basis.

High-performance Desktops with the PEs witch 900TX

Figure 2-6 shows the PEs witch 900TX module used as a high-performance Ethernet switch for high-performance desktops:

Figure 2-6 PEs witch 900TX for High-Performance Desktops



LKG-10111-95F

PEswitch 900TX Ordering Information

Description	Order Number
PEswitch 900TX network module.	DESBF-MA
DEChub ONE-MX docking station for DEChub 900 network modules (for standalone use). Includes AUI network connector, power supply, setup port, OBM port, and 2 optional FDDI ModPMDs (A/M and B/S) ports. (See following table for optional ModPMDs that are available to support your configuration.	DEF1H-##
DEChub ONE docking station for DEChub 900 network modules (for standalone use). Includes AUI network connector, power supply, setup port, and OBM port.	DEHUA-##

Note: ## = Country kit code. Order the following as needed. CA = United States, Canada, and Japan; CD = Denmark; CE = United Kingdom; CI = Italy; CK = Switzerland; CT = Israel; CX = Central Europe; CZ = Australia; DJ = India and South Africa

Optional ModPMDs

Media	Order Number
Multi Mode Optics (ANSI MIC connector)	DEFXM-AA
Multi Mode Optics (SC connector)	DEFXM-SC
Single Mode Optics (ST connector)	DEFXS-BA
Single Mode Optics (SC connector)	DEFXS-SC
Unshielded Twisted Pair (RJ45 connector)	DEFXU-BA

PEswitch 900TX Specifications

Parameter	Specification																
Height	44.45 cm (17.5 in)																
Width	4.45 cm (1.75 in)																
Depth	15.25 cm (6 in) ¹																
Weight	1.8 kg (4 lb) ²																
Operating Temperature	5° C to 50° C (41°F to 122°F)																
Relative Humidity	10% to 95% non-condensing																
Altitude	Sea Level to 4900 m (16,000 ft)																
Power 40 dBA	50.5 W total power 8.0 A, 5 Vdc 0.1 A, 12 Vdc — derived from 15 Vdc 1.7 A, 15 Vdc																
Connectors	6 Shielded 10BaseT (MJ-8 RJ45 Type) — cross-over																
Certification	CE, CSA, FCC, TUV, UL, VCCI																
Standards Compliancy	IEEE 802.1d, IEEE 802.1h, IEEE 802.1i, IEEE 802.3, Ethernet V1 & V2, ANSI/ISO X3*																
Cooling	Three fans																
Acoustics	<table border="1"> <thead> <tr> <th>Product</th> <th>Operating Mode</th> <th>LwAD³</th> <th>LPAm⁴</th> </tr> </thead> <tbody> <tr> <td>DESBF-MA</td> <td>Idle/Operate</td> <td>5.0 Bels</td> <td>36 dBA</td> </tr> <tr> <td>DESBF-MA with DEHUA-C</td> <td>Idle/Operate</td> <td>5.3 Bels</td> <td>40 dBA</td> </tr> <tr> <td>DESBF-MA with DEF1H-C</td> <td>Idle/Operate</td> <td>5.4 Bels</td> <td>39 dBA</td> </tr> </tbody> </table>	Product	Operating Mode	LwAD ³	LPAm ⁴	DESBF-MA	Idle/Operate	5.0 Bels	36 dBA	DESBF-MA with DEHUA-C	Idle/Operate	5.3 Bels	40 dBA	DESBF-MA with DEF1H-C	Idle/Operate	5.4 Bels	39 dBA
	Product	Operating Mode	LwAD ³	LPAm ⁴													
	DESBF-MA	Idle/Operate	5.0 Bels	36 dBA													
	DESBF-MA with DEHUA-C	Idle/Operate	5.3 Bels	40 dBA													
DESBF-MA with DEF1H-C	Idle/Operate	5.4 Bels	39 dBA														

¹ Include an additional 14.99 cm (5.9 in) when attached to a DEChub ONE-MX; when attached to a DEChub ONE, include an additional 10.16 cm (4.0 in).

² Include an additional 2.10 kg (4.63 lb) when attached to a DEChub ONE-MX; when attached to a DEChub ONE, include an additional 1.59 kg (3.5 lb).

³ LwAd = Declared A-weighted sound power level measured in bels re 1 pW. 1 bel = 10 dB.

⁴ LPAm = Declared Average A-weighted sound pressure level measured in dB (re 20 uPa) at the four bystander positions: 1.0 meter from the front, rear, and side edges of the standard test table, and 1.5 meters above the floor.

All data is measured in accordance with ANSI S12.10, ISO 9296 and ISO 7779.

Chapter 3

Features and Functionality

Overview

Introduction

This chapter lists and describes the technical features of Digital's 900-Series switching products.

In This Chapter

The following topics are covered in this chapter:

Topic	See Page
Frame Formats	3-2
AppleTalk Translation	3-10
Rate Limiting	3-14
Frame Filtering/Forwarding	3-15
Managing Switches With HUBwatch	3-19
Out-of-band Management	3-23

Frame Formats

Introduction

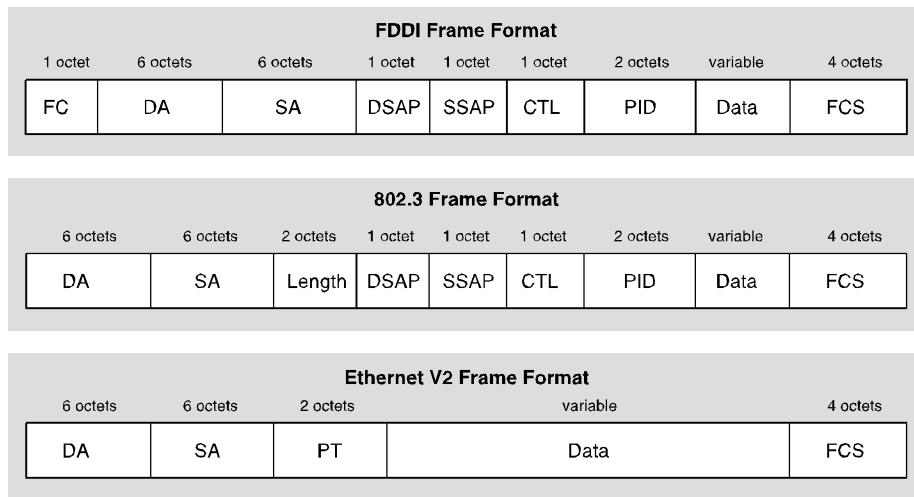
Digital's 900 family of switches are IEEE 802.3 translating switches. Unlike proprietary encapsulating switches (that require a decapsulating device at the receiving end), translating switches guarantee interoperability and transparency to upper level protocols, by creating standardized frames on all interconnected LANs.

Transparent Translation

Digital's 900-Series switches translate all frames that they forward between dissimilar interconnected LANs. Frames destined to be forwarded are first converted into the native frame format of the destination LAN. This allows all stations on an FDDI LAN to communicate transparently with all stations on an 802.3/Ethernet LAN.

As shown in Figure 3-1, frame formats for FDDI, 802.3, and Ethernet are all different.

Figure 3-1 Frame Formats



LKG-10129-96C

Table 3-1 provides a description of the frame format fields shown in Figure 3-1.

Table 3-1 Field Descriptions

Field	Description	Size (octets)
CTL	802.2 control field	1
DA	Destination Address	6
Data	User data	Variable*
DSAP	Destination Service Access Point	1
FC	Frame control	1
FCS	Frame Check Sequence	4
Length	Length of contents that follow, up to (but not including) the FCS field.	2
PID	Protocol Identifier	2
PT	Protocol Type	2
SA	Source Address	6
SSAP	Source Service Access Point	1

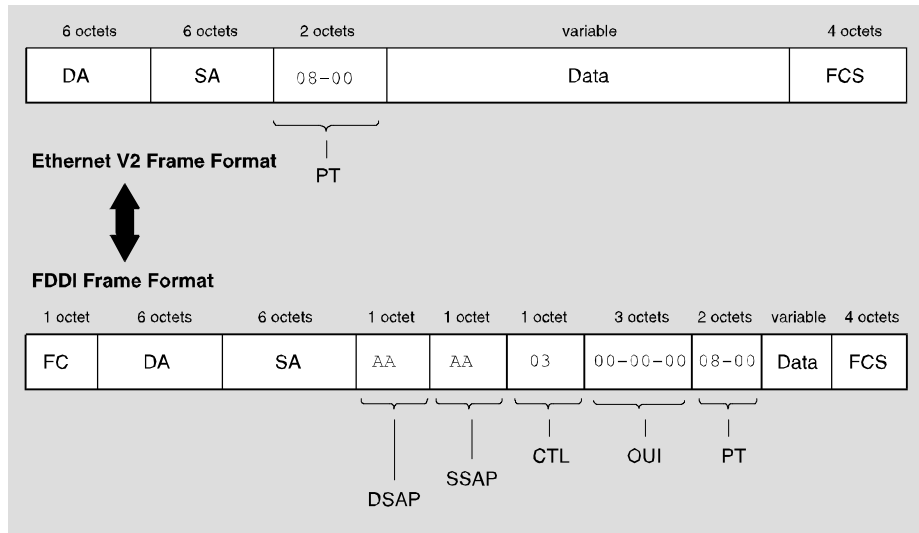
*FDDI: 0-4473 octets

802.3: 41-1495 octets

Ethernet: 46-1500 octets

Translation from the IEEE 802.3 format to the FDDI frame format is fairly straightforward, since both FDDI and 802.3 frames contain an 802.2 Logical Link Control (LLC) header. However, when translating a frame from the Ethernet format to the FDDI format, an 802.2 LLC header must be generated that conforms to Internet standard RFC 1390 (Figure 3-2 provides an example).

Figure 3-2 Ethernet V2/FDDI Translation Example



LKG-10130-96C

Note

Apple ARP (one of the protocols related to AppleTalk) presents a special case that deviates from the descriptions provided in this section (refer to the section titled, AppleTalk Translation).

A standard 802.2 LLC header is created for Ethernet format frames to be sent on FDDI as follows:

- Both the Destination Service Access Point (DSAP) and Source Service Access Point (SSAP) values are set to Sub-Network Access Protocol (SNAP) AA hex.
- The Control field is set to U_I (Unnumbered Information), which has a value of 03.
- The Organizationally Unique Identifier (OUI), the first 3 octets of the Protocol Identifier (PID), is set to 00-00-00 (the Ethernet OUI).
- The remaining 2 octets in the PID are set to the Ethernet Protocol Type (PT).

When translating a frame from the FDDI format to the Ethernet format, the process is reversed to allow the generation of an Ethernet format frame from an FDDI frame.

Digital's translating switches ensure that all 802.3/Ethernet frames transferred between pairs of (Digital) switches are retranslated into their original format. A table in each switch contains the PIDs of special protocols that could otherwise be retranslated into the wrong format. The AppleTalk PID is entered into the table by default.

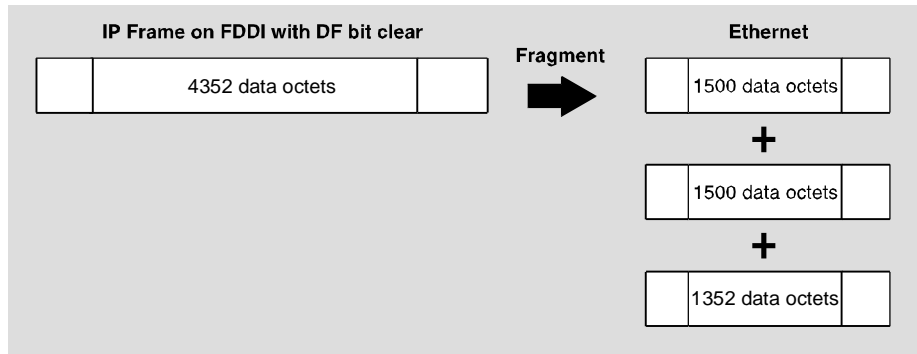
IP Fragmentation

Digital's Ethernet-to-FDDI switches perform IP fragmentation on IP frames received on the FDDI that are to be forwarded on the Ethernet, but are larger than the maximum frame size that Ethernet supports.

The maximum FDDI frame size, including the CRC, is 4495 octets. The maximum Ethernet frame size is 1518 octets. RFC 791, the standard that describes the Internet Protocol, specifies the rules for fragmentation when there is a mismatch in maximum data link size between the source and destination data link.

As shown in the example (see Figure 3-3), Digital's 900 switches break up (fragment) the received frame into legal Ethernet frames in accordance with this specification. An IP header is generated for each of the fragments that are generated, and the destination node reassembles the fragments when received.

Figure 3-3 IP Fragmentation Example



LKG-10131-96C

Note that IP fragments are generated only when the IP fragmentation switch is enabled (by the management software), the Don't Fragment (DF) bit in the IP header is set to Clear, and the IP header is error-free.

Note

The DF bit is set by the station originating the frame.

Although the IP fragmentation switch can be used to *disable* fragmentation, the default setting is *enabled*. If the IP fragmentation switch is enabled, but fragmentation is not occurring, the reason for dropping the IP frames can be detected by examining the IP fragment-related counters. See the documentation on your network management software for more information.

Raw 802.3 IPX Frame Format

Novell stations source two types of IPX frames on CSMA/CD LANs:

1. The normal Ethernet V2.0 format with a Protocol Type (PT) of 81-37.
2. Raw 802.3 frame.

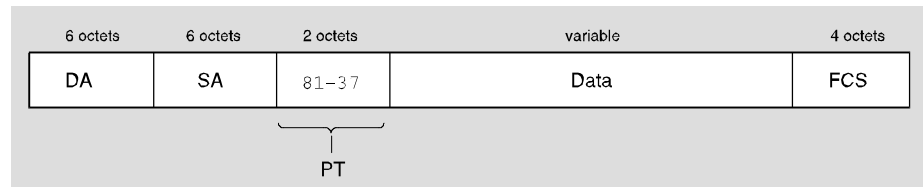
Note

Two other formats (not discussed here) are rarely used but are also sourced by some IPX stations: 802 SAP, and 802 SNAP.

The Raw 802.3 format violates IEEE specifications because it does not contain the standard 802.2 LLC required header. This format is known to cause problems in extended LANs with FDDI components.

It is recommended, whenever possible, to configure IPX stations to use Ethernet V2 format (see Figure 3-4).

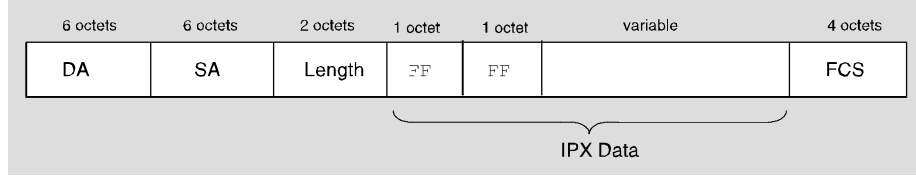
Figure 3–4 Novell IPX: Ethernet V2 Frame Format



LKG-10132-96C

As shown in Figure 3-5, the Raw 802.3 frame does not have the 802.2 LLC header, instead, after the length field on the 802.3 header, it has the IPX (network layer) header.

Figure 3–5 Novell IPX: Raw 802.3 Frame Format

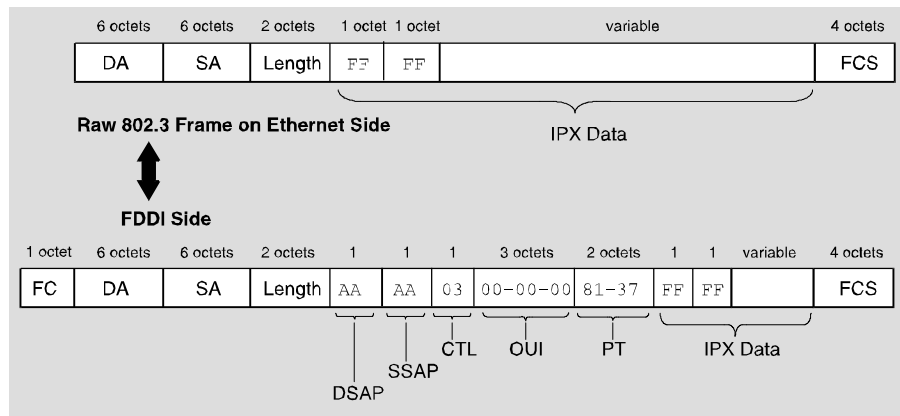


LKG-10133-96C

The first two octets of the IPX header can be used to identify a Raw 802.3 IPX frame. The first two octets of the IPX header (checksum field) are always FF-FF (checksum is disabled in IPX).

IPX translation (see Figure 3-6) involves translating raw 802.3 IPX frames on the Ethernet LAN to SNAP encapsulated frame (RFC 1390) containing a PT of 81-37 on the FDDI side (the opposite is applied from FDDI to Ethernet).

Figure 3–6 Frame Formats when IPX Translation is Enabled



LKG-10134-96C

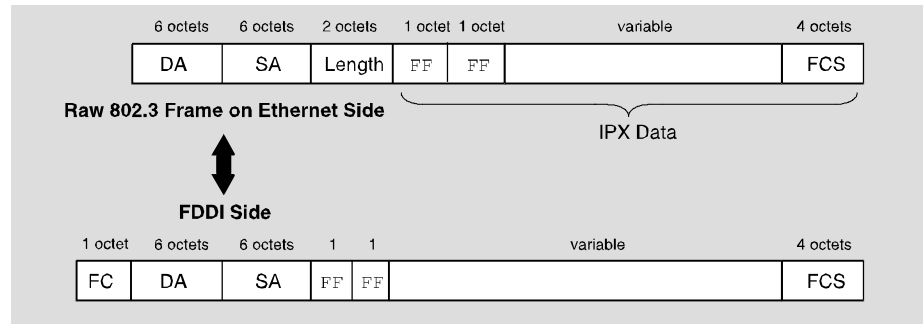
When the switch receives an 802.3 frame while DSAP filtering, it checks the frame's DSAP and SSAP fields. If the field values are FF-FF

(indicating a raw IPX frame), the switch generates a SNAP encapsulated frame on the FDDI with PT of 81-37 (Ethernet protocol type for IPX).

Conversely, when the switch receives a SNAP encapsulated IPX frame from the FDDI that contains a PT of 81-37, the switch converts the frame to a Raw 802.3 IPX frame for transmission to an Ethernet LAN.

IPX translation is disabled by default (see Figure 3-7). It can be enabled via the DEChub setup port or by use of HUBwatch management software.

Figure 3-7 Frame Formats when IPX Translation is Disabled



LKG-10135-96C

AppleTalk Translation

Introduction

Because Apple ARP (one of the protocols related to AppleTalk) does not conform to RFC 1122, it does not operate under the current IEEE 802.1d rules.

On Ethernet, AppleTalk V1 uses Ethernet format frames with a PT value of 80-F3. AppleTalk V2 uses 802 SNAP format frames with a PID value of 00-00-00-80-F3.

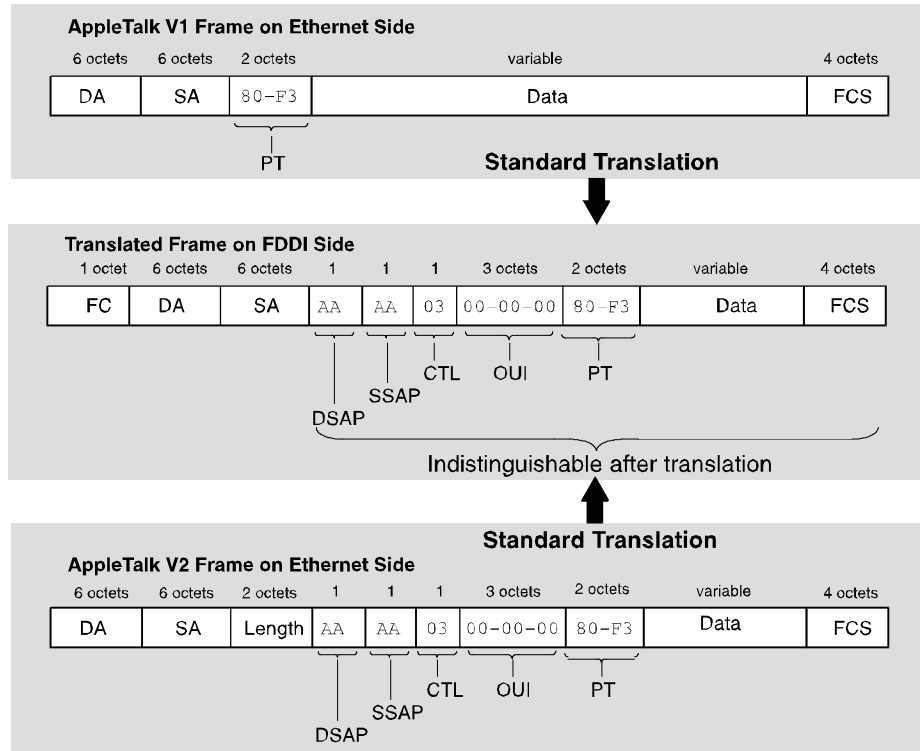
As shown in Figure 3-8, if a frame is translated to FDDI format without formal rules, both frames can translate to SNAP frames with a PID value of 00-00-00-80-F3. These frames are then translated back to Ethernet frames at the second switch (or bridge).

Most protocols that use both formats (for example, TCP/IP) treat Ethernet format frames with a PT of *xx-yy* and 802 SNAP format frames with a PID value of 00-00-00-*xx-yy* as equivalents, as specified by RFC 1122. AppleTalk treats them as two separate protocol versions that are not compatible. The solution is to use special rules when dealing with protocols such as Apple ARP.

Using these special rules, an AppleTalk V1 frame translates, on the FDDI side, to a frame with a PID value of 00-00-F8-80-F3. An AppleTalk V2 frame translates to a frame with a PID value of 00-00-00-80-F3.

At the next switch (bridge), each frame is translated back into its original form and the version information is preserved.

Figure 3–8 Standard Translation



LKG-10136-96C

Standard Ethernet to FDDI Translation

Table 3-2 describes the Standard Ethernet to FDDI translation rules:

Table 3–2 Rules: Standard Ethernet to FDDI Translation

Rule	Description
1	802 format frames traverse the network with the LLC field unchanged.
2	Ethernet format frames are converted into 802 SNAP frames with a Protocol ID consisting of 3 octets of zeros, followed by the Ethernet Protocol Type.

Apple ARP Ethernet-to-FDDI Translation

The 900-series switches are provided with a non-translated protocols (NTP) table that lists protocols which require special handling. Normally, the NTP table contains a single entry: the protocol type for Apple ARP (80-F3).

Switches that are provided with the NTP table use the following rules (see Tables 3-3 and 3-4) for translating between Ethernet and FDDI formats:

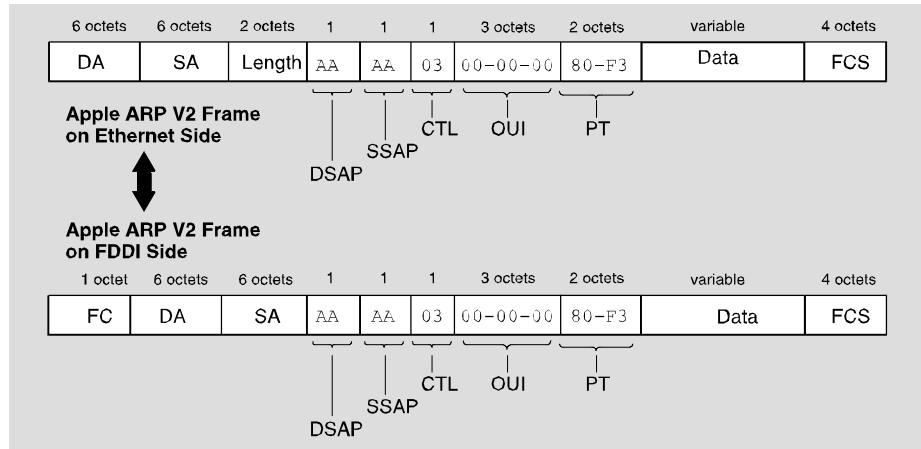
Table 3-3 Rules: Ethernet to FDDI Translation

Rule	Description
1	802.3 format frames traverse the network with the LLC field unchanged (see Figure 3-9).
2	For Ethernet frames, look up the Protocol Type (PT) in the NTP table: If the PT is found in the NTP table, translate to a SNAP frame with Protocol ID (PID) of 00-00-F8 followed by the PT (see Figure 3-10). Otherwise, translate to a SNAP frame with PID of 00-00-00 followed by the PT in the Ethernet frame.

Table 3-4 Rules: FDDI to Ethernet Translation

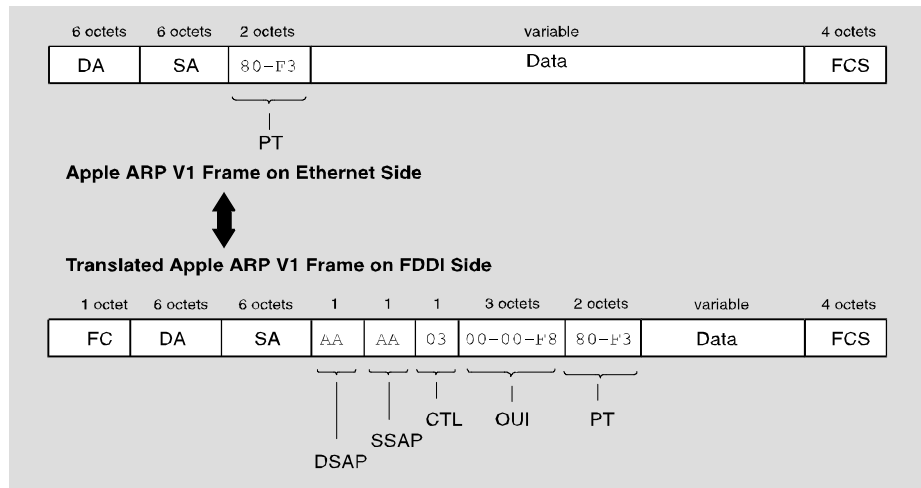
Rule	Description
1	If the frame is SNAP with Protocol ID (PID) beginning with 00-00-F8, translate to Ethernet format (see Figure 3-10).
2	If the frame is SNAP with PID beginning with 00-00-00, check to see if the last two octets of the PID are in the special handling table. If not, translate to Ethernet format. If it is in the table, leave the frame as an 802 format frame (see Figure 3-9).
3	All other frames traverse the network with the LLC field unchanged.

Figure 3-9 Apple ARP V2 Translation



LKG-10137-96C

Figure 3-10 Apple ARP V1 Translation



LKG-10138-96C

Rate Limiting

Introduction

Uncontrolled rates of broadcast and multicast traffic (broadcast storms) place severe strain on network connectivity. Broadcast storms can use up so much bandwidth that the network effectively becomes unusable — nodes, overcome with excessive traffic, are prevented from communicating information on the network.

While it is rare to see an indefinite broadcast storm, it is fairly common for lengthy peaks (several seconds to minutes) to occur in medium- to large-sized networks.

Curbing Broadcast Storms

Digital's 900 switches include a feature called *rate limiting* that curbs the harmful effects of broadcast storms. Specified multicast addresses can be included in the rate limit category. Also, specified protocols (Ethernet PT, SAP or SNAP) can be included in the rate limit if they occur in any multicast frame. Finally, the rate limit can be set in packets-per-second (pps) with a granularity of 100 pps.

Digital's 900 switches do not forward frames in excess of the preset rate limit for specified frames. This feature regulates further propagation of this traffic into the extended LAN by eliminating the peaks of this traffic while forwarding, thus isolating it to the LAN on which the storm originates.

Frame Filtering/Forwarding

Introduction

The 900-Series switches offer the following types of filtering:

- Destination Address Filtering
- Source Address Filtering
- Manual mode/Secure mode
- Protocol Filtering
- Unknown-Protocol Filtering

Destination Address Filtering

Destination address filtering decreases network traffic by keeping local traffic local and only forwarding frames that are destined for the opposite side of the switch.

Each switch has an address database that contains addresses of stations connected to its LANs. When the switch detects a frame on any of its attached LANs, it checks the destination address of that frame against the addresses stored in its database.

If the frame is addressed to a node that has an address that was learned on the *same port* of the switch, the switch filters the frame (it does not forward it to the other switch ports).

Address information can enter the database in either of two ways:

1. **Listening/Learning** — the switch listens to network traffic and acquires a working knowledge of the nodes that are connected to its LAN ports.

It acquires this knowledge by reading the source address of each incoming frame and noting which of the LAN ports that source is located.

2. **Switch Management** — the address database can also receive entries from switch management.

By specifying a station address and the port number of the switch where that station is located, you can lock that station to that port. This creates a permanent address for that node and causes the switch to ignore any learned information that differs from this permanent address.

Address filtering can be used in an inclusive or an exclusive fashion. For example, if you specify a set of node addresses for address filtering, you can have the switch filter messages to those nodes and forward messages to all other nodes (if no other filters match), or you can have the switch forward messages only to those nodes (if no other filters match) and filter messages to all other nodes (manual mode).

Source Address Filtering

Using switch management, you can prevent all frames emanating from a specified node from being forwarded to the other ports of the switch (regardless of their destination address).

Source address filtering can also be used to lock down a specified source node to one side of the switch. This protects against masquerading nodes.

For example, consider a secure station (Station A) that is known to be on switch port 2. In order to prevent stations on other LANs from masquerading as station A, switch management can be used to lock-down station A on switch port 2.

Switch management can also be used to channel all broadcast and multicast traffic to a backbone port.

