DES-3326
24-Port Fast Ethernet
Plus 2-Port Gigabit Module
Layer 3 Switch
User's Guide

First Edition (June, 2001)
651S3326S015
Printed In Taiwan

RECYCLABLE

Wichtige Sicherheitshinweise

1. Bitte lesen Sie sich diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den spätern Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Vervenden Sie keine Flüssig- oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
4. Um eine Beschädigung des Gerätes zu vermeiden sollten Sie nur Zubehörteile verwenden, die vom Hersteller zugelassen sind.
5. Das Gerät is vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sichern Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen. Verwenden Sie nur sichere Standorte und beachten Sie die Aufstellhinweise des Herstellers.
7. Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Die Netzanschlußsteckdose muß aus Gründen der elektrischen Sicherheit einen Schutzleiterkontakt haben.
10. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollete auch nichts auf der Leitung abgestellt werden.
11. Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
12. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
13. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. Elektrischen Schlag auslösen.
14. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.
15. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
    - a – Netzkabel oder Netzstecker sint beschädigt.
    - b – Flüssigkeit ist in das Gerät eingedrungen.
    - c – Das Gerät war Feuchtigkeit ausgesetzt.
    - d – Wenn das Gerät nicht der Bedienungsanleitung ensprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
    - e – Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
    - f – Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
16. Bei Reparaturen dürfen nur Orginalersatzteile bzw. den Orginalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.
17. Wenden Sie sich mit allen Fragen die Service und Repartur betreffen an Ihren Servicepartner. Somit stellen Sie die Betriebssicherheit des Gerätes sicher.
18. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden, Für einen Nennstrom bis 6A und einem Gerätegewicht gr ßer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm2 einzusetzen.

WARRANTIES EXCLUSIVE

IF THE D-LINK PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT D-LINK'S OPTION, REPAIR OR REPLACEMENT. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. D-LINK NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF D-LINK'S PRODUCTS
D-LINK SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY THE CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING OR OTHER HAZARD.

LIMITATION OF LIABILITY

IN NO EVENT WILL D-LINK BE LIABLE FOR ANY DAMAGES, INCLUDING LOSS OF DATA, LOSS OF PROFITS, COST OF COVER OR OTHER INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES ARISING OUT THE INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE OR INTERRUPTION OF A D- LINK PRODUCT, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY. THIS LIMITATION WILL APPLY EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
IF YOU PURCHASED A D-LINK PRODUCT IN THE UNITED STATES, SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Limited Warranty

Hardware:

D-Link warrants each of its hardware products to be free from defects in workmanship and materials under normal use and service for a period commencing on the date of purchase from D-Link or its Authorized Reseller and extending for the length of time stipulated by the Authorized Reseller or D-Link Branch Office nearest to the place of purchase.

This Warranty applies on the condition that the product Registration Card is filled out and returned to a D-Link office within ninety (90) days of purchase. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card.

If the product proves defective within the applicable warranty period, D-Link will provide repair or replacement of the product. D-Link shall have the sole discretion whether to repair or replace, and replacement product may be new or reconditioned. Replacement product shall be of equivalent or better specifications, relative to the defective product, but need not be identical. Any product or part repaired by D-Link pursuant to this warranty shall have a warranty period of not less than 90 days, from date of such repair, irrespective of any earlier expiration of original warranty period. When D-Link provides replacement, then the defective product becomes the property of D-Link.

Warranty service may be obtained by contacting a D-Link office within the applicable warranty period, and requesting a Return Material Authorization (RMA) number. If a Registration Card for the product in question has not been returned to D-Link, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided. If Purchaser's circumstances require special handling of warranty correction, then at the time of requesting RMA number, Purchaser may also propose special procedure as may be suitable to the case.

After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. The package must be mailed or otherwise shipped to D-Link with all costs of mailing/shipping/insurance prepaid. D-Link shall never be responsible for any software, firmware, information, or memory data of Purchaser contained in, stored on, or integrated with any product returned to D-Link pursuant to this warranty.

Any package returned to D-Link without an RMA number will be rejected and shipped back to Purchaser at Purchaser's expense, and D-Link reserves the right in such a case to levy a reasonable handling charge in addition mailing or shipping costs.

Software:

Warranty service for software products may be obtained by contacting a D-Link office within the applicable warranty period. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card. If a Registration Card for the product in question has not been returned to a D-Link office, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided when requesting warranty service. The term "purchase" in this software warranty refers to the purchase transaction and resulting license to use such software.