For example, suppose your servers are on the FDDI backbone and you don't want the Ethernet LAN's multicast address to go to any of the other Ethernets. In this case, you could lock down a multicast or broadcast address to the FDDI backbone by defining an address filter that allows this address on the FDDI port only. This filter prevents multicast or broadcast frames from flooding any of the other Ethernet ports.

Manual Mode/Secure Mode

The switch can be set to manual mode (also known as secure mode) on an arbitrary set of ports. When in manual mode, the switch shuts off its learning capability on the specified set of ports and forwards frames based only on the address and protocol filters configured by management.

It is important to note that manual mode filtering can be specified on a per port basis. If a port has been placed into manual mode and a packet is attempting to *enter* the switch on that port, the packet's source address (SA) is compared to the list of addresses that was manually loaded by the network manager. If the address is found in the table, the packet will be forwarded (if no protocol filter is in effect to block it); if the address is not found, the packet is blocked from entering the switch. On the other hand, if a packet is attempting to *exit* the switch at that port, its destination address (DA) is compared to the list of addresses that was manually loaded, and, if a match is found, the packet will be forwarded; otherwise, the packet is discarded.

Manually-loaded address entries are never aged out of the learning tables. They are permanently stored in the table until the network manager explicitly removes them. This is true for all manually-entered addresses—whether the port is in manual mode (address learning turned off) or auto-learning mode (standard bridge learning).

Protocol Filtering

Switch management can also be used to prevent specified protocols from being forwarded across the switch.

Protocol filtering can be used in an inclusive or an exclusive fashion. For example, if you specify the Local Area Transport (LAT) protocol for protocol filtering, you can have the switch filter only LAT protocol messages and forward all other protocols (if no other filters match), or you can have the switch forward only LAT protocol messages (if no other filters match) and filter all others.

Switches can be set to restrict an Ethernet Protocol type, an 802 DSAP, or an 802 SNAP PID to a set of allowed ports. Frames containing these protocols are only forwarded if both of the following situations are true:

- The source port is in the set of allowed ports for the protocol
- The destination port is also in the set of allowed ports for the protocol.

Note that filtering always takes precedence over forwarding.

For example, if you specify that the switch always forward messages to a particular destination address (for example, node Z), and you also specify that the switch always filter LAT protocols, then any LAT protocol message that is destined for node Z will be filtered. The switch will only forward a frame if no filters are set to filter that frame.

Unknown-Protocol Filtering

Using switch management, you can set the switch to filter or forward on any port, any protocol that does not match a configured protocol filter. By default, a switch will forward an unknown protocol

Managing Switches with HUBwatch

Introduction

HUBwatch is a flexible, network configuration and management application that provides a graphical user interface (GUI). HUBwatch manages network modules installed in a hub as well as the hub itself.

To communicate management and configuration commands to network modules, HUBwatch sends Simple Network Protocol (SNMP) commands to SNMP agents in the network modules or in the hub itself.

Although it is possible to use SNMP commands with any vendor's management station, HUBwatch makes it easy to manage the switches by use of customized window displays.

What You Can Do With HUBwatch

You can use HUBwatch software to:

- View the status and activity of network modules and ports
- Configure LANs on the hub backplane
- Monitor the flow and accuracy of network data
- Configure network modules

How You Use HUBwatch

You can perform the general steps outlined in the table below to manage a DEChub 900 MultiSwitch or a DEChub 90 with installed modules:

Step	Action	Result
1	Run the Application (using the appropriate Hub IP address.)	HUBwatch displays the Hub Front Panel Window. This window shows the modules installed in the hub and indicates their status. It also provides selectable items in a menu bar across the top of the window.
2	Click on an item on the Hub Front Panel menu bar.	HUBwatch presents options in a pulldown menu, enabling you to choose an option applicable to the management task that you wish to perform.
3	Click on an option from the pulldown menu	HUBwatch presents a window in which you can perform the desired management tasks. For example, you can invoke the HUBloader utility in this manner from the Applications pulldown menu to update DEChub firmware
4	Alternatively, double click on a displayed module (such as a DECswitch 900 module) or one of its ports.	.This brings up a module-specific window.
5	Click on an icon displayed in a module-specific window.	HUBwatch displays a subordinate window that allows you to perform additional management tasks for the selected module.

900 Switch Family Windows

The HUBwatch windows include the following information for managing the 900 switch family:

HUBwatch Window	Description
Hub Front Panel	Front panel representation of the hub and installed network modules, including status and port LEDs. Double click on a switch module in the front panel view to open the Switch Summary window.
Switch Summary	Provides key overall, as well as per-port information for the switch. Allows you to set the root priority and port cost for the spanning tree.
Switch Port Information	Provides information related to counters (datalink-independent and datalink-dependent), Ethernet port, and FDDI port information.
FDDI Summary	Provides detailed information specific to the FDDI interface — SMT, Port, and MAC.
Forwarding Database	Use this window for locating where a specific MAC address, IP address, or DECnet address resides.
Address Filter	Allows configuration of filtering rules for destination address (DA) and source address (SA), manual or secure mode for each port (for disabling learning), and rate limiting for multicast addresses.
Protocol Filter	Allows configuration of filtering rules for Ethernet protocol types: 802.DSAP, 802 SNAP or PID; rate limiting for any of these protocols when used in multicast frames; default protocol filtering action for each port.

(Continued on next page.)

HUBwatch Window	Description
Switch Configuration	Provides configuration settings of various switch parameters, such as: rate limit, spanning tree parameters, raw 802.3 IPX switch.
Station Configuration	Used to configure the switch's ports to point to the hub backplane rather than the switch's front panel. This configuration must be done before connecting the port to the specific backplane LANs.
LAN Interconnect	For connection of the switch's ports into any of the backplane LANs set up in the hub. Also for creating and deleting backplane LANs.

For More Information

Topic...	Where to Get More Information...
Using HUBwatch windows	Chapter 4, Managing the 900 Family of Switches, provides a listing of task-based examples that are most often required by network and system managers. Each task description includes the appropriate SNMP MIB object (where applicable) that can be used by non-HUBwatch users.

Out-of-Band Management (OBM)

Introduction

You can use out-of-band management (OBM) facilities to manage DEChub 900 network modules that are installed into a DEChub ONE, DEChub ONE-MX, or DEChub 900 MultiSwitch. These hubs have an OBM port that facilitates an alternative to in-band management products. Thus, if the network providing the in-band connection fails, you can still use HUBwatch to manage devices on the network by sending SNMP requests over Serial Line Internet Protocol (SLIP) via the OBM port.

Note that Open VMS systems do not support SLIP connections directly. Such connections must be made through an access server (DECserver).

The out-of-band management method offers the same functionality as in-band management, except that it is slower and you assign an OBM IP address and the OBM port speed via the HUB setup menu. If you want to switch from managing in-band to managing out-of-band, select the OBM IP address in HUBwatch.

OBM Port and Slip

The OBM Port allows you to manage network modules with HUBwatch over SLIP using a modem, or a direct connection to the OBM port. If your network management application supports PING echo, you can use it to verify the SLIP connection. Typically, you use PING echo to verify that your network connection is operational.

You can also manage DEChubs by establishing a connection from HUBwatch to an access server that supports SLIP. If you have a DECserver 900GM, DECserver 900TM, DECserver 90TL, or a DECserver 90M installed in your hub, you can establish a SLIP connection between one of the access server ports and the Hub Manager OBM port.

For More Information

Topic...	Where to Get More Information...
Setting up SLIP Connections	Refer to Appendix B of the <i>HUBwatch Installation and Configuration Manual</i> .
Cable and adapter Information	Refer to the <i>DEChub 900 MultiSwitch Owner's Manual</i> .

Chapter 4

Managing the 900-Series Switches

Overview

Introduction

This chapter shows how to use switch-specific HUBwatch windows to perform common network management tasks. It provides an overview of the windows and lists each task as a separate heading. Each task description includes the appropriate SNMP MIB object (where applicable) that can be used by non-HUBwatch users.

In This Chapter

The following topics are covered in this chapter:

Topic	See page...
Switch-specific HUBwatch Windows	4-3
Switch Summary Window	4-7
Enabling and Disabling Forwarding on Ports	4-9
Enabling and Disabling the Spanning Tree Algorithm on Ports	4-10

(Continued on next page.)

Topic	See page...
Setting LB100 Compatibility	4-12
Enabling and Disabling Raw 802.3 IPX Translation	4-14
Enabling and Disabling IP Fragmentation	4-16
Enabling and Disabling Rate Limiting	4-18
Setting the Rate Limit	4-20
Setting the Bridge Hello Time	4-23
Setting the Bridge Max Age	4-26
Setting the Bridge Forward Delay	4-29
Setting the No Frame Interval	4-32
Setting the Aging Time	4-33
Setting the Short Aging Time	4-35
Setting the Gateway Address	4-37
Adding and Deleting Trap Addresses	4-39
Creating Address Filters	4-42
Modifying Address Filters	4-46
Creating a Default Filter for all Unspecified Addresses	4-52
Creating Protocol Filters	4-54
Modifying Protocol Filters	4-57
Specifying Default Protocol Filters	4-63
Adding Protocols Not in the Available Protocols List	4-65
Deleting Address and Protocol Filters	4-68
Writing Contents of Forwarding and Filters Database to Files	4-71

Switch-Specific HUBwatch Windows

Introduction

You can use the windows listed in the following table to manage the 900-series switches and bridges. The table describes the windows and their associated tasks.

Window-Task Table

Use this window...	To...
Hub Front Panel	Observe and interpret LEDs.
Switch Summary	Display or assign the switch description. Display switch status information. Display management agent information. Display Spanning tree attributes. Display port attributes and status. Enable or disable forwarding on ports. Enable or disable the spanning tree algorithm on ports. Reset the switch. Reset the switch to factory defaults.
Switch Port Information	Display port counters. Display switch configuration changes.

(Continued on next page.)

Use this window...	To...
Forwarding Database	Display forwarding database counters. Locate a node. Write the contents of the forwarding database to a file.
Address Filters	Create address filters. Modify address filters. Delete address filters. Place a port in manual mode. Save the current list of address filters to a file. Display the most recent port where an address last appeared, for each address. Enable or disable rate-limiting on a multicast address.
Protocol Filters	Create protocol filters. Modify protocol filters. Delete protocol filters. Create default protocol filters. Save the current list of protocol filters to a file. Enable or disable rate-limiting on a protocol.

(continued on next page.)

Use this window...	To...
FDDI Summary	Display FDDI information.
Switch Configuration	Set switch configuration parameters. Set the Gateway address Add or remove trap addresses.
Station Configuration	Configure FDDI ports as ring (A/B) or tree (M/S) ports. Configure ports to point to the module front panel or to the backplane.
LAN Interconnect Expanded View	Create a LAN Segment Connect switch ports to LAN Segments. Disconnect switch ports from LAN segments. Delete a LAN segment. Modify a network segment's characteristics.

Opening Switch Windows

The following table describes how to open any HUBwatch switch window:

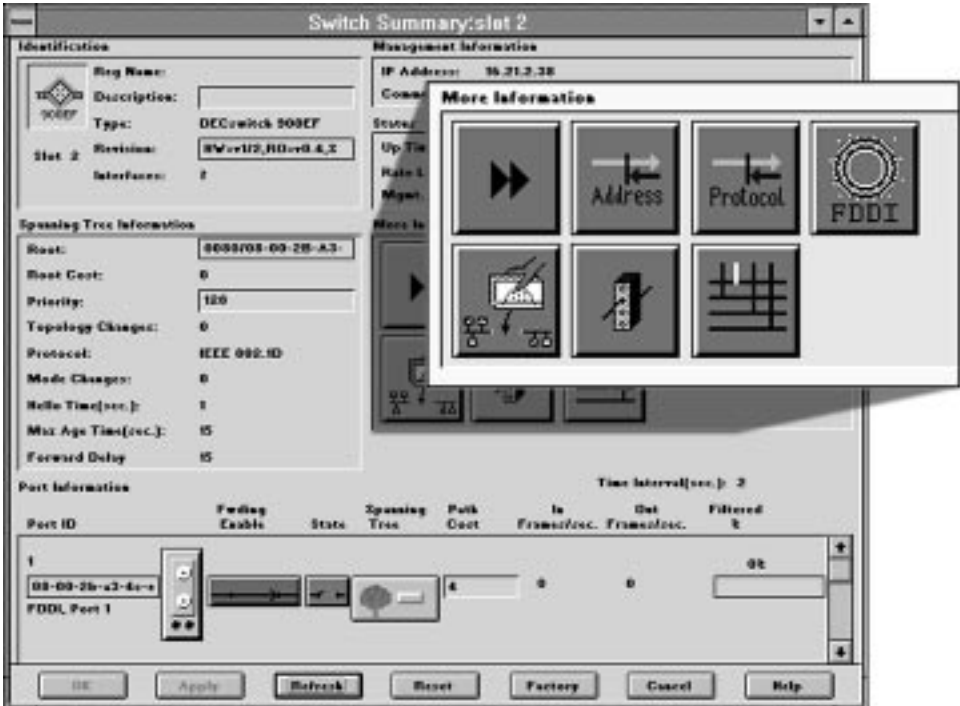
To open this window...	Do this...
Switch Summary	From the Hub Front Panel window, double-click on the switch module. Use the buttons in the Switch Summary window More Information box to reach other windows.
Switch Port Information	From the Switch Summary window, click on any port connector. or From the HUB Front Panel, Physical view, double click on any port connector. or From the Hub Front Panel, Logical View, click on any port button.

Switch Summary Window

Introduction

The More Information box, located in the Switch Summary window (see Figure 4-1), provides a set of click buttons that can be used to access other switch management windows. The buttons are labeled with icons that identify the management function of the various windows you can access (see Table 4-1).








Figure 4-1 Switch Summary Window



Online Help

Click on the Help button at the bottom of any HUBwatch window to open a help topic. Help topics provide details about the current window and provide help for performing management tasks.

Table 4–1 Switch Summary Window Buttons

Button	Description
	Forwarding Database — Click on this button to open the Forwarding Database window.
	Address Filters — Click on this button to open the Address Filters window.
	Protocol Filters — Click on this button to open the Protocols Filters window.
	FDDI Summary — Click on this button to open the FDDI Summary window.
	Switch Configuration — Click on this button to open the Switch Configuration window.
	Station Configuration — Click on this button to open the Station Configuration window.
	LAN Interconnect Expanded View — Click on this button to open the LAN Interconnect window.

Task List

The remainder of this chapter describes how to perform various network management tasks that are listed at the beginning of this chapter. Note that the task description includes the associated SNMP MIB objects, for non-HUBwatch users.





Enabling and Disabling Forwarding on Ports

Overview

This feature allows you to enable or disable forwarding on a selected port. When forwarding is disabled on a port, any frames received on the port (except SNMP requests addressed to the switch) are discarded, and no frames are transmitted on the port.

How to Enable or Disable Ports

To enable or disable forwarding on a port, complete the following steps:

Step	Action
1	Open the Switch Summary window.
2	Click on the port's Fwding Enabled/Disabled button in the Port Information box.
	 Fwding Enable
	 Fwding Disable
3	Click the Apply button to apply the change.
	 Apply button
	Click the OK button to apply the change and close the window.
	 OK button

Relevant SNMP MIB Object

MIB Object...	Where to get more information...
dot1dStpPortEnable	See, RFC 1493: Bridge MIB.

Enabling and Disabling the Spanning Tree Algorithm on Ports

Overview




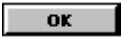
This feature allows you to disable the spanning tree algorithm that is running on a port. This allows you to set up multiple spanning tree domains within a single extended LAN. When the spanning tree algorithm is disabled on a port, the port transitions to the Forwarding State and no longer transmits or receives spanning tree hellos.

Note

If you disable the spanning tree algorithm that is running on a port, you must ensure that no loops exist between the domains. Loops existing between domains cannot be automatically detected while the spanning tree is disabled.

How to Enable or Disable the Spanning Tree Algorithm on a Port

To enable or disable the spanning tree algorithm on a port, complete the following steps:

Step	Action
1	Open the Switch Summary window.
 Spanning Tree Enabled	2 Click, and hold, the port's spanning tree button in the Port Information box until the opposite icon appears.
 Spanning Tree Disabled	Slide the cursor to the appropriate icon, then release the cursor.
 Apply button	3 Click the Apply button to apply the change.
 OK button	4 Click the OK button to apply the change and close the window.

Relevant SNMP MIB Object

MIB Object...	Where to get more information...
ebrIfSpanTurnOffStatus	See, ELAN (DEC Vendor) MIB.

For More Information

Topic...	Where to Get More Information...
Spanning Tree mode options.	See, Setting the LB100 Compatibility.
Spanning Tree Algorithm	See, Appendix C

Setting LB100 Compatibility

Overview

Switches or bridges that have the AutoSelect feature (such as the DECswitch 900 models and the PEs switch 900TX model) can interpret both LAN Bridge 100 and 802.1d Hello messages. Thus, AutoSelect switches or bridges can be combined with either LAN Bridge 100 bridges or IEEE 802.1d bridges in an extended LAN.

An AutoSelect switch or bridge can run either of the spanning tree modes discussed in the following section, but can only use one at any given time. It can change to the other mode, if required to, but it cannot be in both spanning tree modes at the same time.

The LB 100 Compatibility parameter determines the method of selecting the spanning tree mode.

Spanning Tree Mode Options

There are two options for selecting the spanning tree modes:

1. AutoSelect





When set to AutoSelect mode, the switch or bridge uses the IEEE 802.1d implementation of the spanning tree by default, but switches to LAN Bridge 100 (LB100) mode when it detects the presence of a LAN Bridge 100 in the extended LAN.

2. IEEE 802.1d (default)

When set to IEEE 802.1d, the switch or bridge is locked into this mode permanently.

How to Set the LB100 Compatibility

To set the LB100 compatibility, complete the following steps:

Step	Action
 Switch Configuration button	1 Click on the Switch Configuration button in the Switch Summary window. The Switch Configuration window opens.
 Select button	2 Click the Select button to choose IEEE802 or AutoSelect in the LB100 Compatibility: field of the Configuration box.
 Apply button	3 Click the Apply button to apply the change.
	or
 OK button	Click the OK button to apply the change and close the window.

Relevant SNMP MIB Object

MIB Object...	Where to get more information...
ebrLB100SpanningTreeComp	See, ELAN (DEC Vendor) MIB.

Enabling and Disabling Raw 802.3 IPX Translation

Overview





This mode determines whether or not raw 802.3 IPX frames are translated into SNAP encapsulated frames on an FDDI network. This mode is valid only for networks where all IPX stations use the raw 802.3 IPX frame format exclusively.

Recommendation

Digital recommends that IPX stations use the Ethernet Version 2 format for full connectivity of IPX stations across Ethernet networks and FDDI bridged and routed networks.

How to Enable or Disable Raw 802.3 IPX Translation

To enable or disable raw 802.3 IPX translation, complete the following steps:

	Step	Action
 Switch Configuration button	1	Click on the Switch Configuration button in the Switch Summary window. The Switch Configuration window opens.
 Select button	2	Click the Select button to choose Enabled or Disabled in the Raw 802.3 IPX: field of the Configuration box.
 Apply button	3	Click the Apply button to apply the change. or
 OK button		Click the OK button to apply the change and close the window.

Relevant SNMP MIB Object

MIB Object...	Where to get more information...
esysIPXSwitch	See, ELAN (DEC Vendor) MIB.

For More Information

Topic...	Where to Get More Information...
IPX Translation	See, Raw 802.3 IPX Frame Format, in Chapter 3.

Enabling and Disabling IP Fragmentation

Overview



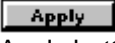

You can control the fragmentation of Internet Protocol (IP) frames on the DECswitch 900EF and the PEs switch 900TX network modules. These switches can be set to break up (fragment) large IP frames that are received on their FDDI lines into smaller frames that can be transmitted onto their IEEE 802.3/Ethernet lines.

The fragmentation of IP frames is necessary because only 1518 bytes are allowed for a frame on an IEEE 802.3/Ethernet segment, whereas a frame on an FDDI ring can be up to 4500 bytes.

When IP Fragmentation is enabled, the bridge or switch performs fragmentation whenever it receives an IP frame from an FDDI station that will not fit into a single Ethernet frame after translation.

How to Enable or Disable IP Fragmentation

To enable or disable IP Fragmentation, complete the following steps:

Step	Action
 Switch Configuration button	1 Click on the Switch Configuration button in the Switch Summary window. The Switch Configuration window opens.
 Select button	2 Click the Select button to choose Enabled or Disabled in the IP Fragmentation: field of the Configuration box.
 Apply button	3 Click the Apply button to apply the change. or
 OK button	Click the OK button to apply the change and close the window.

Relevant SNMP MIB Object

MIB Object...	Where to get more information...
ebrFragmentationSwitch	See, ELAN (DEC Vendor) MIB.

For More Information

Topic...	Where to Get More Information...
IP fragmentation	See, IP Fragmentation, in Chapter 3.

Enabling and Disabling Rate Limiting

Overview

This section describes how to enable or disable the Rate Limit value parameter for specified addresses and protocols.

Rate-limiting allows you to determine the maximum rate at which specified multicast frames are forwarded by the switch or bridge. You can specify any multicast frame by multicast address or by protocol. This option is useful, for example, when you want to limit the spread of broadcast storms on an extended LAN.

The Rate Limit Value





If rate limiting is in effect, the rate limit will be the value you specify for the rate limit (frames/sec) parameter. The rate limit is the total number of frames, for all specified multicast addresses and protocols, allowed per second.

For the rate limit to take effect, you must complete the following steps:

Step	Action
1	Select the addresses or protocols for which you want to set a rate limit: <ul style="list-style-type: none">• If you need help in selecting an address for rate limiting, see the sections titled Creating Address Filters and Modifying Address Filters.• If you need help in selecting a protocol for rate limiting, see the sections titled Creating Protocol Filters and Modifying Protocol Filters.
2	Set the rate limit by completing the steps in the section titled How to Set the Rate Limit .
3	Enable rate limiting on the specified addresses or protocols as described in the following section titled, How to Enable or Disable Rate Limiting .

How to Enable or Disable Rate Limiting

To enable or disable Rate Limiting for the switch or bridge, complete the following steps:

Step	Action
 <p data-bbox="282 541 444 632">Switch Configuration button</p>	<p data-bbox="477 417 1388 478">1 Click on the Switch Configuration button in the Switch Summary window.</p> <p data-bbox="574 541 1084 575">The Switch Configuration window opens.</p>
 <p data-bbox="282 695 444 722">Select button</p>	<p data-bbox="477 653 1388 722">2 Click the Select button to choose Enabled or Disabled in the Rate Limiting: field of the Configuration box.</p>
 <p data-bbox="282 785 444 812">Apply button</p>	<p data-bbox="477 743 1388 783">3 Click the Apply button to apply the change.</p> <p data-bbox="688 806 716 827">or</p>
 <p data-bbox="282 896 406 924">OK button</p>	<p data-bbox="574 854 1388 884">Click the OK button to apply the change and close the window.</p>

Relevant SNMP MIB Object

MIB Object...	Where to get more information...
ebrRateLimitSwitch	See, ELAN (DEC Vendor) MIB.

For More Information

Topic...	Where to Get More Information...
Selecting an address for rate limiting.	See, Creating Address Filters; and Modifying Address Filters.
Selecting a protocol for rate limiting.	See, Creating Protocol Filters; and Modifying Protocol Filters.
Setting the switch rate limit.	See, Setting the Rate Limit.
Rate limiting	See, Rate Limiting, in Chapter 3.

Setting the Rate Limit

Overview

The Rate Limit parameter is the maximum total number of multicast frames, for all rate-limited addresses and protocols, that are allowed to be forwarded per second. This section describes how to set the Rate Limit parameter to suit your needs.

For the rate limit to take effect, you must complete the following steps:

Step	Action
1	Select the addresses or protocols for which you want to set a rate limit: <ul style="list-style-type: none">• If you need help in selecting an address for rate limiting, see the sections titled <i>Creating Address Filters</i> and <i>Modifying Address Filters</i>.• If you need help in selecting a protocol for rate limiting, see the sections titled <i>Creating Protocol Filters</i> and <i>Modifying Protocol Filters</i>.
2	Set the rate limit by completing the steps in the following section titled <i>How to Set the Rate Limit</i> .
3	Enable rate limiting on the addresses or protocols (if you need help, see the section titled <i>Enabling and Disabling Rate Limiting</i>).

How to Set the Rate Limit

To set the Rate Limit for the switch or bridge, complete the following steps:



Switch Configuration button

Step	Action
------	--------

- | | |
|---|--|
| 1 | Click on the Switch Configuration button in the Switch Summary window. |
|---|--|

The Switch Configuration window opens.

- | | |
|---|--|
| 2 | Click on the Rate Limit (frame/secs) : scale slider in the Configuration box, drag the slider to select the appropriate value, and release it. |
|---|--|

Note

The rate limit can be selected with a granularity of 100 frames/second.



Apply button

- | | |
|---|--|
| 3 | Click the Apply button to apply the change. |
|---|--|

or



OK button

Click the **OK** button to apply the change and close the window.

Important

The rate limit will not take effect unless rate limiting is enabled.

Relevant SNMP MIB Object

MIB Object...	Where to get more information...
ebrRateLimit	See, ELAN (DEC Vendor) MIB.

For More Information

Topic...	Where to Get More Information...
Selecting an address for rate limiting.	See, Creating Address Filters; and Modifying Address Filters.
Selecting a protocol for rate limiting.	See, Creating Protocol Filters; and Modifying Protocol Filters.
Enabling or disabling the switch or bridge rate limiting.	See, Enabling and Disabling Rate Limiting.
Rate limiting	See, Rate Limiting, in Chapter 3.

Setting the Bridge Hello Time

Overview

When the current switch or bridge is the root, the Bridge Hello Time determines the interval, in seconds, that all switches and bridges in the spanning tree use for the time between hello messages.

The Bridge Hello Time parameter differs from the Hello Time parameter. The Bridge Hello Time is significant only if the switch, or bridge, becomes the root. If so, the Bridge Hello Time value is administrated to all switches and bridges in the spanning tree and becomes the operational value. The current operational value is reported as the Hello Time parameter by all switches and bridges in the extended LAN.

When you change the Bridge Hello Time, you may also have to change the Bridge Max Age. And when you change the Bridge Max Age, you may also have to change the Bridge Forward Delay.

Note

Entering a value that makes the current value for the Bridge Max Age or Bridge Forward Delay invalid generates an error message.

Default Values

In the following table, the default values are designed to meet the requirements of extended LANs with up to seven switches or bridges (the maximum) between any two LANs. The minimum values are valid only for an extended LAN on which there is no more than one switch, or bridge, between any two LANs.

Parameter	Default	Minimum
Bridge Hello Time	1	1
Bridge Max Age	15	7
Bridge Forward Delay	15	5

Recommendation

Digital recommends that you use the defaults for these parameters, because they are designed to meet the requirements of the maximal network configuration in which the switch or bridge can be placed.

How to Set the Bridge Hello Time

To set the Bridge Hello Time, complete the following steps:



Switch Configuration button

Step	Action
1	Click on the Switch Configuration button in the Switch Summary window. The Switch Configuration window opens.
2	Click in the Bridge Hello Time (secs): field in the Configuration box
3	Enter a value from 1 to 9 (see Note).

Note

The values for the Bridge Max Age, Bridge Hello Time, and Bridge Forward Delay must satisfy the following relationships to be considered valid:

$$2 \times (\text{Bridge_Forward_Delay} - 1.0 \text{ seconds}) \geq \text{Bridge_Max_Age}$$

$$\text{Bridge_Max_Age} \geq 2 \times (\text{Bridge_Hello_time} + 1.0 \text{ seconds})$$



Apply button



OK button

4	Click the Apply button to apply the change. or Click the OK button to apply the change and close the window.
---	--

Relevant SNMP MIB Object

MIB Object...	Where to get more information...
dot1StpBridgeHelloTime	See, RFC 1493: Bridge MIB.

For More Information

Topic	Where to Get More Information
Changing the Bridge Max Age	See, Setting the Bridge Max Age
Changing the Bridge Forward Delay	See, Setting the Bridge Forward Delay
Spanning tree	See, Appendix C.

Setting the Bridge Max Age

Overview

When the current switch or bridge is the root, the Bridge Max Age is the interval, in seconds, after which all switches and bridges in the spanning tree consider a Hello message to be stale.

The Bridge Max Age parameter differs from the Max Age Time parameter. The Bridge Max Age is significant only if the switch or bridge becomes the root. If so, the Bridge Max Age value is administrated to all switches and bridges in the spanning tree and becomes the operational value. The current operational value is reported as the Max Age Time parameter by all switches and bridges in the extended LAN.

When you change the Bridge Hello Time, you may also have to change the Bridge Max Age. And when you change the Bridge Max Age, you may also have to change the Bridge Forward Delay.

Note

Entering a value that makes the current value for the Bridge Hello Time or the Bridge Forward Delay invalid generates an error message.

Default Values

In the following table, the default values are designed to meet the requirements of extended LANs on which there are up to seven bridges or switches (the maximum) between any two LANs. The minimum values are valid only for an extended LAN on which there is no more than one bridge between any two LANs.

Parameter	Default	Minimum
Bridge Hello Time	1	1
Bridge Max Age	15	7
Bridge Forward Delay	15	5

Recommendation

Digital recommends that you use the defaults for these parameters, since they are designed to meet the requirements of the maximal network configuration in which the bridge or switch can be placed.

How to Set the Bridge Max Age

To set the Bridge Max Age, complete the following steps:



Switch Configuration button

Step	Action
1	Click on the Switch Configuration button in the Switch Summary window. The Switch Configuration window opens.
2	Click in the Bridge Max Age (secs): field in the Configuration box
3	Enter a value from 7 to 40 (see Note).

Note

The values for the Bridge Max Age, Bridge Hello Time, and Bridge Forward Delay must satisfy the following relationships to be considered valid:

$$2 \times (\text{Bridge_Forward_Delay} - 1.0 \text{ seconds}) \geq \text{Bridge_Max_Age}$$

$$\text{Bridge_Max_Age} \geq 2 \times (\text{Bridge_Hello_time} + 1.0 \text{ seconds})$$



Apply button



OK button

4	Click the Apply button to apply the change. or Click the OK button to apply the change and close the window.
---	--

Relevant SNMP MIB Object

MIB Object...	Where to get more information...
dot1StpBridgeMaxAge	See, RFC 1493: Bridge MIB.

For More Information

Topic	Where to Get More Information
Changing the Bridge Hello Time.	See, Setting the Bridge Hello Time.
Changing the Bridge Forward Delay.	See, Setting the Bridge Forward Delay.
Spanning tree.	See, Appendix C.

Setting the Bridge Forward Delay

Overview

When the current switch or bridge is the root, the Bridge Forward Delay is the interval, in seconds, that a port remains in each of the Listening states and the Learning states before entering the Forwarding state.

The Bridge Forward Delay parameter differs from the Forward Delay parameter. The Bridge Forward Delay is significant only if the switch or bridge becomes the root. If so, the Bridge Forward Delay value is administrated to all switches and bridges in the spanning tree and becomes the operational value. The current operational value is reported as the Forward Delay parameter by all switches and bridges in the extended LAN.

When you change the Bridge Hello Time, you may also have to change the Bridge Max Age. And when you change the Bridge Max Age, you may also have to change the Bridge Forward Delay.

Note

Entering a value for this parameter that makes the current value for the Bridge Hello Time or the Bridge Max Age parameter invalid generates an error message.

Default Values

In the following table, the default values are designed to meet the requirements of extended LANs on which there are up to seven switches or bridges (the maximum) between any two LANs. The minimum values are valid only for an extended LAN on which there is no more than one switch, or bridge, between any two LANs.

Parameter	Default	Minimum
Bridge Hello Time	1	1
Bridge Max Age	15	7
Bridge Forward Delay	15	5

Recommendation

Digital recommends that you use the defaults for these parameters, since they are designed to meet the requirements of the maximal network configuration in which the bridge or switch can be placed.

How to Set the Bridge Forward Delay (secs)

To set the Bridge Forward Delay, complete the following steps:



Switch Configuration button

Step	Action
1	Click on the Switch Configuration button in the Switch Summary window. The Switch Configuration window opens.
2	Click in the Bridge Forward Delay (secs): field in the Configuration box
3	Enter a value from 5 to 30 (see Note).

Note

The values for the Bridge Max Age, Bridge Hello Time, and Bridge Forward Delay must satisfy the following relationships to be considered valid:

$$2 \times (\text{Bridge_Forward_Delay} - 1.0 \text{ seconds}) \geq \text{Bridge_Max_Age}$$

$$\text{Bridge_Max_Age} \geq 2 \times (\text{Bridge_Hello_time} + 1.0 \text{ seconds})$$



Apply button



OK button

4	Click the Apply button to apply the change. or Click the OK button to apply the change and close the window.
---	--

Relevant SNMP MIB Object

MIB Object...	Where to get more information...
dot1StpBridgeForwardDelay	See, RFC 1493: Bridge MIB.

For More Information

Topic	Where to Get More Information
Changing the Bridge Hello Time.	See, Setting the Bridge Hello Time.
Changing the Bridge Max Age.	See, Setting the Bridge Max Age.
Spanning tree.	See, Appendix C.

Setting the No Frame Interval

Overview

The No Frame Interval is the number of seconds of inactivity on the line after which the switch or bridge tests the port for correct operation. The switch or bridge considers a line inactive if it does not receive any frames on that line.

How to Set the No Frame Interval

To set the No Frame Interval, complete the following steps:



Switch Configuration button



Apply button



OK button

Step	Action
1	Click on the Switch Configuration button in the Switch Summary window. The Switch Configuration window opens.
2	Click in the No Frame Interval (secs): field in the Configuration box.
3	Enter a value from 60 to 60000 (the factory default is 300).
4	Click the Apply button to apply the change. or Click the OK button to apply the change and close the window.

Relevant SNMP MIB Object

MIB Object...	Where to get more information...
ebrNoFrameInterval	See, ELAN (DEC Vendor) MIB.

Setting the Aging Time

Overview

The forwarding database keeps dynamically learned forwarding information active for a specified number of seconds.

During stable operation (for example, when a topology change is not in effect), entries are aged when the Aging Time is exceeded.

The following events occur when an entry is aged out:

- The entry is marked inactive.
- The associated port number information is no longer used in making forwarding decisions.

How to Set the Aging Time (secs)

To set the Aging Time, complete the following steps:



Switch Configuration button



Apply button



OK button

Step	Action
1	Click on the Switch Configuration button in the Switch Summary window. The Switch Configuration window opens.
2	Click in the Aging Time (secs): field in the Configuration box.
3	Enter a value from 10 to 1000000 (the factory default is 120).
4	Click the Apply button to apply the change. or Click the OK button to apply the change and close the window.

Relevant SNMP MIB Object

MIB Object...	Where to get more information...
dot1dTpAgingTime	See, RFC 1493: Bridge MIB.

For More Information

Topic	Where to Get More Information
Changing the forwarding database Short Aging Time.	See, Setting the Short Aging Time.

Setting the Short Aging Time

Overview

Short Aging Time is the number of seconds that the bridge or switch keeps dynamically learned forwarding information active while a topology change is in effect.

How to Set the Short Aging Time

To set the Short Aging Time, complete the following steps:



Switch Configuration button



Apply button



OK button

Step	Action
1	Click on the Switch Configuration button in the Switch Summary window. The Switch Configuration window opens.
2	Click in the Short Aging Time (secs): field in the Configuration box.
3	Enter a value from 5 to 250 (the factory default is 30).
4	Click the Apply button to apply the change. or Click the OK button to apply the change and close the window.

Relevant SNMP MIB Object

MIB Object...	Where to get more information...
ebrFowardingDBShortAgingTime	See, ELAN (DEC Vendor) MIB.

For More Information

Topic	Where to Get More Information
Changing the forwarding database Aging Time.	See, Setting the Aging Time.

Setting the Gateway Address

Overview

The Gateway Address is the IP address of the default gateway (router). A default Gateway Address is required for the switch to deliver traps to a management station that is not on the local subnet.

Note

A subnet mask is not required for communicating with any management station in the IP network.

How to Set the Gateway Address

To set the Gateway Address, complete the following steps:



Switch Configuration button



Apply button



OK button

Step	Action
1	Click on the Switch Configuration button in the Switch Summary window. The Switch Configuration window opens.
2	Click in the Gateway Address field in the Configuration box.
3	Enter an IP address in the form n.n.n.n, where n is an integer value between 1 and 255.
4	Click the Apply button to apply the change. or Click the OK button to apply the change and close the window.

Relevant SNMP MIB Object

MIB Object...	Where to get more information...
esysGatewayAddress	See, ELAN (DEC Vendor) MIB.

For More Information

Topic	Where to Get More Information
Adding and deleting trap addresses.	See, Adding and Deleting Trap Addresses.

Adding and Deleting Trap Addresses

Overview

The **Trap Addresses** box in the Switch Configuration window allows you to add and delete IP addresses of the stations to which the switch or bridge sends event trap messages.

Events Trapped

The switch or bridge sends trap messages for the following events:

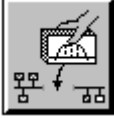




Trap Message	Event
authenticationFailure	An attempt to access the switch or bridge using the incorrect community name.
coldStart	A reboot, turning power to the switch or bridge to off, and then back to on.
linkUp	Generated whenever a port leaves the BROKEN state and enters another state. This trap message is sent when the port enters the FORWARDING state or the BACKUP state.
linkDown	This trap message is sent when a port enters the BROKEN state from another state.

Note

To send event trap message to stations that are not on the local subnet, set the default Gateway Address in the **Configuration** box of the Switch Configuration window.

How to Add and Delete Trap Addresses

To add or delete trap addresses, complete the following steps:

Step	Action
1	<p>Click on the Switch Configuration button in the Switch Summary window.</p>
	<p>The Switch Configuration window opens.</p>
<p>Switch Configuration button</p>	<p>To add a trap address:</p>
	<ol style="list-style-type: none"> a. Click in the Trap Addresses to Add: field in the Trap Addresses box. b. Enter an IP address in the form n.n.n.n, where n is an integer value between 1 and 255. c. Click the Add button to add the address. d. Go to Step 2.
<p>Add button</p>	<p>To delete a trap address:</p>
	<ol style="list-style-type: none"> a. Click on the address you want to delete in the Trap Addresses box. b. Click the Delete button. <p>A confirmation window appears.</p> <ol style="list-style-type: none"> c. Go to Step 2.
<p>Delete button</p>	<p>2 Click the Apply button to apply the change.</p>
	<p>or</p>
<p>Apply button</p>	<p>Click the Cancel button to cancel the operation.</p>
	
<p>Cancel button</p>	

Relevant SNMP MIB Object

MIB Object...	Where to get more information...
<i>To Add Trap Addresses:</i>	
pcomSnmpAuthTrapUserAddr	See, DEChub 900 public common MIB.
<i>To Delete Trap Addresses:</i>	
pcomSnmpAuthTrapUserStatus	See, DEChub 900 public common MIB.

For More Information

Topic	Where to Get More Information
Setting the gateway address.	See, Setting the Gateway Address.



Creating Address Filters

Overview

Address filtering allows you to specify the forwarding behavior of the module for specified addresses, on a per-port basis. The module uses address filters in conjunction with the learned information in its forwarding database to determine if a frame should be forwarded on a particular port.

How to Create Address Filters

To create an address filter, complete the following steps:

Step	Action
 <p data-bbox="282 898 464 957">Address Filters button</p>	<p data-bbox="500 772 1349 835">1 Click on the Address Filters button in the Switch Summary window.</p> <p data-bbox="607 898 1040 932">The Address Filters window opens.</p>
 <p data-bbox="282 1079 402 1138">Add Filter button</p>	<p data-bbox="500 982 987 1016">2 Click on the Add Filter button.</p> <p data-bbox="607 1079 1062 1113">The Add Filter Entry window opens.</p>
	<p data-bbox="500 1163 1349 1226">3 Select your format of specifying the address for the filter by clicking on DECnet or IP or by leaving MAC (the default) on.</p>
	<p data-bbox="500 1247 1349 1373">4 Depending on the type of identifier you chose in the Name or Address text box, enter the MAC address, the DECnet name or address, or the IP name or address for which you are creating the filter.</p>

(Continued on next page.)

Step	Action
5	In the filter port mask, click on the arrow under the port number to specify the filtering status for that port.

A green arrow under a port number indicates that messages are not filtered on the port.

A red arrow tipped with a black horizontal bar indicates that messages are filtered on the port. Initially, all ports are shown as filtered.



Rate Limiting Disabled button

6	Click on the Rate Limiting Disabled button to apply the switch or bridge rate limit to a filter for a multicast address.
---	--



Rate Limiting Enabled button

The button's icon changes to Rate Limiting Enabled.

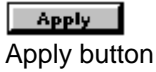


Rate Limiting Not Applicable icon

Note

You can apply rate filtering only to filter multicast addresses. The Rate Limiting Not Applicable icon appears until you enter a multicast address. Also, If rate limiting is not enabled on the switch or bridge, you can choose rate limiting for a filter, but it will not take effect. To enable rate limiting, refer to the section titled Enabling and Disabling Rate Limiting.

(Continued on next page.)



Step	Action
7	Click the Apply button to create the filter (see Note).

Note

HUBwatch software converts other identifiers to the MAC address and checks for a filter for that address. If a filter exists, HUBwatch displays it and asks you to confirm your selection

To replace the existing filter for the address and close the Add Filter Entry window, click on **YES**.

To Cancel the change and close the Add Filter Entry window, click on **No**.

Relevant SNMP MIB Object

MIB Object...	Where to get more information...
<i>For Ethernet Addresses, Use:</i>	
ebrMultiEnetStatus ebrMultiEnetAllowedToGoTo	See, ELAN (DEC Vendor) MIB.
<i>For 802.2 DSAPs, Use:</i>	
ebrMultiSapStatus ebrMultiSapAllowedToGoTo	See, ELAN (DEC Vendor) MIB.
<i>For SNAP PIDs, Use:</i>	
ebrMultiSnapStatus ebrMultiSnapAllowedToGoTo	See, ELAN (DEC Vendor) MIB.

For More Information

Topic	Where to Get More Information
To enable or disable rate limiting.	See, Enabling and Disabling Rate Limiting .
To set the rate limit.	See, Setting the Rate Limit .

Modifying Address Filters

Overview

Modifying address filters includes any, or all, of the following modifications:

- Modifying the MAC Address associated with a filter
- Modifying the Port Mask associated with a filter
- Applying or removing the rate limit from a multicast filter.

How to Modify Address Filters

To modify an address filter, complete the following steps:






Address Filters button

Step	Action
1	<p>Click on the Address Filters button in the Switch Summary window.</p> <p>The Address Filters window opens.</p>
2	<p>Access the Modify Filter Entry window for the filter you want to modify in one of the following ways:</p> <ol style="list-style-type: none"> a. Double click in the Select field in a filter's row. b. Click once in the Select field in a filter's row, then click the Modify Filter button. <p>The Modify Filter Entry window appears showing the selected MAC address and port mask.</p>



Modify Filter button

(Continued on next page.)

Step	Action
 Rate Limiting Enabled button	2 (Cont.) The window also displays a Rate Limiting Enabled button, a Rate Limiting Disabled button, or a Rate Limiting Not Applicable icon, depending on the rate limiting status of the filter.
 Rate Limiting Disabled button	
 Rate Limiting Not Applicable	
3	Make any or all of the following modifications: <ol style="list-style-type: none">Modify the MAC address.Modify the port mask.Apply or remove the bridge's or switch's rate limit from a multicast address filter.

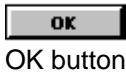
Modifying the MAC Address

To modify the MAC address, complete the following steps:

Step	Action
1	Click in the text entry field.
2	Modify the address.

Note

If a filter for the modified address already exists, HUBwatch displays it and asks you to confirm the replacement.



3	Click the OK button to apply the change and close the window.
---	---

If a filter exists (see Note, above), respond as follows:

- Click on **Yes** to replace the existing filter and close the Modify Filter Entry window.
- Click on **No** to cancel the change and close the Modify Filter Entry window.

Modifying the Port Mask

To modify the port mask, complete the following steps:

Step	Action
1	Click on the arrow under the port number to specify the filtering status for that port: <ul style="list-style-type: none">• A green arrow under a port number indicates that messages are not filtered on the port.• A red arrow, tipped with a black horizontal bar, indicates that messages are filtered on the port.
2	Click the Apply button to apply the change. or Click the OK button to apply the change and close the window.





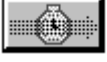


Apply button



OK button

Applying or Removing the Rate Limit from a Multicast Address Filter

To apply or remove the rate limit from a multicast address filter, complete the following steps:

Step	Action
 Rate Limiting Enabled button	1 Click on the Rate Limiting Enabled button or the Rate Limiting Disabled button.
 Rate Limiting Disabled button	The button's icon changes to the opposite state, indicating the change.
 Rate Limiting Not Applicable icon	<p style="text-align: center;">Note</p> You can apply rate limiting only to filters for multicast addresses. When you specify a unicast address, the Rate Limiting Not Applicable icon appears. If rate limiting is not enabled on the switch or bridge, and you choose rate limiting for a multicast address, it will not take effect. To enable rate limiting, refer to the section titled Enabling and Disabling Rate Limiting.
 Apply button	2 Click the Apply button to apply the change. or
 OK button	Click the OK button to apply the change and close the window.

Relevant SNMP MIB Object

MIB Object...	Where to get more information...
<i>For Ethernet Addresses, Use:</i>	
ebrMultiEnetStatus	
ebrMultiEnetAllowedToGoTo	See, ELAN (DEC Vendor) MIB.
<i>For 802.2 DSAPs, Use:</i>	
ebrMultiSapStatus	
ebrMultiSapAllowedToGoTo	See, ELAN (DEC Vendor) MIB.
<i>For SNAP PIDs, Use:</i>	
ebrMultiSnapStatus	
ebrMultiSnapAllowedToGoTo	See, ELAN (DEC Vendor) MIB.

For More Information

Topic	Where to Get More Information
To enable or disable rate limiting.	See, Enabling and Disabling Rate Limiting.
To set the rate limit.	See, Setting the Rate Limit.

Creating a Default Filter for All Unspecified Addresses

Overview




The Address Filters window includes a port mask for all unspecified addresses. This mask allows you to create a filter that will apply to all addresses for which you have not created a specific filter.

Example:

By setting port n to filter messages with all unspecified addresses, you ensure that all messages, except those with the addresses you specify for port n in the the Filters box, will be filtered on port n.

How to Specify a Filter for All Unspecified Addresses

To specify a filter for all unspecified addresses, complete the following steps:

Step	Action
1	Click on the Address Filters button in the Switch Summary window.
 <p data-bbox="289 982 440 1043">Address Filters button</p>	The Address Filters window opens.
2	<p data-bbox="574 1068 1369 1129">Click on the arrow in the Unspecified Filters Defaults port mask until one of the arrows indicates the default port mask you want:</p> <ul data-bbox="574 1152 1369 1297" style="list-style-type: none"> <li data-bbox="574 1152 1369 1213">• A green arrow under a port number indicates that messages are not filtered on the port. <li data-bbox="574 1236 1369 1297">• A red arrow, tipped with a black horizontal bar, indicates that messages are filtered on the port
3	Click the Apply button to apply the change.
 <p data-bbox="289 1356 435 1388">Apply button</p>	or
 <p data-bbox="289 1472 402 1499">OK button</p>	Click the OK button to apply the change and close the window.

Relevant SNMP MIB Object

MIB Object...	Where to get more information...
ebrMultiSwManualFilter	See, ELAN (DEC Vendor) MIB.



Creating Protocol Filters

Overview




Protocol filtering instructs the switch or bridge to always forward or always reject transmissions that are originated under specified protocols.

How to Create a Protocol Filter

To create a protocol filter, complete the following steps:

Step	Action
 Protocol Filters button	<p>1 Click on the Protocol Filters button in the Switch Summary window.</p> <p>The Protocol Filters window opens.</p>
 Add Filter button	<p>2 Click on the Add Filter button</p> <p>The Add Filter Entry window opens.</p>
	<p>3 Scroll through the Available Protocols box until you find the protocol you want:</p> <ul style="list-style-type: none"> • The Available Protocols box displays Ethernet protocols by default. If you want a non-Ethernet protocol, click on DSAP or SNAP to display a list of the corresponding protocols that are available. • To sort the list by type rather than by name, click on Type.
	<p>4 Double click on the protocol to select it.</p>

(Continued on next page.)

Step	Action
5	<p>Specify the filtering status for that port by clicking on the arrows under the port number in the filter port mask:</p> <ul style="list-style-type: none"> • A green arrow under a port number indicates that messages are not filtered on the port • A red arrow tipped with a black horizontal bar indicates that messages are filtered on the port. Initially, all ports are shown as filtered.
 Rate Limiting Disabled button	<p>6 Click on the Rate Limiting Disabled button to apply the switch or bridge rate limit to a filter for a multicast address.</p>
 Rate Limiting Enabled button	<p>The button's icon changes to Rate Limiting Enabled.</p> <p style="text-align: center;">Note</p> <p>If rate limiting is not enabled on the switch or bridge, you can choose rate limiting for a protocol, but it will not take effect. To enable rate limiting, refer to the section titled Enabling and Disabling Rate Limiting.</p>
 OK button	<p>7 Click the OK button to apply the changes and close the Add Filter Entry window.</p> <p style="text-align: center;">Note</p> <p>HUBwatch software checks for a filter for the specified protocol. If a filter already exists, HUBwatch displays it and asks you to confirm your selection.</p> <p>If a filter already exists, respond as follows:</p> <p>Click on Yes to replace the existing filter and close the Add Filter Entry window.</p> <p>Click on No to Cancel the change and close the Add Filter Entry window.</p>

Relevant SNMP MIB Object

MIB Object...	Where to get more information...
<i>For Ethernet Protocol Types, Use:</i>	
ebrMultiEnetStatus ebrMultiEnetAllowedToGoTo	See, ELAN (DEC Vendor) MIB.
<i>For 802.2 DSAPs, Use:</i>	
ebrMultiSapStatus ebrMultiSapAllowedToGoTo	See, ELAN (DEC Vendor) MIB.
<i>For SNAP PIDs, Use:</i>	
ebrMultiSnapStatus ebrMultiSnapAllowedToGoTo	See, ELAN (DEC Vendor) MIB.

For More Information

Topic	Where to Get More Information
To enable or disable rate limiting.	See, Enabling and Disabling Rate Limiting.
To set the rate limit.	See, Setting the Rate Limit.

Modifying Protocol Filters



Overview

Modifying Protocol filters includes any, or all, of the following modifications:




- Modifying the Protocol
- Modifying the Port Mask
- Applying or removing the switch or bridge rate limit from the filter.

How to Modify a Protocol Filter

To modify a protocol filter, complete the following steps:

Step	Action
 <p>Protocol Filters button</p>	<p>1 Click on the Protocol Filters button in the Switch Summary window.</p> <p>The Protocol Filters window opens.</p>
 <p>Modify Filter button</p>	<p>2 Access the Modify Filter Entry window for the filter you want to modify in one of the following ways:</p> <ol style="list-style-type: none"> a. Double click in the Select field in a filter's row. b. Click once in the Select field in a filter's row, then click the Modify Filter button. <p>The Modify Filter Entry window appears showing the selected port mask and protocol, and a list of available protocols.</p>

(Continued on next page.)

Step	Action
 Rate Limiting Enabled button	2 (Cont.) The window also displays a Rate Limiting Enabled button, a Rate Limiting Disabled button, or a Rate Limiting Not Applicable icon, depending on the rate limiting status of the filter.
 Rate Limiting Disabled button	
 Rate Limiting Not Applicable icon	
3	Make any or all of the following modifications: <ul style="list-style-type: none"> • Modify the Protocol. • Modify the port mask. • Apply or remove the bridge's or switch's rate limit from the filter.

Modifying the Protocol

The **Available Protocols** box displays Ethernet protocols by default. If you want a non-Ethernet protocol, click on **DSAP** or **SNAP** to display a list of the corresponding protocols that are available.

To modify the protocol, complete the following steps:

Step	Action
1	Scroll through the Available Protocols box until you find the protocol you want to modify. To sort the list by type, rather than by name, click on Type .
2	Double click on the protocol to select it. The protocol you selected appears in the Available Protocols box.

Note

If you modify a protocol, HUBwatch software checks for a filter for the new protocol. If a filter already exists, HUBwatch displays it and asks you to confirm the replacement.



OK button

3 Click the **OK** button to apply the change and close the window.

If a filter exists (see Note, step 2), respond as follows:

- Click on **Yes** to replace the existing filter and close the Modify Filter Entry window.
 - Click on **No** to cancel the change and close the Modify Filter Entry window.
-

Modifying the Port Mask

To modify the port mask, complete the following steps:

Step	Action
1	<p>Click on the arrow under the port number to specify the filtering status for that port:</p> <ul style="list-style-type: none"> • A green arrow under a port number indicates that messages are not filtered on the port. • A red arrow, tipped with a black horizontal bar, indicates that messages are filtered on the port.
2	<p>Click the Apply button to apply the change.</p> <p style="text-align: center;">or</p> <p>Click the OK button to apply the change and close the window.</p>







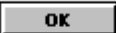
Apply button



OK button

Applying or Removing the Rate Limit from a Multicast Address Filter

To apply or remove the rate limit from a multicast address filter, complete the following steps:

Step	Action
 Rate Limiting Enabled button	1 Click on the Rate Limiting Enabled button or the Rate Limiting Disabled button. The button's icon changes to the opposite state, indicating the change.
 Rate Limiting Disabled button	
 Rate Limiting Not Applicable icon	
 Apply button	2 Click the Apply button to apply the change. or
 OK button	Click the OK button to apply the change and close the window.

Note

If rate limiting is not enabled on the switch or bridge, and you choose rate limiting for a filter, it will not take effect. To enable rate limiting, refer to the section titled **Enabling and Disabling Rate Limiting**.

Relevant SNMP MIB Object

MIB Object...	Where to get more information...
<i>For Ethernet Protocol Types, Use:</i>	
ebrMultiEnetStatus ebrMultiEnetAllowedToGoTo	See, ELAN (DEC Vendor) MIB.
<i>For 802.2 DSAPs, Use:</i>	
ebrMultiSapStatus ebrMultiSapAllowedToGoTo	See, ELAN (DEC Vendor) MIB.
<i>For SNAP PIDs, Use:</i>	
ebrMultiSnapStatus ebrMultiSnapAllowedToGoTo	See, ELAN (DEC Vendor) MIB.

For More Information

Topic	Where to Get More Information
To enable or disable rate limiting.	See, Enabling and Disabling Rate Limiting.
To set the rate limit.	See, Setting the Rate Limit.

Specifying Default Protocol Filters

Overview

The Protocol Filters window includes an **Unspecified Filters Defaults** box that allows you to specify default filters for protocols not listed in the **Filters** box.



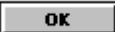
For example, you can specify that all Ethernet protocols not listed in the **Filters** box are filtered on port n.

Initial Setting:

Initially, the **Unspecified Filters Defaults** box shows no ports filtered for any protocol.

How to Specify a Default Protocol Filter

To specify a default protocol filter, complete the following steps:

Step	Action
1	Click on the Protocol Filters button in the Switch Summary window.
 <p>Protocol Filters button</p>	The Protocol Filters window opens.
2	<p>Click on the arrow in the Unspecified Filters Defaults port mask until one of the arrows indicates the default port mask you want:</p> <ul style="list-style-type: none"> • A green arrow under a port number indicates that messages are not filtered on the port. • A red arrow, tipped with a black horizontal bar, indicates that messages are filtered on the port.
 <p>Apply button</p>	3 Click the Apply button to apply the change.
 <p>OK button</p>	or
	Click the OK button to apply the change and close the window.

Relevant SNMP MIB Object

MIB Object...	Where to get more information...
ebrMultiSwProtoEnetOther ebrMultiSwProtoSapOther ebrMultiSwProtoSnapOther	See, ELAN (DEC Vendor) MIB.




Adding Protocols not in the Available Protocols List

Overview




You can create a protocol filter for a protocol that is not in the **Available Protocols** list by using either the Add Filter Entry window or the Modify Filter Entry window.

How To Add a Protocol

To add a protocol, complete the following steps:

	Step	Action
	1	Click on the Protocol Filters button in the Switch Summary window.
Protocol Filters button		The Protocol Filters window opens.
	2	Click on the Add Filter button
Add Filter button		or
		Select a filter and click on the Modify Filter button.
Modify Filter button		The Add Filter Entry or the Modify Filter Entry window opens.

(Continued on next page.)

	Step	Action
 Custom button	3	Click the Custom button. The Protocol Type window opens.
	4	Click in the Protocol ID field and enter the protocol number in either Ethernet, 802.3 DSAP, or ISO style.
 OK button	5	Click the OK button to add the protocol. or
		Click the Cancel button to cancel the operation.
 Cancel button		

Relevant SNMP MIB Object

MIB Object...	Where to get more information...
<i>For Ethernet Protocol Types, Use:</i>	
ebrMultiEnetStatus ebrMultiEnetAllowedToGoTo	See, ELAN (DEC Vendor) MIB.
<i>For 802.2 DSAPs, Use:</i>	
ebrMultiSapStatus ebrMultiSapAllowedToGoTo	See, ELAN (DEC Vendor) MIB.
<i>For SNAP PIDs, Use:</i>	
ebrMultiSnapStatus ebrMultiSnapAllowedToGoTo	See, ELAN (DEC Vendor) MIB.

For More Information

Topic	Where to Get More Information
To enable or disable rate limiting.	See, Enabling and Disabling Rate Limiting .
To set the rate limit.	See, Setting the Rate Limit .

Deleting Address and Protocol Filters

Overview

You can delete previously created protocol and address filters. You can also delete a second filter or all filters at once.

Note

Certain address filters cannot be deleted. They are placed into the switch or bridge address filter database to ensure proper operation. If you attempt to delete any of these address filters, the deletion does not take effect and an SNMP error is returned.

How to Delete Filters

To delete a selected filter, complete the following steps:



Address
Filters
button







Protocol
Filters button

Step	Action
1	Click the Address Filters button or the Protocol Filters button in the Switch Summary window.

The Address Filters window or the Protocol Filters window opens.

(Continued on next page.)

Deleting Address and Protocol Filters

	Step	Action
 Filter Select box	2	Click on the Filter Select box in the filters row to select a filter.
		The filter is highlighted and a check mark appears in the Filter Select box.
 Delete Filter button	3	Click the Delete Filter button to delete the filter.
To delete all filters in one operation:		
 Delete All button	a.	Click the Delete All button at the bottom of the window. A confirmation window appears.
	b.	Click on Yes to delete the filters. Click on No to cancel the operation.

Relevant SNMP MIB Object

MIB Object...	Where to get more information...
<i>For Ethernet Protocol Types, Use:</i>	
ebrMultiEnetStatus ebrMultiEnetAllowedToGoTo	See, ELAN (DEC Vendor) MIB.
<i>For 802.2 DSAPs, Use:</i>	
ebrMultiSapStatus ebrMultiSapAllowedToGoTo	See, ELAN (DEC Vendor) MIB.
<i>For SNAP PIDs, Use:</i>	
ebrMultiSnapStatus ebrMultiSnapAllowedToGoTo	See, ELAN (DEC Vendor) MIB.
<i>To Remove all Management Specified Address Filters, Use:</i>	
ebrRemoveMgmtAddress	See, ELAN (DEC Vendor) MIB.
<i>To Remove all Management Specified Protocol Filters, Use:</i>	
ebrRemoveMgmtProto	See, ELAN (DEC Vendor) MIB.

Writing Contents of Forwarding and Filter Databases to Files

Overview

You can create files containing the list of protocol filters and address filters, respectively.

How to Write the List of Filters to a File:

To write the list of filters to a file, complete the following steps:

Step	Action
1	From the Switch Summary window: click the Forwarding Database button or the Address Filters button or the Protocol Filters button. The appropriate window, (the Forwarding Database window, the Address Filters window, or the Protocol Filters window) opens.



Forwarding Database button



Address Filters button



Protocol Filters button

(Continued on next page.)



File Button

Step	Action
2	Click on the File button

The **File Selection** window appears with the following items:

- A filename Filter box with a default filename filter for HUBwatch protocol or address filter files. You can edit the filename filter by clicking on this box.

To generate a list of files that match the filename Filter, click on **Filter** at the bottom of the window.

- A Directories box.

When you select a directory, the directory in the filename filter changes, but the rest of the filename filter does not.

- A Files box containing a list of files matching the filename filter.

This list is empty until you create a file matching the filename filter and click on **Filter**.

- A Selection box displaying the following default filenames:



`protflt.lis` for protocol filters.

`addrflt.lis` for address filters.

`forwdb.lis` for forwarding database.

(Continued on next page.)

Writing Contents of Forwarding and Filter Databases to Files

Step	Action
3	Either use the default filename in the Selection box or enter a new one by clicking on the Selection box and typing a new filename.
 OK button	4 Click the OK button to write the file to the file named in the Selection box. or
 Cancel button	Click the Cancel button to return to the Protocol or Address Filtering window.

Chapter 5

FDDI Configuration Capabilities

Overview

Introduction

This chapter describes FDDI configuration capabilities that are supported in DEChub 900 FDDI network modules. The descriptions discussed in this chapter assume that the reader is familiar with basic FDDI configuration rules and understands the differences between an A, B, M, and S port. If these terms are not familiar to you, refer to Appendix A in this manual for an overview of FDDI concepts that are discussed in this chapter.

In This Chapter

The following topics are covered in this chapter:

Topic	See page...
Dual Ring Configurations	5-3
Tree Configurations	5-4
DECconcentrator 900MX	5-6
DECconcentrator 900TH	5-7

(Continued on next page.)

Topic	See page...
DECconcentrator 900FH	5-8
DECswitch 900EF	5-9
PEswitch 900TX	5-10
Configuration Guidelines and Rules	5-11
FDDI in the HUB Backplane	5-13
Default Configurations	5-16
FDDI Tree Configuration Examples	5-19
Dual Ring Configuration Examples	5-30
Fault Tolerance in Dual Rings	5-37
Fault Tolerance in Trees	5-39
Token Ordering of Trees or Dual Rings	5-41
Quick PC Trace Option For Concentrators	5-46
Summary of Important Configuration Features	5-47

Because FDDI concentrators (such as the DECconcentrator 900MX and the DECconcentrator 900TH) are key devices in FDDI networks, their capabilities and features are also included in this chapter.

Dual Ring Configurations

Introduction

DEChub 900 FDDI network modules support front panel as well as backplane FDDI ports. When configured in a dual ring topology, ports are assigned a Ring port (A port or B port) by management.

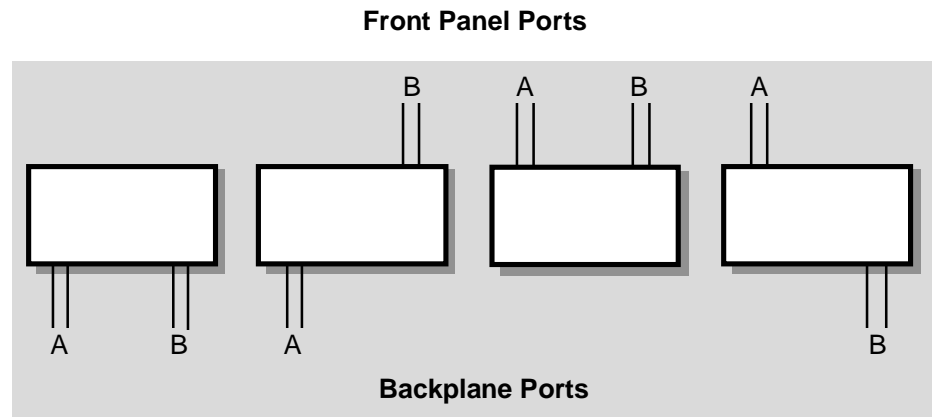
HUBwatch users can assign a ring port using the Station Configuration window. Any SNMP based management software can be used.

Because an individual FDDI network module may support a subset of these configurations, each of the FDDI network module capabilities are described in following sections.

Dual Ring Port Configuration Examples

Figure 5-1 shows the basic dual attachment station (DAS) port configurations that can be management assigned.

Figure 5-1 Dual Ring Port Configurations



LKG-10063-95

Tree Configurations

Introduction

When connected in a tree configuration, front panel ports and backplane ports are assigned a Tree port (M port or S port) by management.

HUBwatch users can assign a tree port using the Station Configuration window. Any SNMP based management software can be used.

Tree Port Configuration Examples

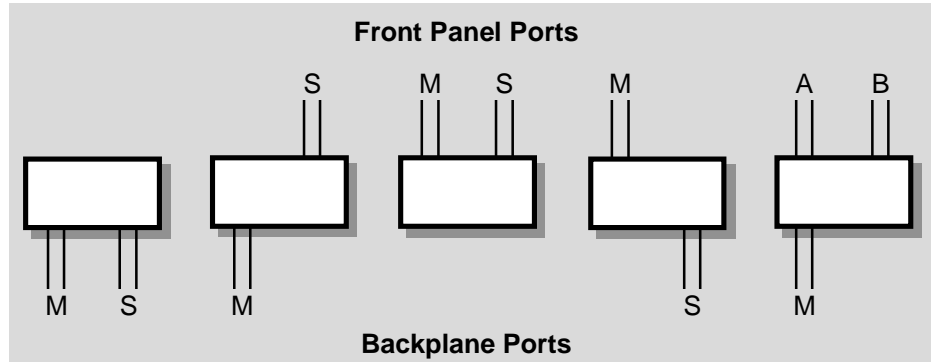
Figure 5-2 shows the tree port configurations that can be management assigned.

Dual Homed Configuration

In Figure 5-2, note the fifth configuration with an M port in the backplane, and (A and B) ports on the front panel. This configuration is only implemented in concentrators and is used for connecting to a dual ring, or in a dual homed configuration.

Also, note that when the user accessible FDDI ports are reconfigured as tree ports, the A port always becomes an M port and the B port always becomes an S port. This is true for either front panel ports or ModPMD ports in a DEChub ONE-MX docking station

Figure 5-2 Tree Port Configurations



LKG-10064-95

DECconcentrator 900MX

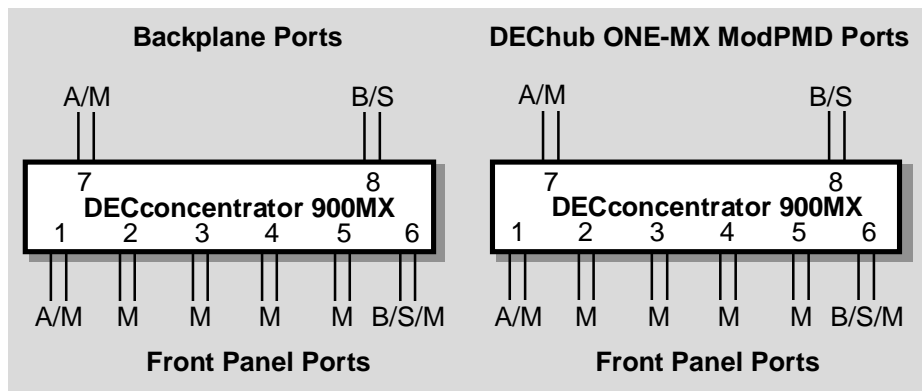
Introduction

The DECconcentrator 900MX is an eight-port FDDI concentrator (six front panel ports and two backplane ports). The two backplane ports, see Figure 5-3, attach to a DEChub 900 MultiSwitch backplane or to a DEChub ONE-MX docking station that supports ModPMDs.

Port Assignments

Port 1 can be configured as either an A or M port and Port 6 can be configured as either a B, S, or M port. Ports 2 to 5 are always M ports. The two backplane ports (ports 7 and 8) are also software configurable using HUBwatch management.

Figure 5-3 DECconcentrator 900MX Port Configuration Capabilities



LKG-10066-95

DECconcentrator 900TH

Introduction

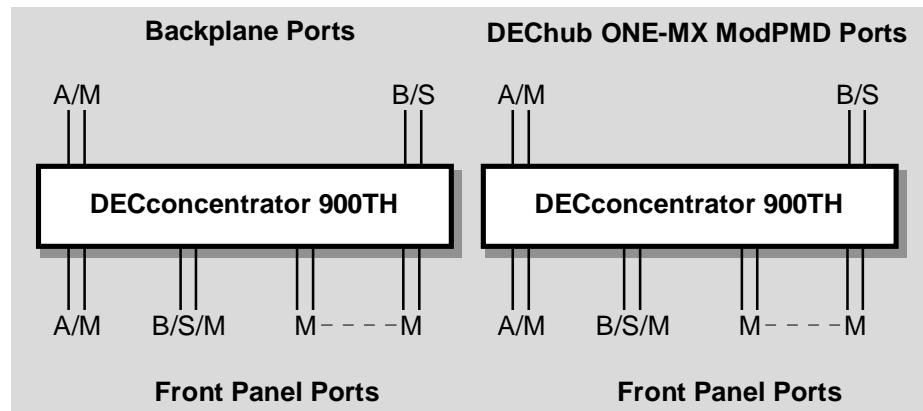
The DECconcentrator 900TH is a 16 port FDDI concentrator (fourteen front panel ports and two backplane ports). The two backplane ports, see Figure 5-4, attach to a DEChub 900 MultiSwitch backplane or to a DEChub ONE-MX docking station that supports ModPMDs.

Twelve of the front panel ports are fixed unshielded twisted pair (UTP) connections. The two remaining ports can be configured for either UTP, multimode fiber (MMF), or single mode fiber (SMF) by the addition of ModPMD modules.

Port Assignments

ModPMD Port 1 can be configured as either an A or M port and ModPMD Port 2 can be configured as either a B, S, or M port. The two backplane ports are also software configurable through HUBwatch management therefore both dual ring and tree connections can be supported.

Figure 5-4 DECconcentrator 900TH Port Configuration Capabilities



LKG-10067-95

DECconcentrator 900FH

Introduction

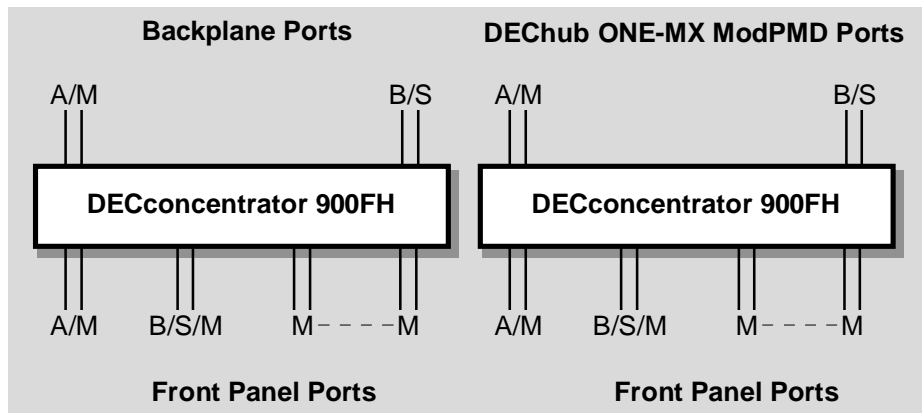
The DECconcentrator 900FH is a 16 port FDDI concentrator (14 front panel ports and two backplane ports). The two backplane ports, see Figure 5-5, attach to a DEChub 900 MultiSwitch backplane or to a DEChub ONE-MX docking station that supports ModPMDs.

Twelve of the front panel ports are fixed multimode fiber (MMF), SC optics connections. The two remaining ports can be configured for either UTP, multimode fiber (MMF), or single mode fiber (SMF) by the addition of ModPMD modules.

Port Assignments

ModPMD Port 1 can be configured as either an A or M port and ModPMD Port 2 can be configured as either a B, S, or M port. The two backplane ports are also software configurable through HUBwatch management, therefore both dual ring and tree connections can be supported.

Figure 5-5 DECconcentrator 900FH Port Configuration Capabilities



LKG-10124-95

DECswitch 900EF

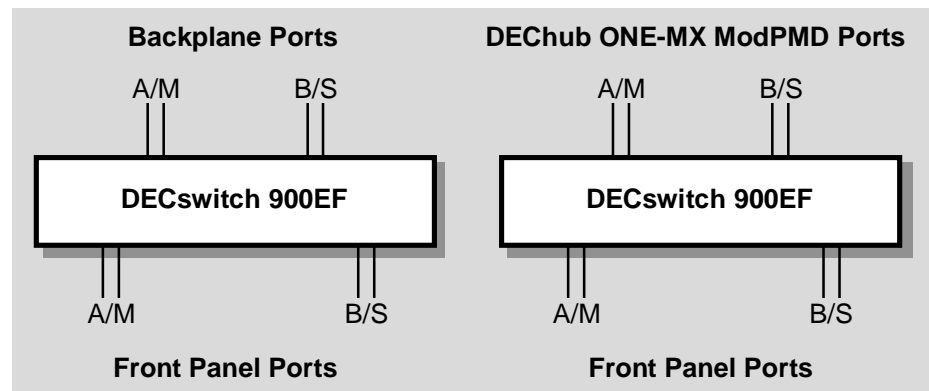
Introduction

The DECswitch 900EF (previously called the DECbridge 900MX) supports two FDDI ports that can be individually assigned to either the module's front panel (Port 1A/M and Port 1B/S) or to the backplane ports for connection to a DEChub 900 MultiSwitch or to a DEChub ONE-MX docking station. Therefore, the DECswitch 900EF module can have only two FDDI ports that are active at any time (for example, two front panel ports, one front panel and one backplane port, or two backplane ports).

Port Assignments

The FDDI port assignments are software configurable via HUBwatch or the set up port menu. Figure 5-6, shows how two front panel ports, two backplane ports, or a front panel port and a backplane port can be configured as A and B ports or M and S ports.

Figure 5-6 DECswitch 900EF Port Configuration Capabilities



LKG-10068-95

PEswitch 900TX

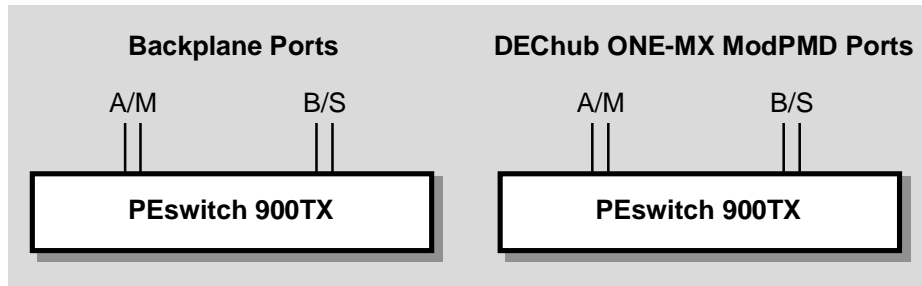
Introduction

Unlike the DECswitch 900EF module, the PEs witch 900TX module supports two FDDI port connections to the DEChub 900 MultiSwitch backplane or to the DEChub ONE-MX docking station only. There are no front panel FDDI ports on the PEs witch 900TX module.

Port Assignments

The FDDI port assignments are software configurable via HUBwatch or the set up port menu. Figure 5-7 shows how the backplane FDDI ports can be configured as either A and B or M and S connections at any time.

Figure 5-7 PEs witch 900TX Port Configuration Capabilities



LKG-10069-95

Configuration Guidelines and Rules

Introduction

This section details the configuration capabilities that are supported in the DEChub 900 family of FDDI products.

Individual FDDI Networks

Individual FDDI networks can be configured as either a dual ring or a tree. This allows compliancy with FDDI configuration rules which operate at the module level and are independent of HUBwatch.

Multiple FDDI Networks

In DEChubs supporting multiple FDDI networks on the backplane, some of the networks can be configured as dual rings and others can be configured as trees, but each of the individual networks can be of only one type. Dual rings of trees can then be constructed by interconnecting the various networks across the front panel.

Single Attachment Concentrator (SAC)

Digital's DEChub 900 family of FDDI products include Single Attach Concentrators (SACs) and Dual Attach Concentrators (DACs). A SAC has one S port and can have up to 15 M ports. A DAC has an A and B port, and can have up to 14 M ports.

Implications:

FDDI rules specify that stations with M ports are concentrators. Consequently, when a FDDI switch (such as, a DECswitch 900EF or a PEs switch 900TX) is configured with M and S ports, it reports as a concentrator in FDDI NIF and SIF frames, and in the FDDI and SNMP MIBs.

HUBwatch, FDDI monitors, and FDDI Ring Maps announce the station type of a treed DECswitch 900EF or PEs switch 900TX as a Single Attach Concentrator (SAC), rather than as a Single Attach Station (SAS).

Dual Ring and Trees

The terms, Dual Ring and Tree, are physical descriptions of the network topology. However, in all cases, the FDDI is a logical ring that enables a token to be passed from station-to-station in the ring. The physical

implementation can be configured as a tree or a dual ring, but in all cases a logical ring exists.

DEChub 900 Backplane

Technically, any type of configuration (dual ring, tree, or dual ring of trees) can be created in the DEChub 900 backplane, however, for ease of use, only dual ring and tree configurations are supported.

Up to four independent FDDI networks can be created across the DEChub 900 backplane. Each of the created FDDI networks can be either a dual ring or a tree on the backplane, but not a mixture of both.

Note

A treed FDDI DEChub 900 backplane can connect to a dual ring that is external to the DEChub 900, and can be part of an overall dual ring of trees configuration.

Point-to-Point Connections

Note that any FDDI connection between two adjacent stations is actually two point-to-point connections, regardless of where the stations are physically located in the configuration (tree or dual ring). This is true for any FDDI product, whether the product is in a hub or operating standalone.

The backplane of the DEChub 900 MultiSwitch is used to make point-to-point connections between DEChub 900 FDDI network modules that are configured in the hub. One backplane channel is needed for each point-to-point connection.

Backplane Channels

Because two point-to-point connections are required between any two ports, two backplane channels are required for each connection between any two ports on the DEChub 900 FDDI network modules, regardless of the actual configuration.

FDDI in the Hub Backplane

Introduction

The DEChub 900 MultiSwitch and the DEChub ONE-MX use a building block approach for configuring FDDI on the backplane. The network manager assigns a port type by selecting a building block. The building block approach works as follows:

FDDI Building Blocks

Building blocks are divided into two groups:

- Ring Building Blocks
- Tree Building Blocks

There are a total of nine building blocks; four building blocks are used for building dual rings, and five building blocks are used for building trees.

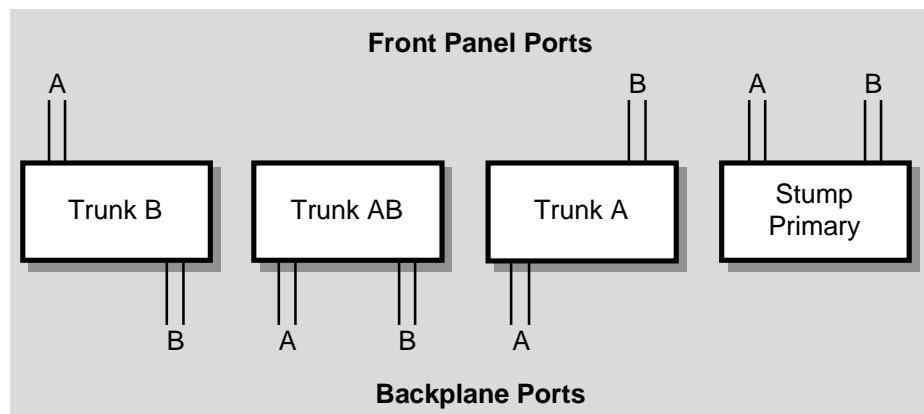
HUBwatch only allows connections to be made between building blocks of the same group (Ring group or Tree group), in order to avoid errors such as connections that break because of the FDDI standard's preference for trees over dual rings.

Ring Building Blocks

The four Ring building blocks, see Figure 5-8, that are used to build dual rings are named as follows:

- Trunk B — Port A connects to the FDDI network module front panel ports. Port B connects to the DEChub 900 backplane or to the DEChub ONE-MX ModPMD
- Trunk AB — Ports A and B connect to the DEChub 900 backplane or to the DEChub ONE-MX ModPMDs
- Trunk A — Port A connects to the DEChub 900 backplane or to the DEChub ONE-MX ModPMD. Port B connects to the FDDI network module front panel ports
- Stump Primary — Ports A and B connect to the FDDI network module front panel ports

Figure 5–8 Ring Building Blocks



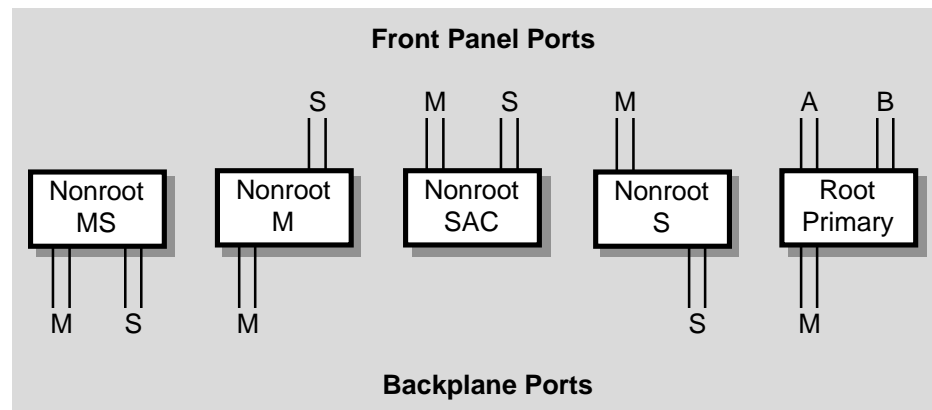
LKG-10070-95

Tree Building Blocks

The five Tree building blocks, see Figure 5-9, that are used to build Trees are named as follows:

- Nonroot MS — Ports M and S connect to the DEChub 900 backplane or to the DEChub ONE-MX ModPMDs
- Nonroot M — Port M connects to the DEChub 900 backplane or to the DEChub ONE-MX ModPMDs. Port S connects to the FDDI network module front panel ports
- Nonroot SAC — Ports M and S connect to the FDDI network module front panel ports
- Nonroot S — Port S connects to the DEChub 900 backplane or to the DEChub ONE-MX ModPMDs. Port M connects to the FDDI network module front panel ports
- Root Primary — Ports A and B connect to the FDDI network module front panel ports. Port M connects to the DEChub 900 backplane or to the DEChub ONE-MX ModPMDs

Figure 5-9 Tree Building Blocks



LKG-10071-95

Default Configurations

Introduction

This section describes the default (or factory set) configurations that apply to the FDDI network modules. Note that the default settings vary according to module type, and whether the module is installed into a DEChub 900 MultiSwitch or a DEChub ONE or DEChub ONE-MX docking station.

FDDI Network Modules in a DEChub 900

When FDDI network modules (DECconcentrator 900MX, DECconcentrator 900FH, DECconcentrator 900TH, and DECswitch 900EF) are installed into a DEChub 900 MultiSwitch, the default configuration is:

- All front panel ports are active
- A and B ports connect to the module's front panel ports.

This means that no redirection to backplane ports or backplane connections are made between FDDI network modules unless the network manager chooses to do so.

The network manager can issue the appropriate HUBwatch commands to establish FDDI networks across the backplane of the DEChub 900 MultiSwitch.

While the default for the PESwitch 900TX is to the backplane ports, no FDDI LAN connections across the DEChub 900 backplane are made by default. The network manager must issue the appropriate HUBwatch commands to connect a PESwitch 900TX to a FDDI backplane LAN.

FDDI Network Modules in a DEChub ONE or DEChub ONE-MX

When FDDI network modules (DECconcentrator 900MX, DECconcentrator 900FH, DECconcentrator 900TH, and DECswitch 900EF) are installed into a DEChub ONE or into a DEChub ONE-MX, the default configuration is:

- All front panel ports are active
- A and B ports connect to the module's front panel ports.

PEswitch 900TX:

The default configuration for the PEs switch 900TX is:

- A port and B port connect to the DEChub ONE-MX ModPMD ports.

No FDDI connections are available when the PEs switch 900TX is installed to a DEChub ONE (see Note).

Note

The DEChub ONE (DEHUA) supports one Ethernet connection and the DEChub ONE-MX (DEF1H) supports one Ethernet connection and up to 2 ModPMD FDDI connections.

Enabling ModPMD Ports

To use the ModPMD ports of the DEChub ONE-MX a network manager must issue the appropriate HUBwatch commands to enable the ModPMD ports, using the building blocks previously described. This task can be accomplished using HUBwatch or through the setup port of the DEChub ONE-MX docking station.

Power Failure Recovery

Modules in a DEChub ONE or DEChub ONE-MX retain their configuration so that, in the event of a power failure, the module returns to the previously configured state. This previous configuration recall ability applies if a module is removed (powered off) and then moved to another DEChub ONE docking station that is of the same model type.

Change of Environment

FDDI network modules in a DEChub ONE or DEChub ONE-MX recognize a change of environment when moved between a DEChub 900 MultiSwitch, a DEChub ONE-MX, or a DEChub ONE docking station.

With the exception of the PEs witch 900TX, the FDDI network modules assume the following default configuration when a change of environment is detected: A port and B port connect to the network module's front panel. The PEs witch 900TX module assumes the following default configuration: A port and B port connect to the module's backplane ports only (and not to any DEChub 900 backplane FDDI LAN) or to the DEChub ONE-MX ModPMD ports.

Example of Module Reacting to Change of Environment

If a DECswitch 900EF module, that is configured with an S port and M port on the ModPMDs, is moved from one DEChub ONE-MX docking station to another, the module powers up with the ModPMDs of the second DEChub ONE-MX enabled as S and M ports (previous configuration recall ability).

If the same module is then moved (from the DEChub ONE-MX docking station) to a DEChub ONE docking station, the module detects an environment change, and powers up with the front panel ports enabled as A and B ports (the module's default configuration).

If the module is again moved back to a DEChub ONE-MX docking station (from the DEChub ONE docking station), the module again detects a new environment, and powers up with the front panel ports enabled as A and B ports (default configuration).

Also, if a module is moved from one DEChub ONE-MX to another that has a different ModPMD configuration, the module powers up and, sensing that it is still in a DEChub ONE-MX, configures the ports per the previous configuration recalled process. The FDDI Network configuration firmware does not detect a change in the media type of the ModPMDs in the DEChub ONE-MX.

FDDI Tree Configuration Examples

Introduction

The DEChub 900 backplane can support many types of FDDI tree configurations. FDDI trees can be contained within the hub backplane and can connect an individual tree in the hub backplane to a higher level of a tree, or can be used to interconnect other hubs.

This section provides 5 examples of FDDI tree configurations that are supported in the DEChub 900 backplane:

- Example 1 — Self-contained Tree of Concentrators in Hub Backplane
- Example 2 — Self-contained Tree of Switches and Concentrators in Hub Backplane
- Example 3 — Tree Connections to an External Concentrator
- Example 4 — Dual Homing and Connection to an External Ring
- Example 5 — FDDI Tree Extensions

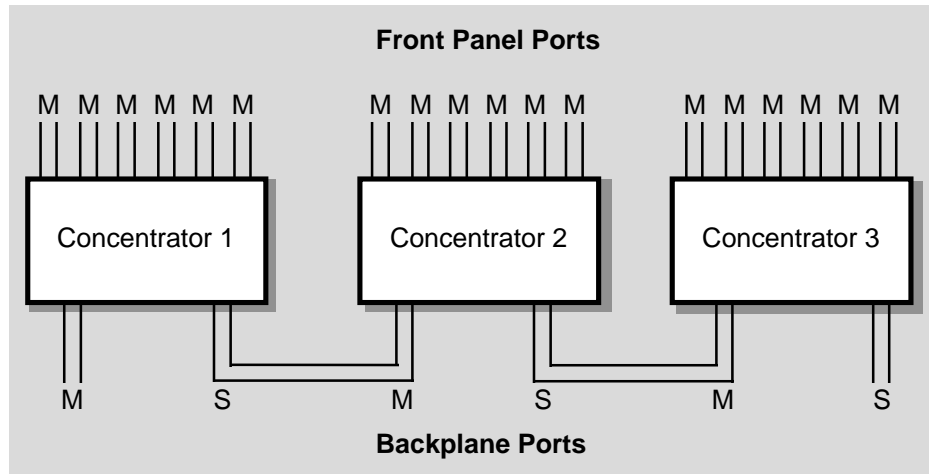
Example 1 — Self-contained Tree of Concentrators in Hub Backplane

In this example (see Figure 5-10), an FDDI tree is constructed entirely within the Hub backplane. The backplane ports of the concentrator modules are enabled as M ports and S ports. The front panel ports become M ports.

The module that is installed in the highest slot number of the Hub (Concentrator 3) is designated as the *top of the tree*, and its M port connects to the S port of the module with the second highest slot number (Concentrator 2).

Two Hub backplane channels are required for each connection. In Figure 5-10, a total of four backplane channels are in use.

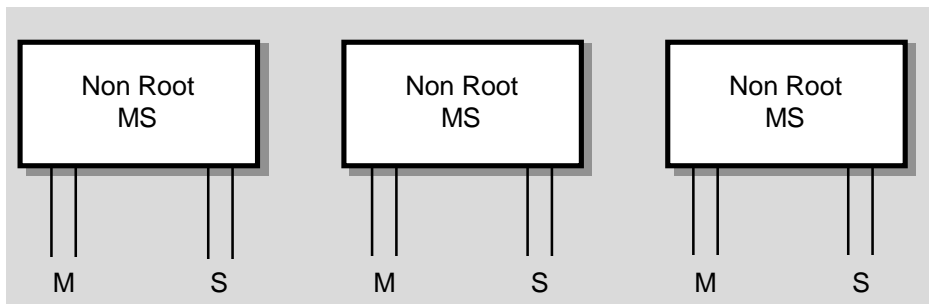
Figure 5-10 DECconcentrator Tree Connections in Hub Backplane



LKG-10074-95

Figure 5-11 shows the Building block representation of the configuration example described in Figure 5-10:

Figure 5-11 Building Block Representation of Example 1



LKG-10075-95

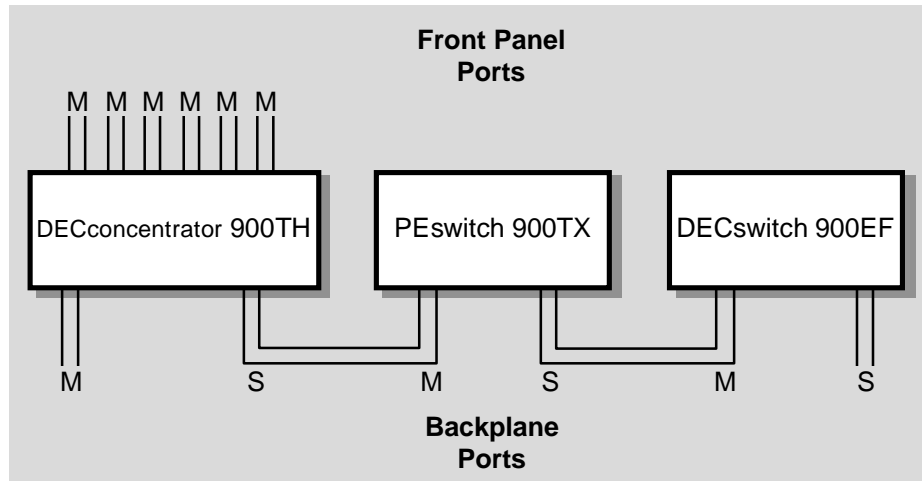
Example 2 — Self-contained Tree of Switches and Concentrators in Hub Backplane

In this example (see Figure 5-12), an FDDI tree is constructed entirely within the Hub backplane, however, a mixture of FDDI network module types (switches and concentrators) are used. The backplane ports of the FDDI network modules are enabled as M ports and S ports. The front panel ports of the concentrators become M ports and the front panel FDDI ports of the switches become unusable.

The module that is installed in the highest slot number of the Hub (DECswitch 900EF) is designated as the *top of the tree*, and its M port connects to the S port of the module with the second highest slot number (PEswitch 900TX).

Two Hub backplane channels are required for each connection. In Figure 5-12, a total of four backplane channels are in use.

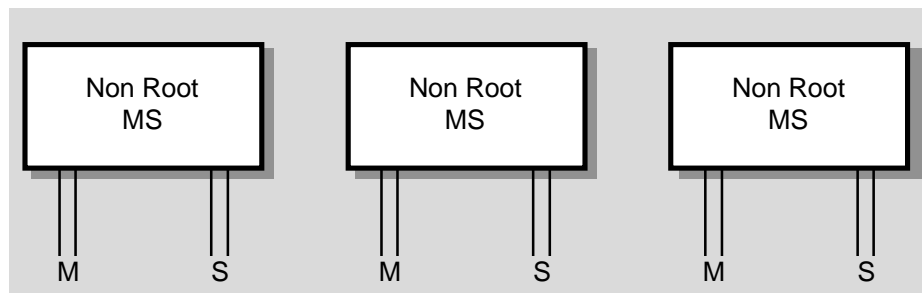
Figure 5-12 Tree Connections with Switches and Concentrators



LKG-10076-95

Figure 5-13 shows the Building block representation of the configuration example described in Figure 5-12:

Figure 5-13 Building Block Representation of Example 2



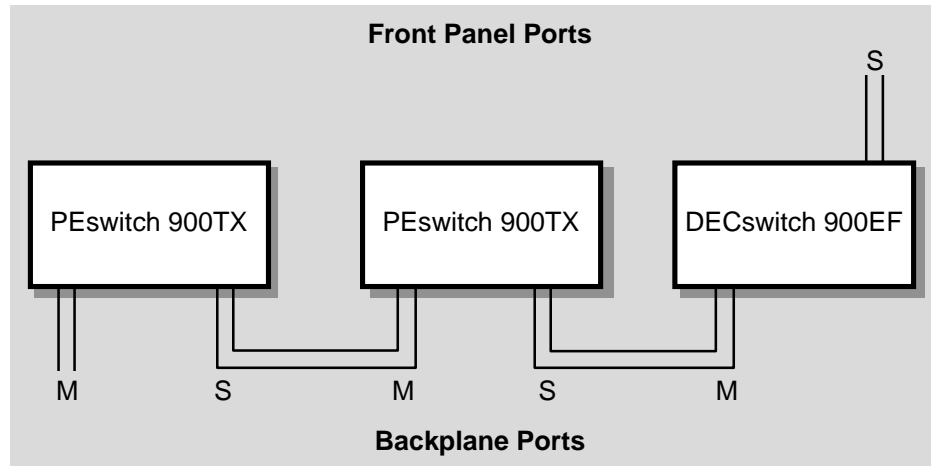
LKG-10077-95

Example 3 — Tree Connections to an External Concentrator

FDDI trees that are constructed within the Hub backplane can connect to an external higher level concentrator by configuring one of the FDDI network modules with a front panel S port, and configuring all other FDDI network modules with backplane M and S ports.

As shown in Figure 5-14, a tree of PEs switch 900TX modules can be connected to an external FDDI ring using either a DECSwitch 900EF network module (or a concentrator) to make the external connection.

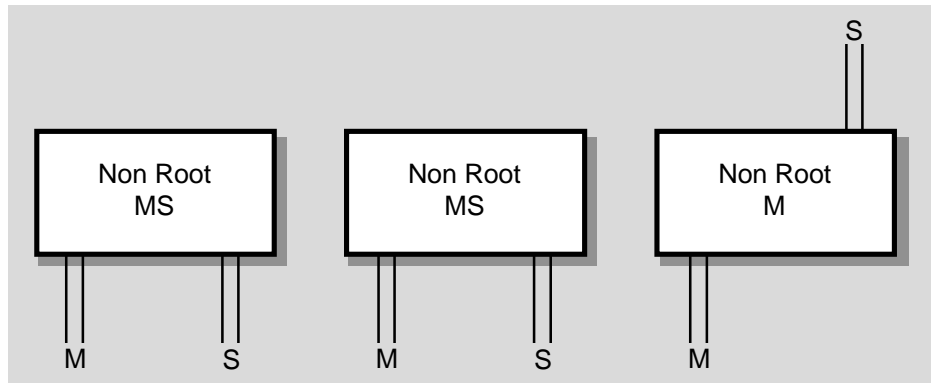
Figure 5-14 Tree Connections to an External FDDI Network



LKG-10078-95

Figure 5-15 shows the Building block representation of the configuration example described in Figure 5-14:

Figure 5-15 Building Block Representation of Example 3



LKG-10079-95

Example 4 — Dual Homing and Connection to an External Dual Ring

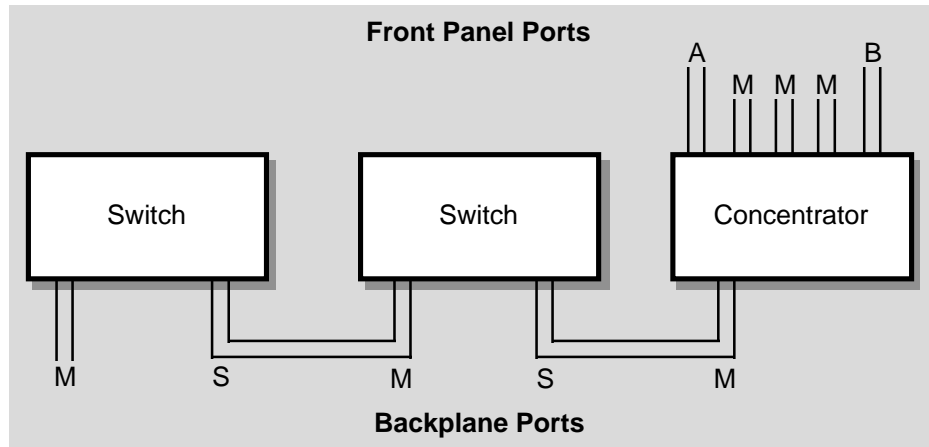
In some cases it is desirable to connect the Hub to an external dual ring, and configure the network modules as FDDI trees within the Hub backplane. In other cases, it is also desirable to have a redundant connection from the Hub to higher level concentrators.

This second case (see Figure 5-16) is commonly referred to as dual homing. Either of these configurations requires the use of a concentrator at the top level of the FDDI tree configuration.

Note

The network modules that are connected through the Hub backplane are single attachment station (SAS) modules. The term *dual homing*, in this case, refers to the connection between the hub based tree and the external concentrators.

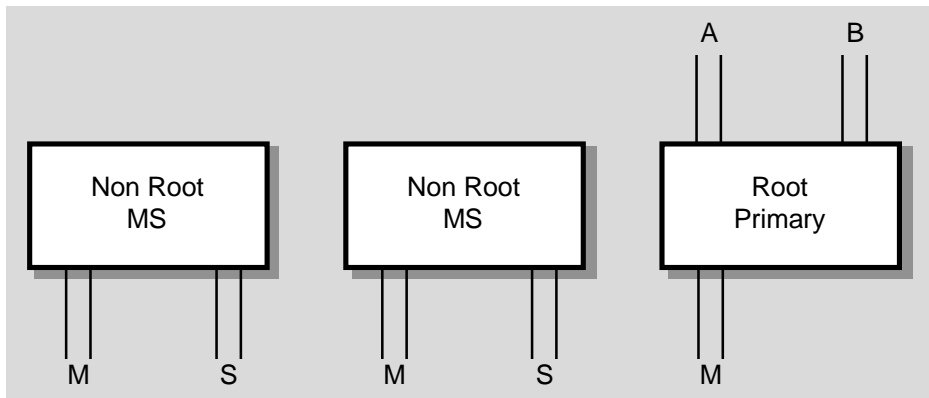
Figure 5-16 Dual Homed Connections to an FDDI Network



LKG-10080-95

Figure 5-17 shows the Building block representation of the configuration example described in Figure 5-16:

Figure 5-17 Building Block Representation of Example 4



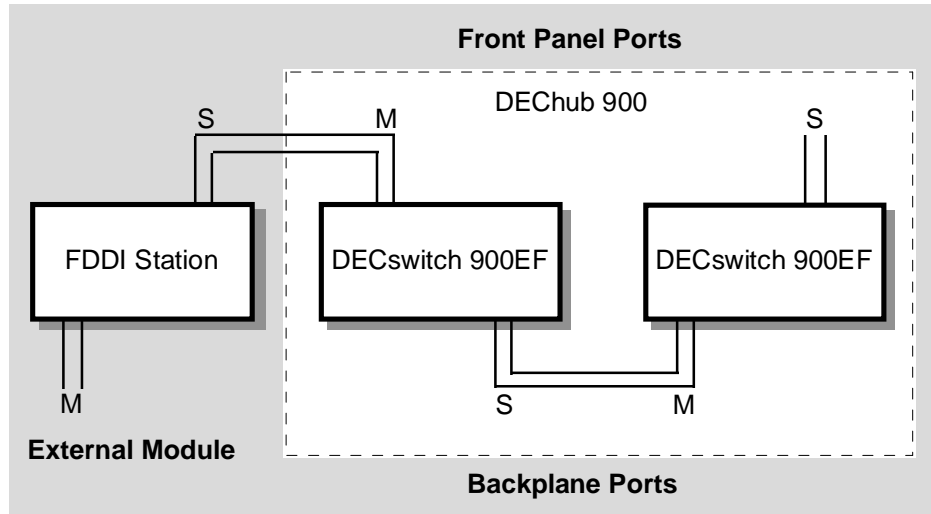
LKG-10081-95

Example 5 — FDDI Tree Extensions

You can configure an FDDI network module, that is at the end of a branch of an FDDI tree, with front panel M ports. The M port can then be used to connect to an external FDDI network module or to an additional hub (see Figure 5-18).

This configuration is used in situations where it is necessary to configure multiple hubs or hub network modules into trees (for example, when more than 8 modules are required in the same closet).

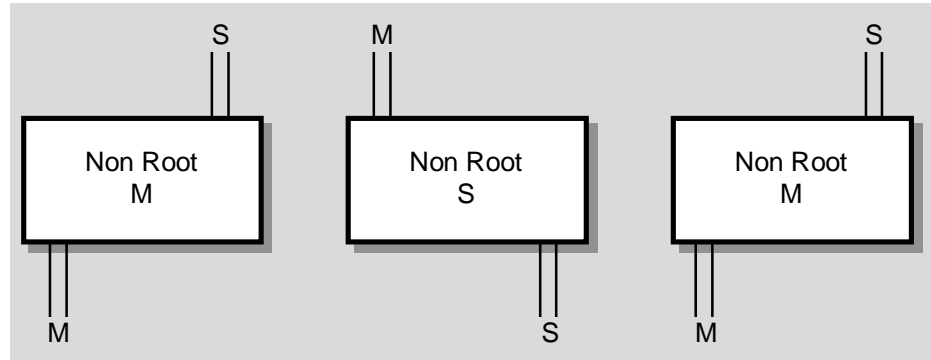
Figure 5-18 Hub-Based Tree Connections to an External FDDI Network



LKG-10082-95

Figure 5-19 shows the Building block representation of the configuration example described in Figure 5-18:

Figure 5-19 Building Block Representation of Example 5



LKG-10083-95

Dual Ring Configuration Examples

Introduction

Both dual rings and trees are supported across the DEChub 900 MultiSwitch backplane. However, because it has more robust and quicker fault tolerance capabilities than tree configurations, the dual ring configuration is more effective to use across the backplane.

This section provides 4 examples of FDDI dual ring configurations that are supported in the DEChub 900 backplane:

- Example 1 — Dual Ring Concentrators with Connection to External Dual Ring
- Example 2 — Dual Ring Switches with Connection to External Dual Ring
- Example 3 — PEs switch 900TX Connections to External Dual Ring
- Example 4 — Self Contained Dual Ring in the Backplane

Example 1 — Dual Ring Concentrators with Connection to External Dual Ring

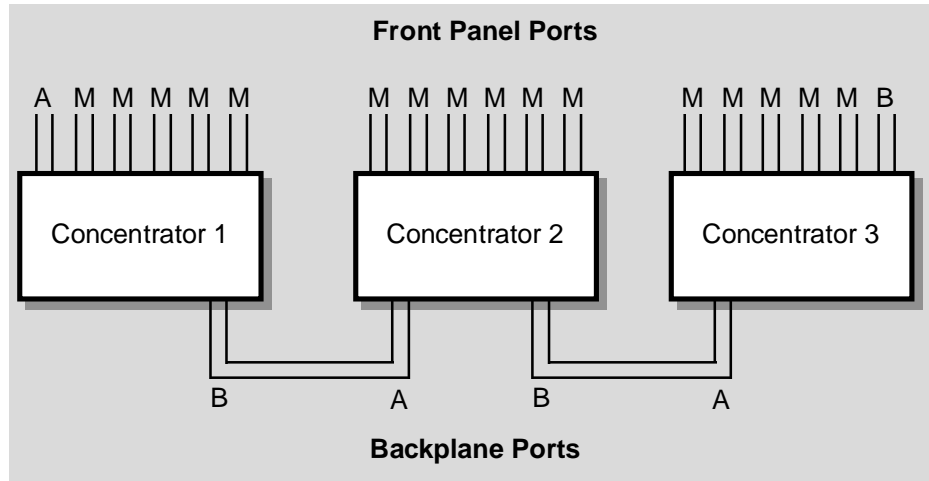
As shown in Figure 5-20, all of the concentrators connect directly to the dual ring for this dual ring configuration:

Concentrator 3 has one of its front panel ports configured as the external B port connection to the dual ring and one of its backplane ports configured as the A port.

Concentrator 2 uses both backplane ports as the A port and B port connections to the dual ring.

Concentrator 1 uses the backplane B port connection to the dual ring allowing the dual ring to exit through a front panel A port.

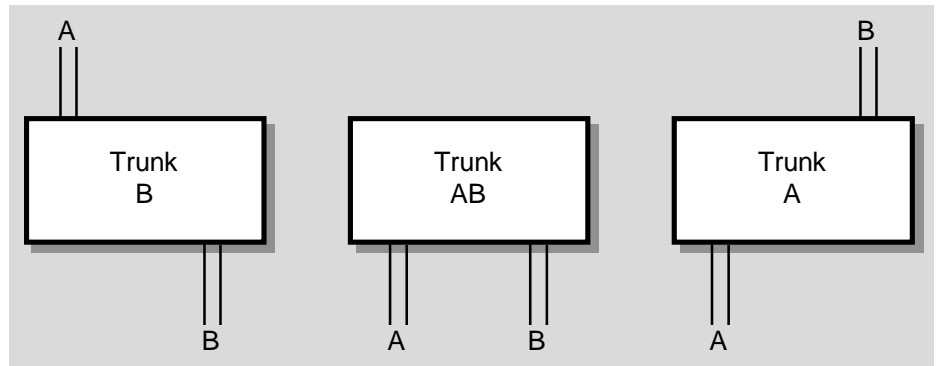
Figure 5–20 DECconcentrator Dual Ring Connections to an FDDI Network



LKG-10084-95

Figure 5-21 shows the Building block representation of the configuration example described in Figure 5-20:

Figure 5–21 Building Block Representation of Example 1



LKG-10085-95

Example 2 — Dual Ring Switches with Connection to External Dual Ring

As shown in Figure 5-22, all of the DECswitch 900EF modules (Switches 1 through 3) can connect directly to the dual ring for this dual ring configuration (similar to the concentrators shown in Example 1):

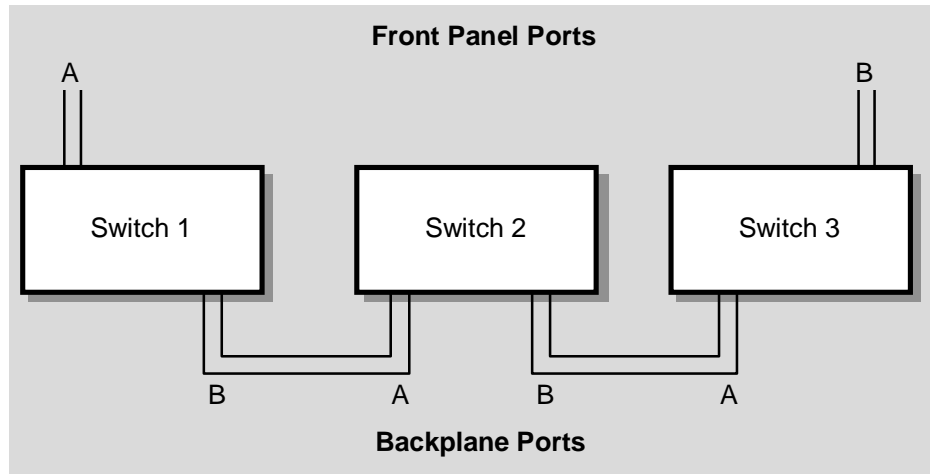
Switch 3 has its B port assigned to the front panel port connection and the A port assigned to the backplane port connection.

Switch 2 has its A and B ports assigned to the backplane ports only (the module's front panel ports are not active, nor usable).

Switch 1 has its B port assigned to a backplane port and its A port is assigned to the front panel port.

You can also assign both A and B ports to the front panel ports (the Stump Primary building block, see Figure 5-8), which allows a single DECswitch 900EF or DECconcentrator in a DEChub 900 to connect to an external FDDI backbone network.

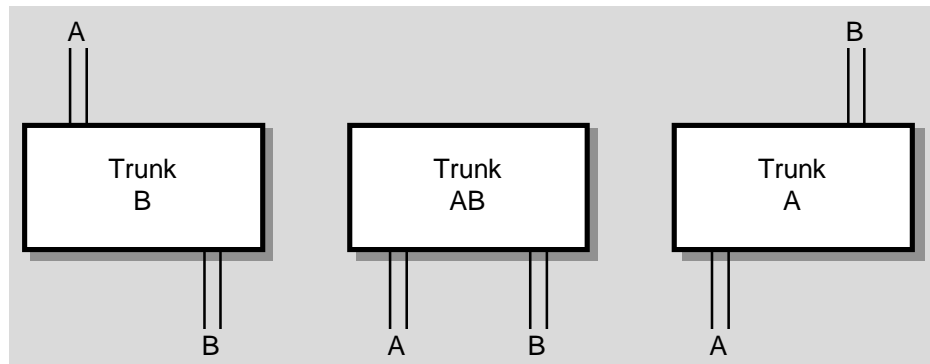
Figure 5-22 Dual Ring Connections for DECswitch 900EF



LKG-10086-95

Figure 5-23 shows the Building block representation of the configuration example described in Figure 5-22:

Figure 5-23 Building Block Representation of Example 2



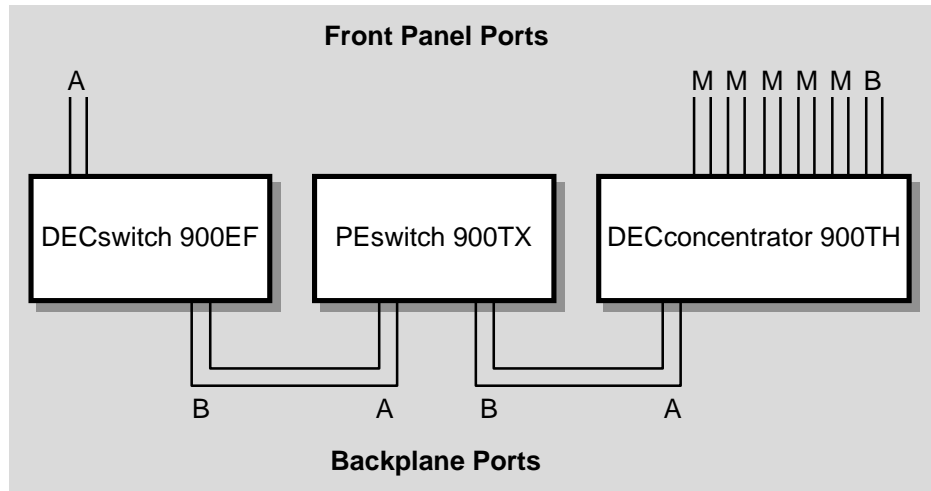
LKG-10087-95

Example 3 — PEs witch 900TX Connections to External Dual Ring

The PEs witch 900TX module can be configured into a dual ring, however, because the module does not have front panel FDDI port connectors, two DECswitch 900EF modules or two DECconcentrator modules (in any combination) are required to complete the connection to an external FDDI network.

As shown in Figure 5-24, the FDDI dual ring connections to a PEs witch 900TX are made by means of the DEChub 900 backplane: (1) the dual ring enters through the DECconcentrator 900TH; (2) it then passes through the DEChub 900 backplane to a PEs witch 900TX. (3) From the PEs witch 900TX it again passes through the DEChub 900 backplane to exit through a DECswitch 900EF.

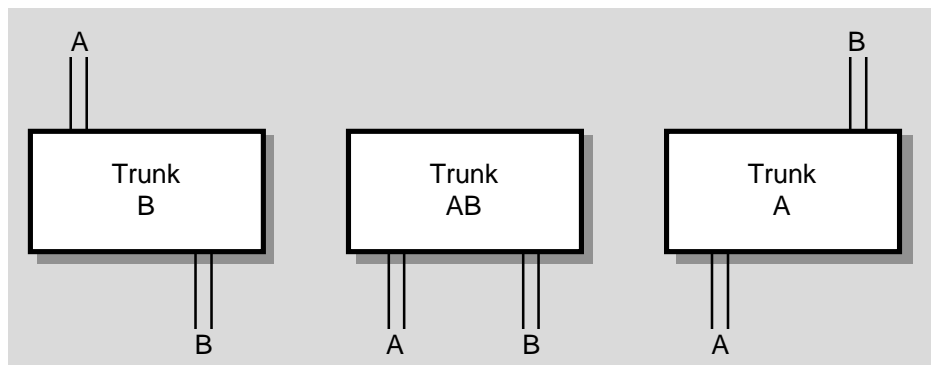
Figure 5–24 Dual Ring Connections for PEswitch 900TX



LKG-10088-95

Figure 5-25 shows the Building block representation of the configuration example described in Figure 5-24:

Figure 5–25 Building Block Representation of Example 3



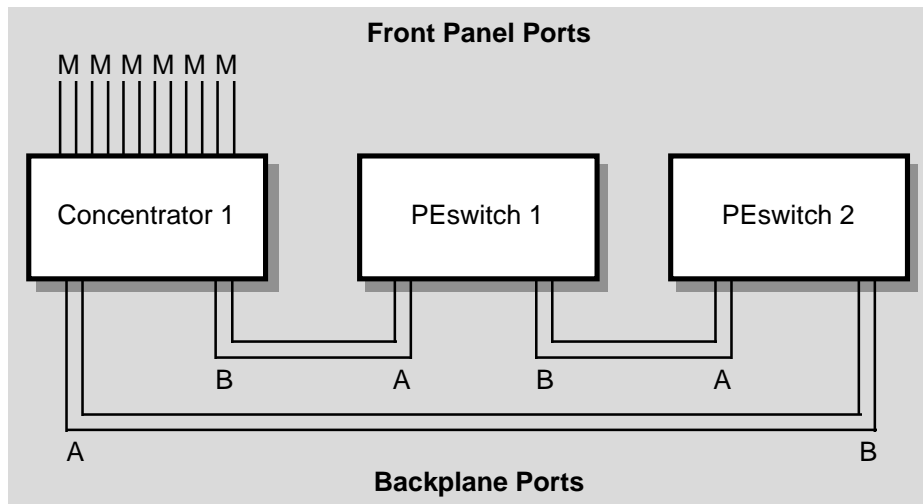
LKG-10091-95

Example 4 — Self Contained Dual Ring in the Backplane

You can create a dual ring, that is completely contained in the DEChub 900 backplane, by connecting all the backplane ports of the FDDI network modules together (see Figure 5-26).

Note that the DECconcentrator in Figure 5-26 is providing M port tree connections to externally treed FDDI stations (such as, bridges, concentrators or end user stations that use S, A, or B ports). The Concentrator is not connected to an external M port such as an external concentrator's M port.

Figure 5-26 Self-Contained Dual Ring in the Backplane



LKG-10092-95

Fault Tolerance in Dual Rings

Introduction

This section describes the fault tolerant safeguards (for dual rings) that are built into DEChub 900 network modules.

Maintaining Network Connectivity

When a concentrator or switch in a dual ring is removed (hot swapped), the FDDI ring wraps according to FDDI standards. If the removed module has both A and B ports that are connected to the DEChub 900 backplane, the Hub Manager detects the removal and reconnects the two neighboring (upstream and downstream) FDDI stations.

If a network module is detected as being unavailable, the Hub Manager will also patch-out the module (as long as Auto Healing has been enabled).

This is a distinct advantage that FDDI modules, which are configured into a dual ring in a DEChub, have over individual nonhub-based FDDI network modules.

Note

Because ring wrap occurs much faster than backplane healing, it always occurs first. Thereafter, the Hub Manager firmware automatically reconnects the disconnected DAS stations through the DEChub 900 backplane, allowing the dual ring to unwrap. Fault recovery (unwrapping of the dual ring in the DEChub 900 backplane) is supported in all DEChub 900 FDDI network modules.

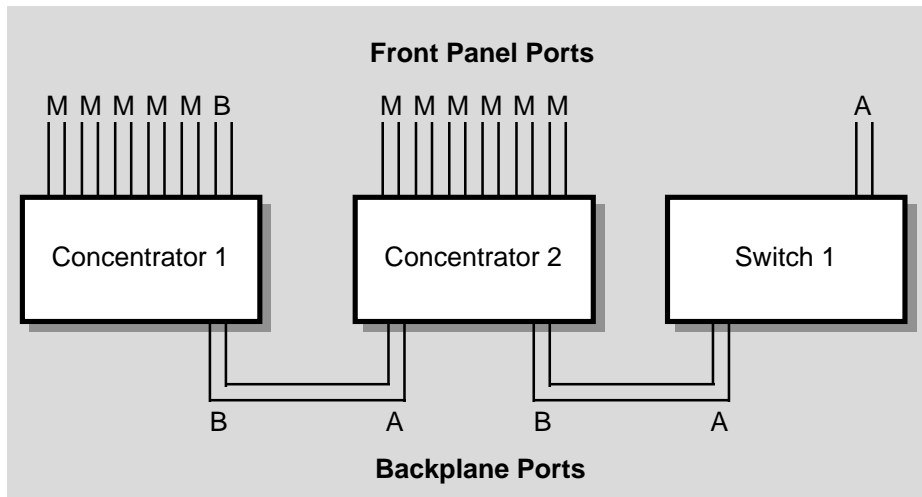
Example of Dual Ring Backplane Healing

As shown in Figure 5-27, if Concentrator 1 is removed, Concentrator 2 and Switch 1 continue communications with each other and with all other FDDI stations on the DAS backbone. This is so, because Concentrator 2 (sensing the change) wraps the FDDI dual ring.

If Concentrator 2 fails, Concentrator 1 and Switch 1 wrap the dual ring and communications can continue. Within seconds of this particular ring wrap, where Concentrator 2 has become unavailable, the Hub Manager automatically reconnects Switch 1 to Concentrator 1 and the dual ring unwraps.

If, at a later time, a replacement concentrator of the same type is installed into the same slot that held Concentrator 2, the replacement concentrator will be automatically reinserted into the ring through the Auto Healing feature.

Figure 5-27 Ring Configuration



LKG-10093-95

Fault Tolerance in Trees

Introduction

This section describes the fault tolerant safeguards (for trees) that are built into DEChub 900 network modules.

Maintaining Network Connectivity

When a concentrator or switch in a tree is removed (hot swapped), the FDDI tree splits into two independent networks, per the FDDI standard.

If the removed module has both M and S ports that are connected to the DEChub 900 backplane, the Hub Manager detects the removal and reconnects the two neighboring (upstream and downstream) FDDI stations.

If a network module is detected as being unavailable, the Hub Manager will also patch-out the module (as long as Auto Healing has been enabled).

This is a distinct advantage that FDDI modules, which are configured into a tree in a DEChub, have over nonhub-based FDDI network modules.

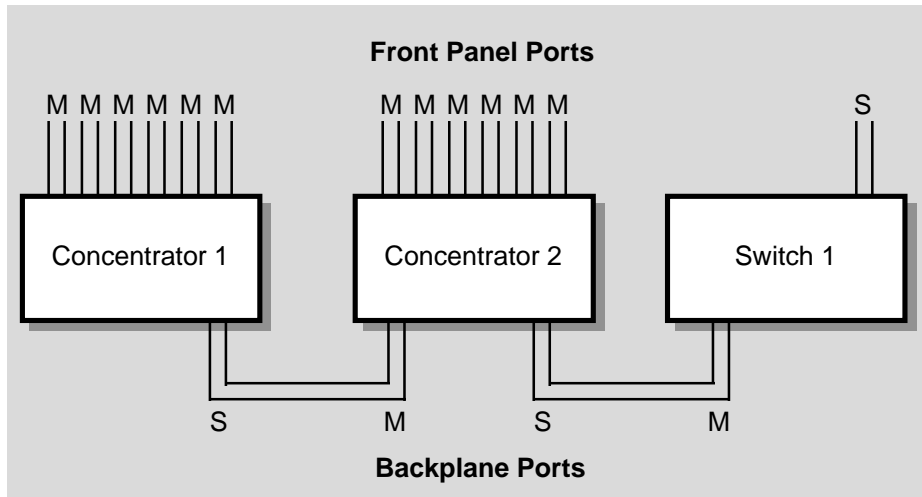
Example of Tree Backplane Healing

As shown in Figure 5-28, if Concentrator 1 is removed, Concentrator 2 and Switch 1 continue communications with each other and with all other FDDI stations in the tree.

If Concentrator 2 fails, Concentrator 1 and Switch 1 can no longer communicate with each other. Within seconds of when Concentrator 2 becomes *unavailable*, the Hub Manager automatically reconnects Switch 1 to Concentrator 1 and the tree is reestablished.

If, at a later time, a replacement concentrator of the same type is installed into the same slot that held Concentrator 2, the replacement concentrator will be automatically reinserted into the tree through the Auto Healing feature.

Figure 5-28 Tree Configuration



LKG-10125-95

Token Ordering of Trees or Dual Rings

Introduction

The DEChub 900 backplane uses a defined token order algorithm for FDDI dual rings or trees that are created in the hub. This section describes how the algorithm controls the token flow in the DEChub 900 backplane.

Token Flow Algorithm

The token flow is defined as the order in which the token flows to the MAC addressed slots in the DEChub 900 backplane. The token flow is from slot 1 towards slot 8, whether the backplane network is a dual ring or a tree. If there are multiple FDDI networks, each of the networks independently orders the token flow, from the lowest slot to highest slot, as closely as is allowed by the FDDI rules.

The token flow algorithm ensures that repaired modules return to the same token order that had been assigned prior to the occurrence of a module fault.

Note

The token flow algorithm also matches the power shedding algorithm (which sheds modules from slot 1 towards slot 8).

The following examples illustrate the concept of the token flow algorithm:

Example 1 — Token Flow Through Dual Ring Network Modules

Figure 5-29 shows a hub that is configured as a dual ring with FDDI network modules in slots 1, 2, 3, 4, 6, and slot 8.

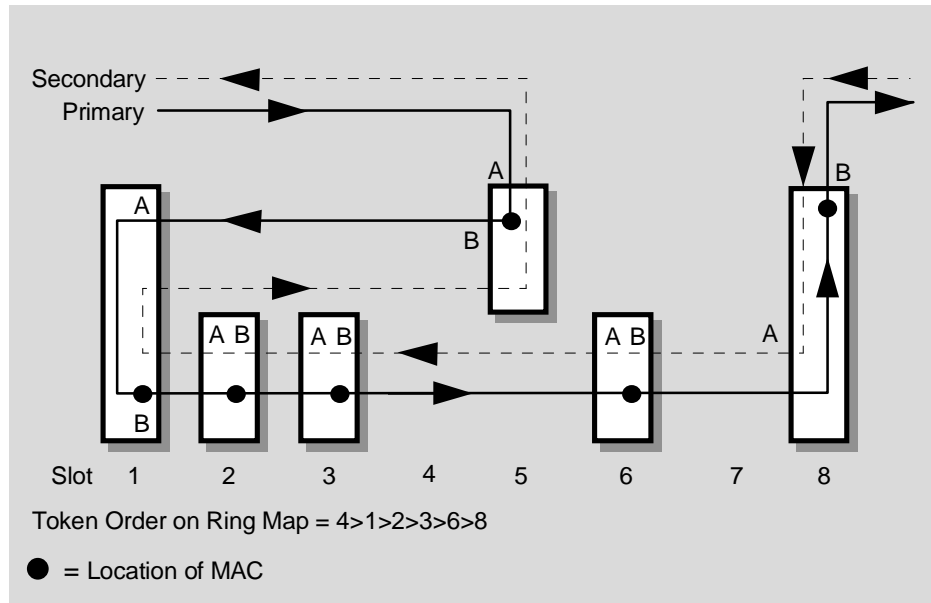
Note that the front panel A port is shown on the module in slot 4, and the B port is shown on the module in slot 8. Therefore, the token, which is flowing on the primary ring, enters the hub at slot 4 and exits from slot 8.

A ringmap, showing the order of token flow, is based on the ordering of the MACs in the ring. In this example, HUBwatch configures the backplane so that the token enters the A port of slot 4, encounters the MAC for slot 4, and the next MAC it sees is in slot 1. The token then flows, in order, through the MACs in slots 1,2,3, 6, and finally slot 8. Therefore, a ringmap records the token order as:

4>1>2>3>6>8.

To accomplish this ordering, the Hub Manager firmware automatically connects the B port of Slot 4 to the A port of Slot 1. The process is repeated for the other modules, so that the token always flows in the correct order.

Figure 5–29 Token Flow through Dual Ringed DEChub 900 Modules



LKG-10072-95

Example 2 — Token Flow Through Treed Network Modules

Figure 5-30 shows the same hub that is now configured into a tree configuration with FDDI network modules in slots 1, 2, 3, 4, 6, and 8.

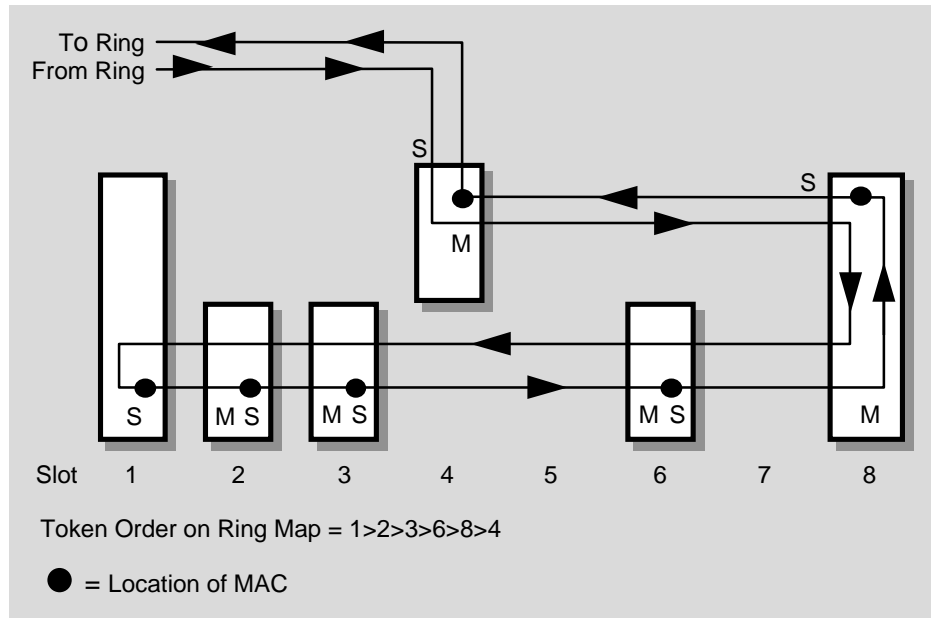
Note that the front panel S port is shown on the module in slot 4, therefore the token enters and exits the hub at slot 4.

A ringmap, showing the order of token flow, is based on the ordering of the MACs in the ring. FDDI rules require that a station's MAC be located immediately prior to the port where the token exits the station. The token enters the S port of slot 4 and flows, in order, through the MACs in slots 1, 2, 3, 6, 8 and finally slot 4. To do this the S port of slot 8 must connect to the M port of slot 4.

In this example a ringmap records the token order as:

1>2>3>6>8>4.

Figure 5-30 Token Flow through Treed DEChub 900 Modules



LKG-10073-95

Quick PC Trace Option for Concentrators

Introduction

A Quick PC Trace option is supported for all DEChub FDDI concentrator modules.

PC Trace Description

As defined by the FDDI standard, PC Trace is a method for recovering from a stuck beacon condition. All stations that are in the fault domain perform some level of hardware diagnostic test before attempting to reenter the FDDI network.

Normally, concentrator modules run their full set of hardware diagnostics. This takes approximately one minute, but gives the highest level of assurance that any hardware failure would be found.

Quick PC Trace Description

To decrease the recovery time following a trace, use the quick PC Trace option. When this option is enabled, only a subset of the hardware diagnostics is run whenever a PC Trace occurs. The reduced set of diagnostic tests completes in approximately 10 seconds. This feature can be enabled and disabled only from the configuration screen of the module's setup port.

Note

The DECswitch 900EF and the PESwitch 900TX do not have this optional feature because they normally recover from PC Traces very rapidly (less than 10 seconds). This is because they are FDDI end stations and have a much smaller set of FDDI-specific diagnostics to run than an FDDI concentrator.

Summary of Important Configuration Features

Introduction

This section reviews the FDDI configuration features of the DEChub 900 FDDI network modules:

Support for Dual Ring and Tree connections

ALL DEChub FDDI modules support dual ring connections (A and B ports) and tree connections (M and S ports) across the DEChub 900 MultiSwitch backplane, or out the front panel of individual FDDI network modules that are configured into a DEChub 900 MultiSwitch.

ALL DEChub FDDI network modules support dual ring connections (A and B ports) and tree connections (M and S ports) when configured standalone into a DEChub ONE or DEChub ONE-MX docking station.

Note

The PEs switch 900TX module does not have front panel ports and requires a DEChub ONE-MX docking station, with appropriate ModPMDs, for standalone FDDI connections.

Support for Multiple independent FDDI networks

Multiple independent FDDI networks (trees and/or dual rings) are supported across the backplane of the DEChub 900.

Support for Automatic Healing Patch-Around for Failed Modules

An automatic healing capability to patch-around failed modules is supported for both trees and dual rings across the backplane of the DEChub 900.

Support for Quick PC Trace capability

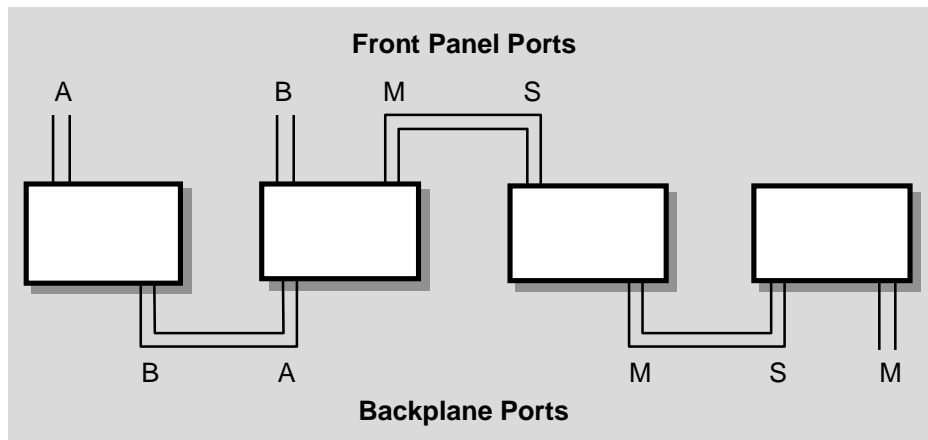
A Quick PC Trace capability has been added to concentrators, to minimize the time it takes to return to operation following a PC Trace. This option is selectable from the module setup screens, whether the module is installed in a DEChub 900, a DEChub ONE, or a DEChub ONE-MX.

Dual Ring of Trees Topology

DEChub 900s can participate in a dual ring of trees topology as either part of the dual ring *or* as part of the tree. For example, a dual ring of trees can be constructed by first building a dual ring, then a tree, and connecting them together with a cable on the front panel (see Figure 5-31).

Note that while the connections are all in one network, HUBwatch manages the connections as though they are in unconnected LANs.

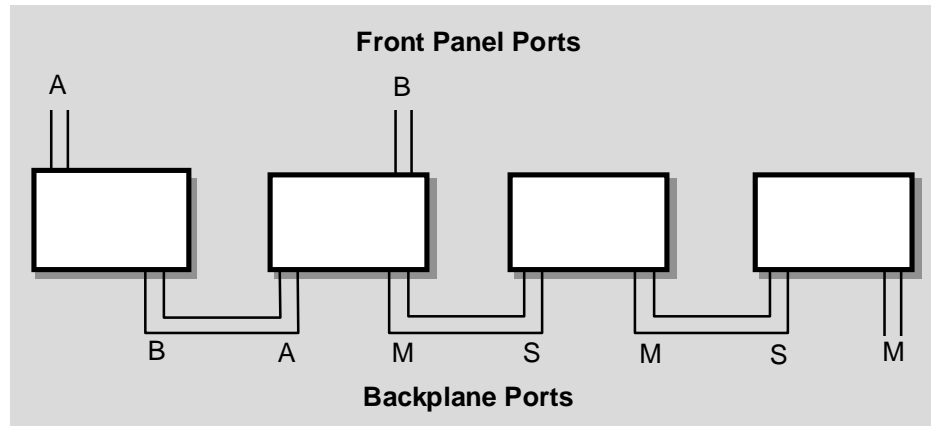
Figure 5-31 Legal Dual Ring of Trees Topology



LKG-10090-95

A dual ring of trees is *not* supported across the backplane. Figure 5-32 illustrates an illegal dual ring of trees topology.

Figure 5–32 Illegal Dual Ring of Trees Topology



LKG-10089-95

Dual Homing

Dual-homing to multiple FDDI modules in a DEChub 900 can be supported in 2 ways:

1. Each module can be individually dual-homed via its front panel ports (assuming the module has front panel ports)
2. One concentrator module can be dual-homed and the other FDDI modules can be treed off of that concentrator

Chaining

Additional DEChubs or standalone FDDI network modules can be chained off any DEChub FDDI network module (including switches) that is configured as a tree building block.

Self-Contained Dual Ring Restriction

Attempting to build a self-contained dual ring configuration in the DEChub with eight FDDI modules will not work. This is because there are 14 backplane channels that can be used for FDDI connections and 16

channels would be required to interconnect 8 modules in a hub-contained dual ring. Note that this configuration can be accomplished with 14 backplane channels *and* one DAS cable between two devices' front panel ports.

Self-Contained Tree Configuration

You can build a self-contained *tree configuration* in the DEChub 900 with eight FDDI modules. This configuration can be built because it requires only 14 backplane channels.

Network Module Front Panel Default

The FDDI defaults on the following modules are to the front panel ports:

- DECswitch 900EF
- DECconcentrator 900FH
- DECconcentrator 900MX
- DECconcentrator 900TH

The FDDI default for the PEs switch 900TX is to the backplane FDDI port. This is because there are no front panel FDDI ports on the PEs switch 900TX network module. This fact is sometimes overlooked when considering default configurations.

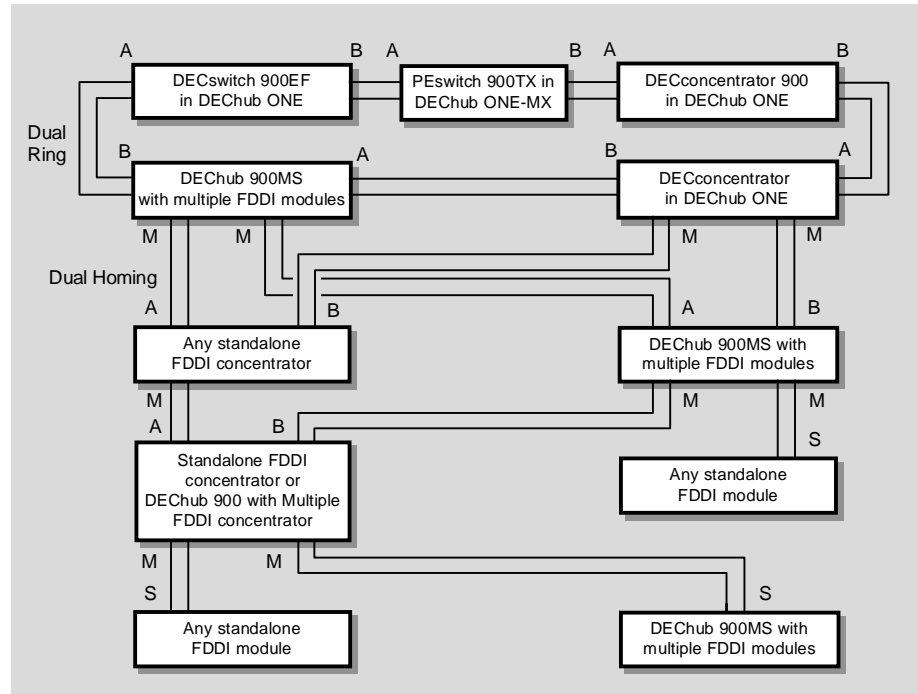
Port Configuration when in DEChub ONE-MX

FDDI network modules that are installed in a DEChub ONE-MX can configure their FDDI ports either with HUBwatch, or via an FDDI port configuration menu on the DEChub ONE-MX setup port.

Valid FDDI Configurations

Figure 5-33 shows a mixture of DEChub types with various DEChub FDDI network modules to demonstrate the flexibility of the DEChub network products:

Figure 5–33 Valid FDDI Configurations for DEChub FDDI Modules



LKG-10094-95

For More Information

Topic...	Where to Get More Information...
Features, topologies, and components of the FDDI local area network standard.	Refer to <i>A Primer on FDDI: Fiber Distributed Data Interface</i> .
Digital Equipment Corporation's DECconcentrator 900 FDDI network modules.	Refer to the <i>DEChub 900 Network Modules, Concentrator Reference manual</i> .

Appendix **A**

FDDI Overview

Overview

Introduction

Fiber Distributed Data Interface (FDDI) is a set of ANSI/ISO standards for a 100 Mbps token passing ring which uses Multimode fiber, Single mode fiber, Unshielded Twisted Pair, Screened/Shielded Twisted Pair or any combination of the four as the transmission medium. This Appendix provides an overview of the applicable FDDI standards that govern the use of FDDI network modules.

In This Appendix

The following topics are covered in this appendix:

Topic	See page...
The Dual Ring	A-3
Station Types	A-4
Media Types and Maximum Distances	A-6

(Continued on next page.)

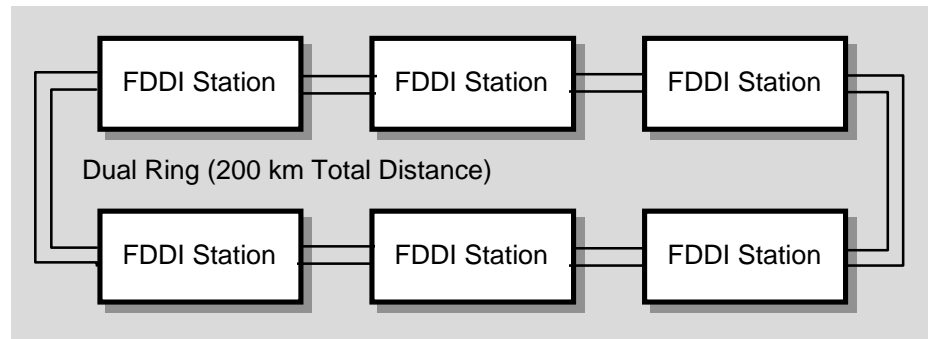
Overview

Topic	See page...
Station Configurations	A-7
Physical Topologies	A-9
Station States	A-12
Connection Rules	A-14
Ring Operation	A-18

The Dual Ring

The most basic FDDI network is constructed of two independent rings and is commonly referred to as a dual ring (see Figure A-1). A dual ring connects to each FDDI station in the network. Each ring can span up to 100 km, which allows for a distance of 200 km (2 x 100 Km/ring) for the FDDI dual ring. As many as 500 stations can be attached to the dual ring — typical configurations usually have no more than 200 stations.

Figure A-1 FDDI Dual Ring



LKG-10095-95

All FDDI networks operate as logical token rings, where the right to transmit is granted by the possession of a token. There is one token per ring, and it is passed from station to station, according to a set of rules known as the timed token protocol. A station wishing to transmit on the ring first captures the token. It then transmits frames for a period of time determined by the timed token rules, and then releases the token immediately after completing its transmission.

A transmitting station is also responsible for removing the frames it transmitted from the ring, once they have circled the ring and returned to the station. This process is called frame stripping.

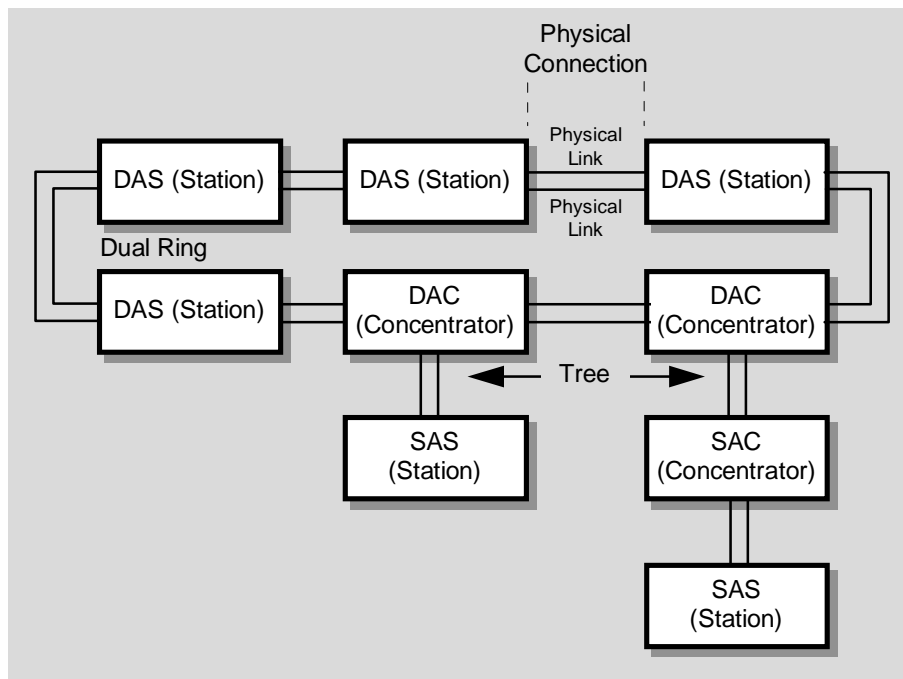
Station Types

FDDI Network Building Blocks

As shown in Figure A-2, FDDI networks are constructed using the following two types of devices:

- Stations — there are two types of stations: Dual Attachment Stations (DAS) and Single Attachment Stations (SAS).
- Concentrators — there are two types of concentrators: Dual Attachment Concentrators (DAC) and Single Attachment Concentrators (SAC).

Figure A-2 FDDI Station Types



LKG-10096-95

Dual Attachment Stations

Dual Attachment Stations (DAS) attach directly to the dual ring.

Single Attachment Stations

Single Attachment stations connect to the ring via a concentrator, that can be of two types:

- Dual Attachment Concentrator (DAC) — attaches directly to the dual ring
- Single Attachment Concentrator (SAC) — attaches to the ring through other concentrators.

Physical Connection

As shown in Figure A-2, all devices, whether they are single attachment stations or dual attachment stations, connect to each other via a full-duplex connection, called a physical connection.

Each physical connection comprises two physical links (a single fiber-optic cable for each physical link):

- Single Attachment Stations and Single Attachment Concentrators connect to a concentrator, or to another station, via one physical connection.
- Dual Attachment Stations and Dual Attachment Concentrators connect to each other via two physical connections.

Media Types and Maximum Distances

Important Characteristics

FDDI allows links to be built from the following media types.

Fiber Media	Fiber Type (Microns)	Power Budget (decibels)	Maximum Link Distance (Kilometers)
Multimode Fiber (MMF)	62.5/125	11	2.0
Singlemode Fiber (SMF)	8-to-10/125	22	60

Copper Media	Copper Type	Maximum Link Distance
Unshielded Twisted Pair (UTP)	100 ohm Category 5 Twisted Pair	100 meters
Screened Twisted Pair	100 ohm Category 5 Twisted Pair	100 meters
Shielded Twisted Pair	150 ohm Category 5 Twisted Pair (equivalent to IBM Type 1 cable.)	100 meters

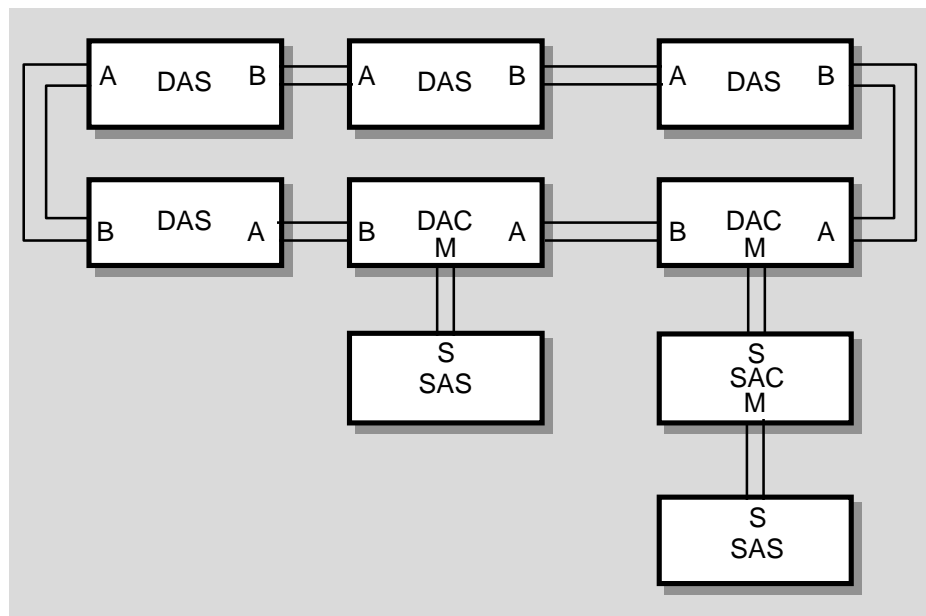
Station Configurations

Identifying Stations and Concentrators

Stations and Concentrators (see Figure A-3) can be identified by the types of ports that they use to attach to other stations:

- **A and B Ports** — Dual Attachment Stations have A and B ports for attachment to other stations in the dual ring, or to concentrator M ports.
- **M Port** — All concentrators, (SAC or DAC), are identifiable by the presence of M ports. The M port allows the attachment of other stations or concentrators.
- **S Port** — If the concentrator also has an S port, it is a SAC; if it has A and B ports it is a DAC. A Single Attachment Station has an S port for connection to a concentrator M port.

Figure A-3 FDDI Port Types



LKG-10097-95

MAC Location

The FDDI rules require that a station's Media Access Control (MAC) be physically located immediately prior to the port where the token exits the station. For Dual Attachment devices this means that the MAC is immediately ahead of the B port; for Single Attachment devices it is immediately ahead of the S port.

Physical Topologies

Topology Types

Although all FDDI networks are logical rings, the following physical topology types can be created:

- Dual Rings
- Trees
- Dual Ring of Trees

Dual Ring Topologies

Dual Ring topologies (as shown in Figure A-1) are created by connecting only Dual Attachment Stations. The A port of one DAS station connects to the B port of the next DAS station, forming a physical connection between the two stations. The connections can continue until up to 500 stations are included in the dual ring.

Independent Rings

Because there are two physical links per physical connection (see figure A-2), two operating links are created between each DAS station when the ring is formed. This design allows for two independent rings, the primary ring and the secondary ring, to be formed.

The primary ring enters the DAS station at the A port, and exits the DAS station at the B port. The secondary ring enters the DAS station at the B port and exits the DAS station at the A port.

Backup Benefit:

In general, all data traffic between stations is carried on the primary ring and the secondary ring is idle during this time. The FDDI standards allow both rings to be used for carrying data traffic, but in practice this is rarely done. The common practice is to use the secondary ring as a backup for the primary ring.

A benefit of having dual rings is that, in case of a failure, the secondary ring can be used to patch the primary ring. If a station detects that one of its A or B ports has failed, it wraps the primary and secondary rings together, thus restoring operation to the other stations in the ring. Wrapping occurs very quickly, usually in well under a half a second.

Tree Topologies

FDDI also allows for the creation of tree topologies. Tree topologies start with a standalone concentrator at the top of the tree. Stations (DAS or SAS) or other concentrators (DACs) connect to this concentrator, and branch out from the top of the tree.

How to Identify Trees

The distinguishing feature of a tree topology is the connection to an M port. Single attachment stations (S ports) typically connect to a concentrator, but Dual Attachment Stations (A and B ports) can also connect to the M ports.

Benefit:

A major advantage of the use of trees built with concentrators is the ability of the concentrator to electronically disconnect stations from the ring in case of failure, or, by management control.

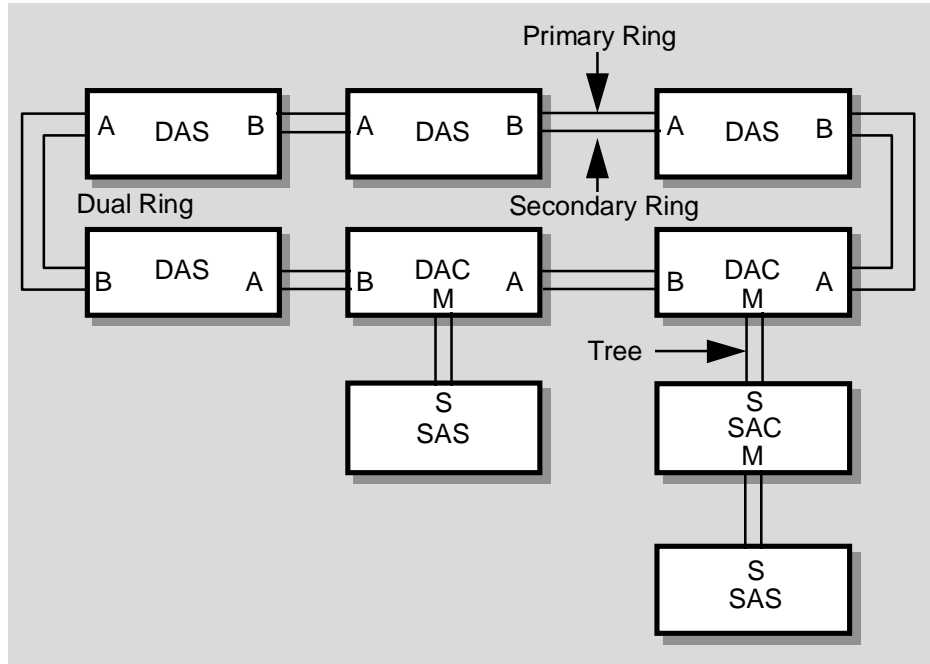
Dual Ring of Trees Topology

The third, and most common, FDDI configuration (see Figure A-4) is referred to as the Dual Ring of Trees. This configuration type is a very robust topology and is a hybrid of the Dual Ring and Tree topologies.

How to Identify Dual Ring of Trees:

Dual Attachment Concentrators (DACs) and Dual Attachment Stations (DASs) attach together in a dual ring, with treed stations connected to the concentrators' M ports. The concentrator connects stations attached to these M ports into the flow of the primary ring.

Figure A-4 FDDI Topologies



LKG-10098-95

Station States

Definition

The station state is defined by FDDI standards as: the internal configuration of the paths *within* the station. Stations can be in one of two states: the Through state or the Wrap state (see Figure A-5).

For example, DAS or DAC stations that are in an (unwrapped) dual ring are in the Through state. If a station detects a failure, causing it to *wrap* the rings together, that station transitions to the Wrap state.

FDDI Naming Convention

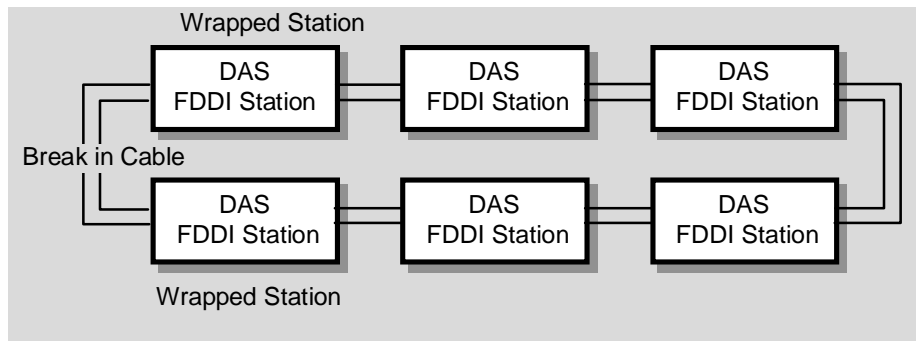
When transitioning to the Wrap state, the station can adjust its internal configuration in a number of ways that are specified by the FDDI standard. The FDDI standard requires that each station configuration type has a specific naming format, and that the station is required to use that specific naming format when reporting internal configuration status to management.

- All Digital SAS and SAC devices report: wrap_S
- All Digital DAS and DAC devices in the wrapped state report: c_wrap_A (concatenated wrap A) or c_wrap_B (concatenated wrap B)

Where c_wrap_A indicates: concatenated wrap A.

To explain further, c_wrap_A means that the B port is not active, the station has wrapped the ring, and the A port is the active port.

Figure A-5 Wrapped FDDI Ring



LKG-10099-95

FDDI Connection Rules

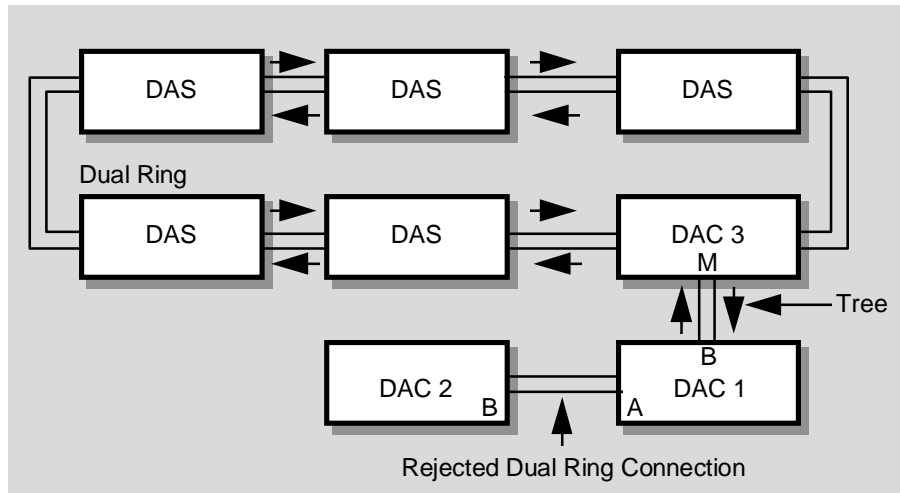
Predictability

FDDI connection rules can seem complex and sometimes confusing, however, once clarified and understood, one can easily see how the applied rules prevent the formation of non-useful topologies that can disrupt communications among stations in the ring. FDDI connection rules also ensure that the ring always converges to a pre-defined topology.

For example, as shown in Figure A-6, if Port A (DAC 1) is connected to Port B (DAC 2), and then Port B (DAC 1) is connected to an M-port of (DAC 3), Port A (DAC 1) breaks its connection to Port B (DAC 2).

This behavior is referred to as taking the tree connection over the ring connection. This particular rule ensures that the same topology is always formed, independent of the order in which the physical connections are made.

Figure A-6 FDDI Connection Rules



LKG-10100-95

How Rings are formed

FDDI rings are formed by the completion of physical connections between pairs of ports. The ports signal various parameters that are necessary for the successful completion of the connections.

When a port attempts to form a connection with another port, it indicates both its own port type, and whether it wishes to form a connection with the port type that it senses at the other end of the link.

Undesirable Connections

One type of connection, the M Port-to-M Port connection, is always rejected. Other types of connections, such as A port to A port and B port to B port connections are undesirable, but can be formed if the connection rules of one of the stations allows the connection.

Example

For example, if a Digital FDDI product attempts to form an A port to A port connection with another Digital FDDI product the connection is rejected.

The connection is rejected because Digital products are designed to avoid connection to similar ports (both ports signal that they do not wish to connect to a remote A port).

If the Digital FDDI product attempts to form an A port to A port connection to a non-Digital station, and the non-Digital station's A port signals that it wants to accept the connection to the Digital A port, the Digital station honors the request (per the ANSI standard's rules for connection of ports).

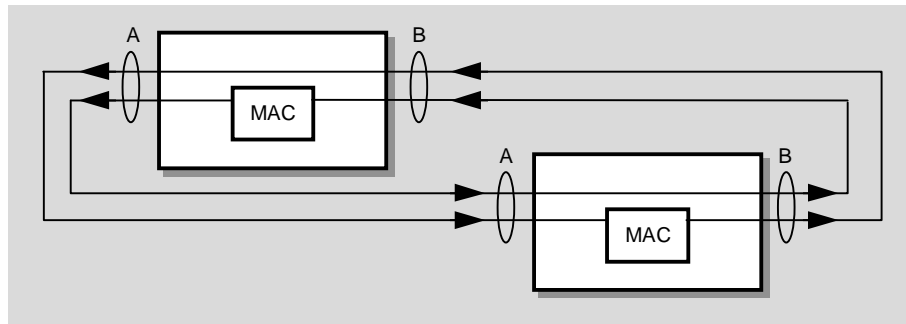
The result of this type of connection is graphically shown in the following subsection.

Result

The resulting configuration (see Figure A-7) is that, although the stations are connected, one station's MAC address is in the primary ring, and the other station's MAC address is in the secondary ring.

Because the rings are isolated when in the Through state, the stations are unable to communicate, even though their ports have formed a valid physical connection.

Figure A-7 Connecting to Similar Ports



LKG-10021-95

Summary of FDDI Connection Rules

Table A-1 summarizes the FDDI connection rules.

Table A-1 FDDI Connection Rules and Station States

Port A	Port B	Topology	Station State
M	—	Tree	c_wrap_A
—	M	Tree	c_wrap_B
M	M	Tree	c_wrap_B (Dual Homed)
B	—	Peer ¹	c_wrap_A
—	A	Peer ¹	c_wrap_B
B	A	Peer ¹	Through
A	—	Peer ¹	c_wrap_A
—	B	Peer ¹	c_wrap_B
S	—	Peer ¹	c_wrap_A
—	S	Peer ¹	c_wrap_B
S	S	Peer ¹	Through
S	M	Tree	c_wrap_B (Tree Preference) ²
M	S	Tree	c_wrap_A (Tree Preference) ²
S	A	Peer ¹	Through
B	S	Peer ¹	Through
B	M	Tree	c_wrap_B (Tree Preference) ²
M	A	Tree	c_wrap_A (Tree Preference) ²

¹ Indicates dual ring connection.

² Tree topology always takes precedence over ring topology when simultaneous or conflicting connections are made.

Ring Operation

Overview

FDDI rings operate according to the rules of the Timed Token Protocol.

The operation of the ring can be divided into two states:

1. Ring Initialization State
2. Steady State Operation

Ring Initialization State

The FDDI ring is initialized by a process known as the *claim token process*, that is invoked whenever a station enters or exits the ring, or if a failure of the normal ring operation is detected. The purpose of the claim token process is to set the operational timers for the ring, and to choose a station that is responsible for creating the token.

Claim Token Process

All stations send a special frame, known as a *claim frame*, containing a bid for the length of time that the station is willing to wait between receipt of tokens. The station that wins the bidding is the station whose bid indicates that it needs the token the most often. If the outcome of the bidding indicates a tie, the station with the highest MAC address wins.

The outcome of the claim process is that all stations agree to abide by this time period, which is known as T_Negotiated (T_Neg). Typical values for T_Neg are in the range of 5-10 ms, with 8 ms being a common choice.

Varying the value of T_Neg can dramatically change the utilization and latency of a very busy FDDI ring, but it has minimal affect on the utilization or latency of a lightly loaded ring. Digital recommends not changing the value of T_Neg from the device manufacturer's default setting.

Beacon Process

If a ring fails to complete the claim process within a certain time, the ring enters the *beacon process*. The beacon process causes special frames known as *beacon frames* to traverse the ring in an attempt to isolate the location of the fault.

Understandably, when beacon frames are detected traversing the ring, it usually indicates a serious problem with the operation of the ring.

Steady State

In the steady state, the token circulates around the ring. The time for a token to circle once around the ring without being used by anyone is known as the *token latency*. Stations that wish to transmit must capture the token, and can transmit as long as allowed by the token holding rules.

All stations keep a timer called *the valid transmission timer (TVX)* which they use for timing valid activity on the ring. If, for any reason, a token gets lost, the TVX timer expires, and all stations enter the claim process to elect a new token.

During the Steady State, all stations in the ring exchange frames that report their adjacent stations. This information is communicated via Station Management (SMT) frames, that are sent at a rate of approximately 1 every 10 to 30 seconds.

Using these frames, all stations on the ring determine their upstream and downstream neighbors. For example, Station 2 is said to be downstream of Station 1 if Station 2 receives the token after it was received by Station 1.

For More Information

Topic...	Where to Get More Information...
Features, topologies, and components of the FDDI local area network standard.	<i>Fiber Distributed Data Interface, An Introduction (Digital Press)</i> <i>Fiber Distributed Data Interface (Order No. EK-DFSLD-SD-002)</i> <i>FDDI Handbook, Raj Jain</i>
Digital Equipment Corporation's DECconcentrator 900 FDDI network modules.	Refer to the <i>DEChub 900 Network Modules, Concentrator Reference manual</i>

Appendix **B**

Accessing MIBs and RFCs

Overview

Introduction

This appendix describes how to access this product's online release notes, public MIBs, Digital's private MIBs, firmware images, and requests for comments (RFCs).

Accessing Online Information

You can access this information from Digital's Internet ftp server at:

`ftp.digital.com (16.1.0.2)`

To Access...	Use...
MIBs, release notes, and firmware update files.	Anonymous ftp
MIBs and release notes	ftpmail
RFCs	Electronic mail

Using Anonymous ftp

You can access any of Digital's DEChub MIBs, firmware update files and release notes over the Internet by using ftp.

When you use ftp, you must include the following parameters:

- Connect to `ftp.digital.com`
- For a username, enter `anonymous`
- For a password, enter your Internet mail address, for example:

`name@system.company.com`

- Change directory to:

`/pub/DEC/hub900/<directory_name>`

(See Table B-1 for a list of directory names.)

Table B-1 Directory Names Available

Name	Contents¹
mibs	DEChub MIBs
firmware	DEChub firmware images
firmware/hubloader	HUBloader utility
release	DEChub product release notes

¹ Digital suggests reading the README file in each directory to understand the contents of that directory.

You can also access these directories from the World-Wide Web using a browser. The Universal Resource Locator (URL) is as follows:

```
file://ftp.digital.com/pub/DEC/hub900/
```

The following example shows how to copy a README file. User input in the example is shown underlined.

Note

User input is case sensitive; you must type it as shown.

```
% ftp ftp.digital.com
Connected to ftp.digital.com
220 FTP.DIGITAL.COM FTP Service Process
Name: anonymous
331 ANONYMOUS user ok, send real ident as password.
Password: milano@netman.stateu.edu
230 User ANONYMOUS logged in at Tue 10-May-1994 10:24-EST, job 54.
ftp> cd /pub/DEC/hub900/<directory_name>
331 Default name accepted. Send password to connect to it.
ftp> ascii (See note below.)
220 Type A ok.
ftp> get README
200 Port 19.54 at host nnn.nn.nn.nn accepted.
150 ASCII retrieve of /pub/DEC/hub900/mibs/README started.
226 Transfer completed. 40239 (8) bytes transferred.
40239 bytes received in 23.65 seconds (5.8 Kbytes/s)
ftp> quit
%
```

Note

To transfer binary files, such as firmware updates, replace the `ascii` command shown in this example with `binary` or `image`.

Using ftpmail

Digital offers Internet ftpmail access to private MIB and release note information, in ASCII text form, at `ftp.digital.com`, with up-to-date documents stored in:

```
/pub/DEC/hub900/<directory_name>
```

(See Table B-1 for a list of directory names.)

To use ftpmail, complete the following steps:

Step	Action
------	--------

1	Send a mail message to <code>ftpmail@ftp.digital.com</code> .
---	---

2	Ignore the subject line.
---	--------------------------

3	Include the word <code>connect</code> in the first line of the body.
---	--

4	Include <code>get</code> commands for each document required, for example:
---	--

```
get /pub/DEC/hub900/<directory_name>/README
```

(See Table 1 for a list of directory names.)

5	<code>quit</code>
---	-------------------

Requests are acknowledged, then queued and processed every 30 minutes. Because of the number of requests, it may take a day or two before you receive a reply.

Note

For more timely access, consider using anonymous ftp. Refer to the section titled `Using Anonymous ftp`.

Using Electronic Mail

The DDN Network Information Center (NIC) of SRI International provides automated access to NIC documents and information through electronic mail. This is especially useful for people who do not have access to the NIC from a direct Internet link, such as BITNET, CSNET, or UUCP sites.

To use the mail service, complete the following steps:

Step	Action
1	Send a mail message to SERVICE@NIC.DDN.MIL.
2	In the SUBJECT field, request the type of service that you want, followed by any needed arguments.

Normally the message body is ignored, but if the SUBJECT field is empty, the first line of the message body is taken as the request.

The following are example SUBJECT lines to obtain DDN NIC documents:

```
HELP
RFC 822
RFC INDEX
RFC 1119.PS
FYI 1
IETF 1IETF-DESCRIPTION.TXT
INTERNET-DRAFTS 1ID-ABSTRACTS.TXT
NETINFO DOMAIN-TEMPLATE.TXT
SEND RFC: RFC-BY-AUTHOR.TXT
SEND IETF/1WG-SUMMARY.TXT
SEND INTERNET-DRAFTS/DRAFT-IETF-NETDATA-NETDATA-00.TXT
HOST DIIS
```

Requests are processed automatically once a day. Large files are broken down into separate messages.

Appendix C

The Spanning Tree

Overview

Introduction

This appendix provides an overview of the spanning tree algorithm, a process that is used by Digital's 900-series switches and bridges that implement the IEEE 802.1d MAC Bridge specification. In this section, the terms switch and bridge imply the same meaning.

For a detailed description of the spanning tree, see the *Bridge and Extended LAN, Reference Manual*.

The following topics are covered in this appendix:

Topic	See page...
The Spanning Tree Algorithm	C-2
The Spanning Tree Computation Process	C-4
Bridge Spanning Tree Parameters	C-7
Port Spanning Tree Parameters	C-13

The Spanning Tree Algorithm

Introduction

Every extended LAN of any mesh complexity is logically configured into a network topology called a spanning tree. This is accomplished by a continuous, distributed process that is determined by the spanning tree algorithm. The algorithm ensures that the configuration contains no loops (that there is only one path between any two nodes) and that all LANs are connected.

Although the spanning tree algorithm is continuous and self-maintaining, some parameters can be set by management. Other parameters cannot be set but are determined by the spanning tree computation process and can be displayed by management. Chapter 4 of this manual provides examples of spanning tree displays and settable parameters.

This section discusses the two different implementations of the spanning tree algorithm used by Digital's switches and bridges, the properties of the algorithm, and how the algorithm computes the spanning tree.

Implementations of the Spanning Tree Algorithm

Digital bridges use either of two implementations of the spanning tree algorithm: the implementation used by Digital's LAN Bridge 100 or the implementation described by the IEEE 802.1d MAC Bridge specification. Both implementations produce identical spanning tree logical configurations for any network configuration.

Properties of the Spanning Tree Algorithm

The spanning tree algorithm has the following properties:

- **Loop detection** — If bridges (or switches) are accidentally or deliberately configured into a loop, the algorithm computes a loop-free topology that still spans the entire network.
- **Automatic backup (using redundant bridges)** — Bridges can be deliberately configured in a redundant path so that one of the bridges in the loop can serve as the backup for another. The process automatically configures a redundant bridge as a backup bridge. The backup bridge does not forward frames.
- **Determinism** — A fixed set of rules controls the process so that when variables change, the results are predictable.
- **Low network overhead** — The messages that control the spanning tree are usually transmitted at 1-second intervals (default), thus using a very small percentage of the available network bandwidth.
- **Management** — The algorithm allows tuning of parameters by management to control the topology.

The Spanning Tree Computation Process

Introduction

The spanning tree computation process is a continuous process that sets up the spanning tree when bridges are initialized and maintains the spanning tree thereafter.

Establishing the Spanning Tree

Establishing the spanning tree involves these steps:

Step	Action
1	Bridges in the extended LAN elect a unique root bridge.
2	Bridges in the extended LAN elect a designated bridge for each LAN.
3	Redundant paths are removed from the logical spanning tree.

The spanning tree is self-maintaining, and performs these functions after it is established:

- Replaces a failed forwarding bridge with a backup bridge.
- Removes a redundant bridge when a loop is detected.
- Maintains address timers that control the aging of forwarding database address entries.

How Bridges Communicate with Other Bridges

The spanning tree algorithm is a distributed process in which all bridges in the extended LAN participate. Each bridge maintains information about itself and the spanning tree in databases: one database for the bridge spanning tree parameters and one database for each bridge port for port spanning tree parameters. These parameters are used for computing the spanning tree and for providing results of the spanning tree computation.

Bridges communicate with each other with a minimum-size packet called a Hello message, referred to in the IEEE 802.1d specification as a Configuration Bridge Protocol Data Unit (BPDU).

The Hello messages provide the following information:

Attribute	Meaning
Best Root	The Best Root parameter indicates the bridge ID that this bridge believes is the root bridge. In the 802.1d specification, the name for this parameter is Designated Root.
My Cost	The cost of the path to the root from the bridge that is transmitting the Hello messages.
Bridge ID	The unique identifier of the bridge that is transmitting the Hello messages.
Port ID	The unique identifier of the port on which the Hello message was transmitted.
Root Age	Indicates the age, in seconds, of the last Hello message sent by the designated root. This parameter is referred to as the Message Age in the 802.1d specification.
Actual Forward Delay	The length of time interval that the port spends in the Preforwarding state before entering the Forwarding state. In the IEEE 802.1d specification, the Actual Forward Delay is equivalent to the first half of the Forward Delay used in the Digital LAN Bridge 100 implementation, and is the time spent by the bridge in each of the Listening and Learning states before transitioning into the Forwarding state.

(Continued on next page)

Attribute	Meaning
Actual Listen Time	Specifies the age of a Hello message (in seconds), after which the bridge considers the message to be stale. This parameter is referred to as the Max Age in the 802.1d specification.
Actual Hello Interval	Specifies the value of an interval timer that controls how often a bridge sends a Hello message.
Hello Flags	Flags used by the designated bridge to notify other bridges of an impending topology change.

Per-Port Control of Spanning Tree Algorithm

The DECswitch 900EE, the DECswitch 900EF, and the PEs switch 900TX switches provide the ability to turn off the spanning tree selectively on individual ports. These switches accomplish this by using an SNMP MIB object that can be set by HUBwatch (refer to the section titled Enabling and Disabling the Spanning Tree on Ports, in Chapter 4 of this manual).

When the spanning tree algorithm is turned off on a port, that port no longer participates in the spanning tree computation process. No Hello messages are transmitted on the port, and any Hello messages that are received on the port are discarded. This feature helps in setting up isolated spanning tree domains (where topology changes in one domain do not affect the other domains, and connectivity between the domains is still maintained).

For example, to set up two isolated spanning tree domains, start with two extended LANs with no connectivity between them. Next, turn off the spanning tree algorithm on one switch port on each of the extended LANs. Establish connectivity between these two ports by connecting them together, while ensuring that there are no other paths between the two extended LANs.

Bridge Spanning Tree Parameters

Introduction

Bridge spanning tree parameters describe and determine the spanning tree. Several bridge spanning tree parameters can be set with bridge management; others cannot be set but are determined by the spanning tree computation process and can be displayed with bridge management.

This section describes all of the bridge spanning tree parameters.

Actual Forward Delay

The Actual Forward Delay parameter indicates the Forward Delay currently in use by the root bridge. The Forward Delay for a bridge may be set with bridge management, but once the spanning tree computation process is complete, the bridge uses the root bridge's Forward Delay. If the bridge becomes the root bridge, its Forward Delay value becomes the Actual Forward Delay for all bridges in the network.

During the first half of the Forward Delay, bridges send and listen to Hello messages, participating in the spanning tree computation process. During the second half, bridges examine frames received on both ports, adding station address entries in their forwarding databases (this is the Learning state).

Actual Hello Interval

The Actual Hello Interval parameter indicates the Hello interval currently in use by the root bridge. The Hello Interval parameter for a bridge may be set with bridge management, but once the spanning tree computation process is complete, each bridge uses the root bridge's Hello Interval parameter value. If the bridge becomes the root bridge, its Hello Interval parameter value becomes the Actual Hello Interval for all bridges in the network.

Actual Listen Time

The Actual Listen Time parameter indicates the Listen Time currently in use by the root bridge. The Listen Time for a bridge may be set with bridge management but, once the spanning tree computation process is complete, the bridge uses the root bridge's Listen Time. If the bridge becomes the root bridge, its Listen Time value becomes the Actual Listen Time for all bridges in the network.

Bad Hello Limit

The Bad Hello Limit parameter specifies the number of successive Hello intervals during which a bridge may receive bad Hello messages before the bridge performs a link test on the port. A bad Hello message may indicate a port problem. The Bad Hello Limit parameter works with other spanning tree parameters.

Bad Hello Reset Interval

The Bad Hello Reset Interval parameter specifies how many Hello intervals without bad Hello messages a bridge will wait before it resets the Bad Hello Count for a port.

This parameter indicates how long a bridge will hold the current value of the Bad Hello Count, even though the bridge is not receiving bad Hello messages. The bridge automatically restarts this timer each time it receives another bad Hello message. The timer is expressed in Hello intervals.

Best Root

The Best Root parameter indicates the bridge ID that this bridge believes is the root bridge. In the 802.1d specification, the name for this parameter is Designated Root. The Best Root Age parameter indicates the age, in seconds, of the most recent Hello message from the Best Root. When the value of the Best Root Age exceeds the value of the Listen Time parameter, the bridge assumes the root has expired and sends out Hello messages on all of its ports, declaring itself to be the root bridge and the designated bridge on its LANs.

Forwarding Database Normal Aging Time

The Forwarding Database Normal Aging Time parameter specifies how long a bridge retains learned station address entries in its forwarding database during normal network operation. If an address does not appear in the source field of a frame for a period of time defined by this parameter, its entry in the forwarding database is marked inactive and may be removed.

Forwarding Database Short Aging Time

The Forwarding Database Short Aging Time parameter specifies how long a bridge retains learned station address entries in its forwarding database when a topology change is in progress.

Forward Delay

The Forward Delay parameter specifies the period of time that a bridge's ports stay in the Preforwarding state before entering the Forwarding state. This value is significant only for the root bridge, since it administers the Actual Forward Delay for all bridges in the spanning tree.

In the IEEE 802.1d specification, the Forward Delay is equivalent to the first half of the Forward Delay used in the Digital LAN Bridge 100 implementation, the time spent by the bridge in each of the Listening and Learning states before transitioning into the Forwarding state.

Hello Interval

The Hello Interval parameter specifies the time interval between the transmission of Hello messages when this bridge attempts to become the root, or *is* the the root bridge.

Inlink

The Inlink parameter indicates the port number of this bridge's port on the path to the root bridge. In the IEEE 802.1d specification, this parameter is called the Root Port.

LAN Bridge 100 Bridge Being Polled

The LAN Bridge 100 Bridge Being Polled parameter indicates the bridge ID of the LAN Bridge 100 that the Auto-Select root bridge is polling.

This parameter applies only to an Auto-Select root bridge operating in LAN Bridge 100 spanning tree mode.

LAN Bridge 100 Poll Time

The LAN Bridge 100 Poll Time parameter specifies the number of seconds an Auto-Select root bridge waits between making LAN Bridge 100 poll attempts. The root polls the network to determine whether any LAN Bridge 100 models are present. If a LAN Bridge 100 responds within the time set by the LAN Bridge 100 Response Timeout parameter, the Auto-Select root stays in LAN Bridge 100 spanning tree mode and the bridge address is stored in the LAN Bridge 100 Bridge Being Polled parameter for the next poll.

This parameter applies only to an Auto-Select root bridge operating in LAN Bridge 100 spanning tree mode.

LAN Bridge 100 Response Timeout

The LAN Bridge 100 Response Timeout parameter specifies the number of seconds an Auto-Select root bridge will wait for a response to a LAN Bridge 100 poll.

This parameter applies only to an Auto-Select root bridge in LAN Bridge 100 spanning tree mode.

LAN Bridge 100 Spanning Tree Compatibility Bridge

The LAN Bridge 100 Spanning Tree Compatibility parameter specifies whether the LAN Bridge 150, LAN Bridge 200, or DECbridge 500/600 series bridge is functioning as an Auto-Select bridge or as an 802.1 spanning tree bridge.

Listen Time

The Listen Time parameter specifies the age of a Hello message (in seconds), after which the bridge considers the message to be stale. This value is significant only for the root bridge, since it administers Actual Listen Time for all bridges in the spanning tree. In the IEEE 802.1d specification, the name for this parameter is Max Age.

My Cost

The My Cost parameter indicates the bridge's current path cost to the root bridge.

No Frame Interval

The No Frame Interval parameter specifies the number of seconds that a bridge waits without receiving a frame on a port before the bridge suspects a problem and runs a link test on the port.

Root Priority

The Root Priority parameter is the most significant byte of the bridge ID. It can be used to establish the root bridge or designated bridge.

During the spanning tree computation process, Hello messages from all bridges in the network are compared so that the root bridge and designated bridges can be determined. The bridge with the lowest bridge ID becomes the root bridge, with Root Priority values compared first and hardware addresses second.

Spanning Tree Mode

The Spanning Tree Mode parameter indicates whether the switch is operating in LAN Bridge 100 spanning tree mode or 802.1d spanning tree mode.

Spanning Tree Mode Changes

The Spanning Tree Mode Changes parameter indicates the number of times that the mode of the spanning tree changed from 802.1 spanning tree mode to LAN Bridge 100 spanning tree mode.

Tell Parent Flag

The Tell Parent Flag parameter indicates that the bridge needs to send a Topology Change Notification on its inlink to its parent bridge, the next closest bridge in the path to the root.

Topology Change Flag

The Topology Change Flag parameter indicates that the root bridge has been notified of a topology change in the network and that bridges are to use the Forwarding Database Short Aging Time.

Topology Change Timer

The Topology Change Timer indicates the number of seconds that the root bridge sends Hello messages with the Topology Change Flag set. In LAN Bridge 100 spanning tree mode, the Topology Change Timer is the sum of the Forward Delay parameter value and the Short Aging Time parameter value.

For 802.1 bridges, the duration is one half the Forward Delay parameter value plus the Listen Time parameter value.

Port Spanning Tree Parameters

Introduction

Port spanning tree parameters consist of one settable parameter and several nonsettable parameters. Port spanning tree parameters describe the spanning tree from each port's perspective. The Line Cost parameter can be modified with bridge management; all others are nonsettable but can be displayed with bridge management.

A database of port spanning tree parameters is associated with each port.

Acknowledgment Flag

The Acknowledgment Flag indicates that the port has received the Topology Change Notification from a bridge lower down in the spanning tree (further from the root bridge). The acknowledgment is sent in the next Hello message. In the IEEE 802.1d specification, this parameter is called the Topology Change Detected flag.

Bad Hello Count

The Bad Hello Count parameter indicates the number of consecutive Hello intervals during which the bridge received a bad Hello message on a port. When the value of the Bad Hello Count reaches the Bad Hello Limit set for the bridge, the bridge resets this counter, increases the Bad Hello Limit Exceeded Count by one, and performs a link test on the port.

Note that if the Clear Time Count parameter value reaches the value of the Bad Hello Reset Interval bridge parameter before the Bad Hello Count reaches the Bad Hello Limit, the port resets the Bad Hello Count.

Bad Hello Limit Exceeded Count

The Bad Hello Limit Exceeded Count indicates the number of times that this bridge's Bad Hello Limit has been exceeded since its initialization.

Clear Time Count

The Clear Time Count parameter indicates the number of consecutive Hello intervals during which the bridge has received no bad Hello messages on this port. When the Clear Time Count reaches the Bad Hello Reset Interval bridge parameter, the bridge resets the Clear Time Count and the Bad Hello Count.

Designated Bridge ID

The Designated bridge ID parameter indicates the bridge ID of the designated bridge on this LAN (the LAN connected to this port).

Designated Bridge Link Number

The Designated Bridge Link Number parameter indicates the port number of the designated bridge on this LAN (the LAN connected to this port). This parameter is referred to as the Designated Port in the 802.1d specification.

Designated Root Age

The Designated Root Age parameter indicates the age, in seconds, of the last Hello message sent by the designated root.

Designated Root ID

The Designated Root ID parameter indicates the bridge ID of the bridge considered to be the root bridge on this port.

Forward Delay Timer

The Forward Delay Timer parameter indicates the time remaining before the port will leave the PREFORWARDING state and enter the FORWARDING state.

Line Cost

The Line Cost parameter specifies the cost value for the port, which is used to determine the path cost to the root bridge. The Line Cost parameter may be set by network management. This parameter is referred to as the Path Cost in the 802.1d specification.

Port Address

The Port Address parameter indicates the hardware address of the port, which may differ from the bridge address.

Possible Loop Flag

The Possible Loop Flag parameter indicates whether the bridge has detected a loop condition in a situation where the Bad Hello Count is not zero.

Root Path Cost

The Root Path Cost parameter indicates the cost to the root bridge for the designated bridge on this LAN. This parameter is referred to as the Designated Cost in the 802.1d specification.

Repairing Nonvolatile Flash Memory

Overview

Introduction

This appendix describes how to repair a nonvolatile flash memory that has been corrupted by an interrupt during an upgrade to the module.

In This Appendix

The following topics are covered in this appendix:

Topic	See page...
Power Interrupts During Upgrades	D-2
Symptoms of Corrupted Nonvolatile Flash Memory	D-3
The Recovery Process	D-5

Power Interrupts During Upgrades

Introduction

Upgrading your module is a process that is fully described in the specific module's Installation manual and also in the *DEChub 900 MultiSwitch Owner's Manual*. This feature allows you to keep your module up to date with the latest firmware release from Digital.

The upgrade process is a quick and simple procedure (typical time for completion is about 5 minutes). However, during the time that the old firmware image is erased and replaced by the new firmware image, the power must not be interrupted. An interrupt during this stage of the process can corrupt the firmware image load.

Although this is unlikely to happen, this section explains how to recover in the event of an untimely power interrupt during the upgrade.

Symptoms of Corrupted Nonvolatile Flash Memory

Introduction

This section describes some symptoms that indicate nonvolatile flash memory is corrupted.

Interrupt During Firmware Image Loading

If power to the module is interrupted during the time that the new firmware image is writing to the nonvolatile Flash memory, the module becomes non-operational and the module LEDs display the following sequence:

ROM Version	Module OK LED	Port State LED
V0.2	Off	Port 1, on (green)
V0.4	Off	Port 1, blinking (green) once every 8 seconds.

BootP Request Broadcast

If the nonvolatile Flash memory is corrupted, vital information, stored in nonvolatile Flash memory, is lost and the module cannot process the Simple Network Management Protocol (SNMP) used by the HUBloader.

The loss of the nonvolatile Flash memory causes the switch to broadcast a BootP request to the broadcast address on port 2 only (the AUI port).

Note

You must configure your BootP Server to respond to the BootP request that is broadcast from the switch.

Symptoms of Corrupted Nonvolatile Flash Memory

The source address for the BootP request is the switch's Port 1 address, (listed on the module's address label).

The BootP request from the switch expects the following information from the BootP server:

- The module's IP address — required for Trivial File Transfer Protocol (TFTP)
- The BootP server's IP address
- The filename of the firmware load image

The Recovery Process

Introduction

The recovery process includes the following steps:

Step	Action
1	Configuring the BootP and TFTP servers
2	Connecting the Ethernet AUI cable
3	Powering up the switch
4	Monitoring the Firmware Upgrade with LEDs

Configuring Your BootP and TFTP Server

Note

The exact procedure for configuring your BootP server depends on the system type used by your TFTP load host.

To configure an Ultrix BootP Server, complete the following steps (for a different system, see the `bootp man` pages):

Step	Action
1	Copy the firmware image load filename (<code>filename.bin</code>) to the <code>/tftp</code> directory.
2	Add a line similar to the following to the <code>/etc/bootptab</code> : <pre>defba:ht=1:ha=08002ba34b08:ip=16.20.216.186:bf=//filename.bin</pre> <p>Note: Replace the physical address and the IP address with those of your switch.</p>
3	Enable the BootP process (if it is not already running).

Connecting the Port 2 Ethernet AUI Cable

Connect the Ethernet cable to Port 2 of your switch module (refer to your switch installation guide if you need help installing the cable).

Powering Up the Switch

Power up the switch according to instructions in the module's installation manual.

Monitoring Firmware Upgrade With LEDs

When the switch is connected to the network (via port 2) and powered up, it broadcasts the BootP request. If the BootP and TFTP servers are configured correctly, the module's LED indications inform the user of the status of the load.

The module's LED sequence is as follows:

Stage	Description	Indication
1	Port State LED 1 lights (green), or blinks (green) once every 8 seconds, depending on the ROM version.	Indicates that the switch is broadcasting BootP requests.
2	Port State LED 2 lights (green) after receiving the BootP response.	Indicates that the TFTP process has started. This process can take from 5 to 60 seconds (depends on your network and server load).
3	Port State LED 3 lights (green) after the TFTP transfer is complete.	Indicates that a Cyclic Redundancy Check (CRC) of the firmware load image is being performed. This takes approximately 2 seconds.

Stage	Description	Indication
4	Port State LED 4 lights (green)	Indicates that the CRC is correct and that the new firmware image is overwriting the old (corrupted) firmware image. This can take up to 40 seconds.
5	Port State LED 5 lights (green) for up to 2 minutes.	Indicates that the FDDI processor's nonvolatile Flash memory has loaded successfully, and that the main processor's nonvolatile Flash memory programming is in progress.
6	All Port State LEDs flash alternately between (green/yellow) for 10 seconds, then all Port State LEDs turn off for 10 seconds (see Note).	Indicates that the firmware image load is successful. the module resets, runs self-test, and then begins executing the new firmware image.

Note: If all Port State LEDs turn on yellow (after Port State LED 4 or 5 lights green) a loading error has occurred. If this occurs, retry the loading process. If the problem persists, contact your Digital service representative.

Glossary

This glossary is a comprehensive source of definitions for the 900-Series switch products.

address filtering

Filtering of packets by switches based on source or destination addresses of the packets.

address forwarding database

See forwarding database.

agent

A task running on the object being managed. The agent responds to requests for information by the network management station (NMS). An SNMP agent is responsible for performing get and set operations, for generating the appropriate traps, and controlling access.

Aging Time

A spanning tree parameter that controls how long a bridge keeps each learned entry in the forwarding database. If an entry is stored longer than the aging time, the bridge marks that entry as Inactive and allows it to be overwritten.

algorithm

A computational function that determines how values for a particular object are obtained.

attachment unit interface (AUI)

A 15-pin “D” Sub connector interface that allows stations to connect to the Ethernet/IEEE 802.3 network.

backbone

A core network (usually high speed) to which multiple local area networks (LANs) are often connected by means of bridges or routers, and over which traffic can pass.

Bad Hello

If a designated bridge receives a Hello message on the port on which it is designated, and the message contains worse root information, the message is considered “bad” and is called a Bad Hello message.

bandwidth

A measure of the amount of traffic the media can handle at one time. In digital communications, bandwidth describes the amount of data, in bits per second, that can be transmitted over the line.

BootP

A protocol that is used by a network node to determine the Internet Protocol (IP) address of its Ethernet interfaces used for network booting.

bridge (or MAC Bridge)

An intelligent, protocol-independent, store-and-forward device that operates as a Data Link Layer relay. Used to connect similar or dissimilar local area networks (LANs). A collection of LANs connected by bridges is referred to as an Extended LAN.

community

A set of attributes that are managed as a group. Community names are used in SNMP to control access. Each SNMP software request contains a community name that the agent uses as a password to verify that the requester is authorized to access the agent’s management information base (MIB) or a subset of that MIB.

concentrator

The FDDI concentrator is a Physical Layer repeating device that allows the attachment of multiple single attachment stations, dual attachment stations, or other concentrators to the FDDI network.

cyclic redundancy check (CRC)

A method of detecting errors in a frame by performing a mathematical calculation of the number of bits in the frame and appending the result to the end of the frame. The receiving station performs the same calculation on the frame and then checks that the result matches the CRC at the end of the frame.

destination address (DA)

The field in a frame that contains the address of the station to which the frame is being sent.

downstream neighbor address (DNA)

The MAC address that identifies the most recently known downstream neighbor. Stations determine the downstream neighbor by exchanging neighborhood information frames (NIFs) as part of the neighbor notification protocol. Stations also use the protocol to determine the existence of duplicate address conditions.

Destination Service Access Point (DSAP)

The destination and source address fields of a LLC PDU.

Dual Attachment Station (DAS)

An FDDI station that offers two connections to the FDDI dual counter-rotating ring.

Ethernet

A network communications system developed and standardized by Digital, Intel, and Xerox, using baseband transmission, CSMA/CD access, and logical bus topology. This industry-standard protocol is specified by ISO 8802-3 ANSI/IEEE Standard 802.3.

Ethernet station

An addressable node on an Ethernet network capable of transmitting and receiving data.

Fiber Distributed Data Interface (FDDI)

A set of ANSI/ISO standards that define a high-bandwidth (100-Mb/s), general-purpose, shared local area network (LAN) connection between computers and peripheral equipment in a timed-passing, dual ring-of-trees configuration.

Fiber Distributed Data Interface (FDDI) station

A node on an FDDI ring capable of transmitting, receiving, and repeating data.

Filtering

Filtering allows you to prevent, on a per-port basis, a bridge from forwarding frames specified by address or protocol.

forwarding database

A table maintained by a bridge that contains station addresses, the port on which the addresses are located, and the age of these entries. A bridge forwards or filters frames based on the information in the forwarding database. A bridge creates its forwarding database by learning the source port and source address of each incoming frame.

frame

A group of digits (bits) transmitted as a unit, over which a coding procedure is applied for synchronization. Frames are transmitted in packets on Ethernet LANs.

Graphical User Interface (GUI)

A display format that enables the user to choose commands, start programs, and see lists of files and other options by pointing to icons and menu items on the screen. Choices can be generally activated either with the keyboard or with a mouse. The HUBwatch application uses graphical user interfaces.

Hello interval

A spanning tree parameter that controls how often a bridge sends a hello message.

Hello messages

A hello message determines which bridges are elected as designated bridges and which bridge becomes the root bridge. When the spanning tree computation is complete, the root bridge originates the Hello message and the other bridges propagate it down the spanning tree.

hub

A central device, usually in a star topology local area network (LAN), to which stations and other devices are connected.

icon

A pictorial representation on a user interface used to indicate an object, for example, a network module.

IEEE

Institute of Electrical and Electronics Engineers.

in-band management

Managing a device over a network.

Internet Protocol (IP)

The network protocol offering a connectionless-mode network service in the Internet suite of protocols.

Internet Protocol (IP) address

The IP address is a series of numbers that identifies a device's network address on the Internet.

Internet Protocol (IP) name

A unique alphanumeric string that identifies a device on the Internet.

Local Area Network (LAN)

A data communications network that spans a limited geographical area. The network provides high-bandwidth communication over coaxial cable, twisted-pair, fiber, or microwave media and is usually owned by the user.

LAN Segment

A portion of a LAN (of a single media type) that is organized in a bus, a ring, or a point-to-point configuration.

LB100

Digital's LAN Bridge 100 product.

light-emitting diode (LED)

A semiconductor light source used as an indicator of status on a network module (or other device).

Listening

A bridge state, in which a bridge identifies the addresses of messages received from the network.

MAC address

A 48-bit binary number (usually represented as a 12-digit hexadecimal number) encoded in a device's circuitry to identify it on a local area network. Each MAC address is unique and is assigned by IEEE 802.

management agent

(See) Simple Network Management Protocol (SNMP) agent.

manual mode

The condition in which a bridge does not learn addresses but only uses addresses you specify, because you have created a filter for all unspecified addresses.

MAU (Ethernet)

When used in the context of network modules such as switches, this acronym stands for media access unit.

MAU (Token Ring)

When used in the context of token ring LANs and modules, this acronym stands for multistation access unit.

management information base (MIB)

A dynamic, virtual collection of data about a managed object. The managed object provides this data to the network management station (NMS) which gathers the values from the managed object and loads them into the MIB representing the object.

multicast address

A type of network addressing that enables a node to send messages or data packets to an address that represents a group of stations rather than a single station.

multiswitch backplane

A backplane that allows flexible allocation of its signals so that multiple local area network (LAN) segments can be managed. The DEChub 900 MultiSwitch has a multiswitch backplane.

network

A collection of computers, terminals, and other devices together with the hardware and software that enables them to exchange data and share resources over either short or long distances.

node

Any intelligent device that communicates with other devices in the network. A node is often referred to as a station.

out-of-band management (OBM)

Management of a network module or device (such as the DEChub 900 MultiSwitch backplane) over a telephone line or direct line to a dedicated management port rather than over the data network.

Protocol Data Unit (PDU)

A data object exchanged by protocol layers that contains both protocol control information and user data.

protocol

A formal set of rules governing the format, timing, sequencing, and error control of exchanged messages on a data network.

A protocol can also include facilities for managing a communications link or contention resolution.

A protocol can relate to data transfer over an interface, between two logical units directly connected, or on an end-to-end basis between two end users over a large and complex network. There are hardware protocols and software protocols.

protocol filtering (MAC layer)

A feature in some bridges that can be programmed to forward or reject transmissions that are originated under specified MAC protocols.

rate limit

The total number of frames on all ports allowed by a bridge per second.

ring

Connection of two or more stations in a circular logical topology. Information is passed sequentially between active stations, where each one, in turn, examines or copies the data, and returns it to the originating station, which removes the data from the network.

root bridge

In an extended local area network (LAN), the root bridge controls the spanning tree configuration by originating hello messages.

The spanning tree algorithm determines the root bridge by comparing the bridge IDs for all bridges in the extended LAN and by selecting the bridge with the lowest bridge ID (root priority and hardware MAC address).

root priority

A spanning tree parameter that determines a bridge's priority for becoming the root of the logical spanning tree. The root priority parameter value is used as a prefix to the bridge's address to form the bridge's identification, for example, 128/08-00-2B-2C-08-21.

single attachment station (SAS)

An FDDI station that offers one S port for attachment to the FDDI ring.

Serial Line Internet Protocol (SLIP)

Used for transmitting Internet Protocol (IP) packets across serial lines.

Simple Network Management Protocol (SNMP)

A high-level, standards-based protocol for network management.

Simple Network Management Protocol (SNMP) agent

An entity in a device that responds to SNMP requests.

source address (SA)

The address of the station that originated the data transmitted on a network.

spanning tree

A method of creating a loop-free, logical topology on any mesh topology in an extended local area network. Formation of a spanning tree topology for transmission of messages across bridges is based on the industry-standard spanning tree algorithm defined in IEEE 802.1d.

spanning tree algorithm

A specific computation that determines how a spanning tree topology is formed.

spanning tree mode

Determines whether or not a bridge is using a loop-free logical topology.

standalone

A network module in a single configuration, such as a DEChub ONE.

Station Management (SMT)

The entity within a station on the FDDI ring that monitors and exercises overall control of station's FDDI activity.

Transmission Control Protocol (TCP)

The transport protocol offering a connection-oriented transport service in the Internet suite of protocols.

topology

The logical or physical arrangement of nodes on a network.

traps

Messages generated in Simple Network Management Protocol (SNMP) agents. The firmware monitors the device for faults and sends messages to monitoring software.

For the HUBwatch application, the Alarms Poller software communicates with the SNMP agents in a hub or a community and arranges for specific traps to be sent to the network management station running the HUBwatch application.

The trap table in the Alarms Definition file determines which traps to monitor. Cold start, warm start, and authentication failure are examples of traps monitored by the alarms software.

The Alarms Poller software uses Internet Protocol (IP) addresses and community names to communicate with specific SNMP agents, such as the DECagent 90, the Hub Manager, and modules with built-in SNMP agents.

User Datagram Protocol (UDP)

The protocol offering a connectionless-mode transport service in the Internet suite of protocols.

upstream neighbor address (UNA)

An FDDI MAC address that identifies the most recently known upstream neighbor. Stations determine the upstream neighbor by exchanging neighborhood information frames (NIFs) as part of the neighbor notification protocol. Stations also use the protocol to determine the existence of duplicate address conditions.

window

A portion of the screen used for displaying information.

workgroup

An administrative grouping that consists of a relatively small number of devices attached to a LAN that is isolated from the extended LAN backbone by a bridge or a router.

Index

A

Accessing

- MIBs and RFCs, B-1
- online help, 4-7
- online information, B-2

Address Filters

- creating, 4-43
- creating default filter for unspecified addresses, 4-53
- deleting, 4-69
- list of, 4-72
- modifying, 4-47
- relevant SNMP MIB object, 4-45, 4-52, 4-54, 4-71

Aging Time

- relevant SNMP MIB object, 4-35
- setting the, 4-34

Anonymous ftp

- using, B-2

AppleTalk Translation, 3-10

B

Backplane healing

- dual ring configurations, 5-37
- tree configurations, 5-39

Beacon Process, A-19

Bridge Forward Delay

- default values, 4-30
- relevant SNMP MIB object, 4-32
- setting the, 4-30

Bridge Hello Time

- default values, 4-24
- relevant SNMP MIB object, 4-26
- setting the, 4-24

Bridge Max Age

- default values, 4-27
- relevant SNMP MIB object, 4-29
- setting the, 4-27

Broadcast Storms, 3-14

C

Chaining, 5-49

Change of Environment, 5-18

Claim Token Process, A-18

Cut-Through Switches, 1-5

D

DECconcentrator 900FH, 5-8

ModPMDs, 5-8

port assignments, 5-8

DECconcentrator 900MX, 5-6

ModPMDs, 5-6

port assignments, 5-6

- DECconcentrator 900TH, 5-7
 - ModPMDs, 5-7
 - port assignments, 5-7
- DEChub ONE
 - change of environment, 5-18
 - power failure recovery, 5-17
- DEChub ONE-MX
 - change of environment, 5-18
 - enabling ModPMD ports, 5-17
 - ModPMDs, 2-14, 2-20, 5-6, 5-7, 5-8, 5-9, 5-10, 5-17
 - power failure recovery, 5-17
- DECswitch 900EE module, 2-5
 - department backbone, 2-8
 - ordering information, 2-8
 - specifications, 2-9
- DECswitch 900EF module, 2-10, 5-9
 - department backbone, 2-13
 - ModPMDs, 5-9
 - ordering information, 2-14
 - port assignments, 5-9
 - specifications, 2-15
- Destination Address (DA) filtering, 3-15
- Dual Homing, 5-26, 5-49
- Dual Ring of Trees Topology, A-10
 - how to identify, A-10
- Dual Ring Topologies, A-9
 - backup benefit, A-9
 - independent rings, A-9

E

- Electronic mail
 - using, B-5

F

- FDDI
 - backplane channels, 5-12
 - backplane healing, 5-37, 5-39
 - beacon process, A-19

Index-2

- building blocks, 5-13, A-4
- claim token process, A-18
- configuration guidelines and rules, 5-11
- connection rules, A-14
- DEChub 900 backplane, 5-12
- default configurations, 5-16
- dual attachment station, A-5
- dual homed configuration, 5-4
- dual homing, 5-26
- dual ring, A-3
- dual ring and tree, 5-11
- dual ring configuration, 5-3
- dual ring configuration examples, 5-30
- dual ring of trees topology, A-10
- dual ring topologies, A-9
- fault tolerance in dual rings, 5-37
- fault tolerance in trees, 5-39
- how rings are formed, A-15
- in Hub backplane, 5-13
- individual network, 5-11
- MAC location, A-8
- media types and maximum distances, A-6
- multiple networks, 5-11
- naming convention, A-12
- physical connection, A-5
- physical topologies, A-9
- point-to-point connections, 5-12
- ring building blocks, 5-14
- ring initialization state, A-18
- ring operation, A-18
- single attachment concentrator, 5-11
- single attachment station, A-5
- station configurations, A-7
- station states, A-12
- station types, A-4
- steady state, A-19
- summary of FDDI connection rules, A-17

- summary of important configuration features, 5-47
- supported configurations, 5-1
- tree building blocks, 5-15
- tree configuration, 5-4
- tree configuration examples, 5-19
- tree topologies, A-10
- undesirable connections, A-15
- FDDI network modules
 - in a DEChub 900, 5-16
 - in a DEChub ONE, 5-17
 - in a DEChub ONE-MX, 5-17
- Filtering
 - destination address, 3-15
 - manual mode/secure mode, 3-17
 - source address, 3-16
 - types of, 3-15
- Forwarding
 - enabling and disabling on ports, 4-9
 - relevant MIB object, 4-9
- Frame Filtering/Forwarding, 3-15
 - types of, 3-15
- Frame Formats, 3-2
- ftpmail
 - using, B-4

G

- Gateway Address
 - relevant SNMP MIB object, 4-39
 - setting the, 4-38

H

- HUBwatch
 - for managing switches, 3-19. *See also* Chapter 4
 - how you use it to manage switches, 3-20
 - online help, 4-7
 - opening switch windows, 4-6

- switch family windows, 3-21, 4-3
- switch summary window, 4-7
- switch summary window buttons, 4-8

I

- IP Fragmentation, 3-5
 - enabling and disabling, 4-16
 - example of, 3-6
 - relevant SNMP MIB object, 4-17

L

- LAN switch, 1-2
- LAN Switching, 1-5

M

- MAC Address
 - modifying the, 4-49
- Managing Switches
 - with SNMP MIB objects, 4-8
- Manual mode/Secure mode, 3-17
- ModPMDs
 - enabling ModPMD ports, 5-17
 - ordering, 2-14, 2-20
- Multicast address filters
 - applying or removing the rate limit, 4-62

N

- Network management
 - task list, 4-1
- Network Module Front Panel Default, 5-50
- No Frame Interval
 - relevant SNMP MIB object, 4-33
 - setting the, 4-33
- Nonvolatile flash memory
 - power interrupts during upgrades, D-2
 - repair of, D-1

O

- OBM. *See* Out-of-Band Management (OBM)
- Online help, 4-7
- Online information
 - accessing, B-2
- Out-of-Band Management (OBM), 3-23
 - port and slip, 3-23

P

- PC Trace Description, 5-46
- PEswitch 900TX module, 2-16, 5-10
 - high-performance desktops, 2-19
 - ordering information, 2-20
 - port assignments, 5-10
 - specifications, 2-21
- Port Configuration when in DEChub ONE-MX, 5-50
- Port Mask
 - modifying, 4-50, 4-61
- Ports
 - disabling spanning tree algorithm, 4-10
 - disabling forwarding, 4-9

Index-4

- enabling forwarding, 4-9
- enabling spanning tree algorithm, 4-10

Power Failure Recovery, 5-17

Protocol filtering, 3-18

Protocol Filters

- creating, 4-55
- creating filters for protocols not in Available Protocols list, 4-66
- deleting, 4-69
- list of, 4-72
- modifying, 4-58
- relevant SNMP MIB object, 4-57, 4-63, 4-65, 4-67, 4-71
- specifying a default filter, 4-64

Q

Quick PC Trace Description, 5-46

Quick PC Trace Option for Concentrators, 5-46

R

Rate Limiting, 3-14

- applying or removing from a multicast address filter, 4-51
- enabling and disabling, 4-18
- relevant SNMP MIB object, 4-19, 4-23
- setting rate limit, 4-21
- value, 4-18

Raw 802.3 IPX frame format, 3-7

enabling and disabling translation, 4-14

relevant SNMP MIB object, 4-15

Ring Initialization State, A-18

S

Short Aging Time
 relevant SNMP MIB object, 4-37
 setting the, 4-36

SNMP MIB objects, 4-8

Source Address (SA) filtering, 3-16

Spanning Tree
 actual forward delay parameter, C-7
 actual Hello Interval parameter, C-7
 Actual Listen Time parameter, C-8
 Bad Hello Limit parameter, C-8
 Bad Hello Reset Interval parameter, C-8
 Best Root parameter, C-8
 bridge parameters, C-7
 establishing the, C-4
 per-port control, C-6
 port parameters, C-13

Spanning tree algorithm, C-2
 computation process, C-4
 enabling and disabling on ports, 4-10
 implementation of, C-2
 mode options, 4-12
 properties of, C-3
 relevant SNMP MIB object, 4-11

Station States, A-12

Store-and-Forward switches, 1-5

Switch
 AutoSelect feature, 4-12
 cell switches, 1-2
 comparisons of models, 2-3
 cut-through switch, 1-5
 departmental switching, 1-3
 desktop switching, 1-3
 effectiveness of, 1-9
 enterprise switching, 1-4
 filtering/forwarding frames, 3-15
 for curbing broadcast storms, 3-14
 frame formats, 3-2

 frame switches, 1-2
 IP fragmentation, 3-5
 management of, 4-1
 microsegmentation, 1-2
 models of, 2-1
 out-of-band management, 3-23
 performing common management tasks, 4-1
 product comparisons, 2-3
 properties of, 1-2
 rate limiting, 3-14
 SNMP management with MIB objects, 4-8
 store-and-forward switch, 1-5
 translation, 3-2
 what is a, 1-2

Switching
 dissimilar networks, 1-10
 Ethernet LANs, 1-9
 FDDI networks, 1-9

T

Token flow algorithm, 5-41

Token Ordering of Trees or Dual Rings, 5-41

Translation, 3-2
 example of, 3-4

Trap Address
 adding and deleting, 4-40
 events trapped, 4-40
 relevant SNMP MIB object, 4-42

Tree Topologies, A-10
 advantage of, A-10
 how to identify, A-10

U

Unknown-Protocol filtering, 3–18

Upgrades

power interrupts during, D–2

V

Valid FDDI Configurations, 5–50

W

Window-Task Table, 4–3