D-Link warrants that its software products will perform in substantial conformance with the applicable product documentation provided by D-Link with such software product, for a period of ninety (90) days from the date of purchase from D-Link or its Authorized Reseller. D-Link warrants the magnetic media, on which D-Link provides its software product, against failure during the same warranty period. This warranty applies to purchased software, and to replacement software provided by D-Link pursuant to this warranty, but shall not apply to any update or replacement which may be provided for download via the Internet, or to any update which may otherwise be provided free of charge.

D-Link's sole obligation under this software warranty shall be to replace any defective software product with product which substantially conforms to D-Link's applicable product documentation. Purchaser assumes responsibility for the selection of appropriate application and system/platform software and associated reference materials. D-Link makes no warranty that its software products will work in combination with any hardware, or any application or system/platform software product provided by any third party, excepting only such products as are expressly represented, in D-Link's applicable product documentation as being compatible. D-Link's obligation under this warranty shall be a reasonable effort to provide compatibility, but D-Link shall have no obligation to provide compatibility when there is fault in the third-party hardware or software. D-Link makes no warranty that operation of its software products will be uninterrupted or absolutely error-free, and no warranty that all defects in the software product, within or without the scope of D-Link's applicable product documentation, will be corrected.

D-Link Offices for Registration and Warranty Service

The product's Registration Card, provided at the back of this manual, must be sent to a D-Link office. To obtain an RMA number for warranty service as to a hardware product, or to obtain warranty service as to a software product, contact the D-Link office nearest you. An address/telephone/fax/e-mail/Web site list of D-Link offices is provided in the back of this manual.

Trademarks

Copyright ©2001 D-Link Corporation.
Contents subject to change without prior notice.
D-Link is a registered trademark of D-Link Corporation/D-Link Systems, Inc. All other trademarks belong to their respective proprietors.

Copyright Statement

No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems Inc., as stipulated by the United States Copyright Act of 1976.

FCC Warning

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

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

VCCI Warning

注意
この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づく第一種情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

BSMI Warning

警告使用者
這是甲類的資訊產品,在居住的環境中使用時,可能會造成射頻干擾,在這種情況下使用者會被要求採取某些適當的對策.

Table of Contents

About This Guide 1

Overview of this User's Guide 1

Introduction 3

Layer 3 Switching 3
The Functions of a Layer 3 Switch 5
Features 5
Ports 6
Performance Features 6
Layer 2 Features 6
Layer 3 Switch Features 8
Traffic Classification and Prioritization 9
Management 9
Optional Redundant Power Supply 10
Fast Ethernet Technology 11
Gigabit Ethernet Technology 11

Unpacking and Setup 12

Unpacking 12
Installation 13
Desktop or Shelf Installation 13
Rack Installation 14
Power on 15
Power Failure 16

Identifying External Components 17

Front Panel 17
Rear Panel 18
Side Panels 19
Optional Plug-in Modules 19
1000BASE-T Module 20
1000BASE-SX Fiber Module 20
1000BASE-LX Fiber Module 21

GBIC Two-Port Module 22
LED Indicators.....22

Connecting The Switch.....24

Switch to End Node 24
Switch to Hub or Switch.....25
10BASE-T Device.....26
100BASE-TX Device 27

Switch Management and Operating Concepts 28

Local Console Management 28
Diagnostic (console) port (RS-232 DCE).....29
IP Addresses and SNMP Community Names.....30
Traps.....32
MIBs 33
SNMP.....34
Authentication 35
Packet Forwarding.....35
MAC Address Aging Time 36
Filtering.....36
Spanning Tree Protocol 38
STP Operation Levels.....39
Bridge Protocol Data Units 41
Creating a Stable STP Topology 42
STP Port States.....42
User-Changeable STA Parameters.....45
Illustration of STP 46
Port Aggregation.....49
Setting Up IP Interfaces.....51
Notes About VLANs on the DES-3326 51
IEEE 802.1Q VLANs 53
802.1Q VLAN Packet Forwarding 54
802.1Q VLAN Tags 55
Port VLAN ID.....57
Tagging and Untagging.....59
Ingress Filtering 59
Layer 3-Based VLANs 60
VLANs in Layer 2 Only Mode 61

DHCP Servers 63
Broadcast Storms 65
  Segmenting Broadcast Domains 66
  Eliminating Broadcast Storms 66
IP Addressing and Subnetting 67
  Definitions 67
  IP Addresses 68
  Address Classes 70
  Subnet Masking 72
  Calculating the Number of Subnets and Nodes 73
  Classless InterDomain Routing – CIDR 74
Internet Protocols 77
  Protocol Layering 77
  Layer 1 80
  Layer 2 80
  Layer 3 81
  Layer 4 81
  Layer 7 82
  TCP/IP 82
Packet Headers 84
  TCP Level 84
  IP Level 86
  Ethernet Level 87
  Well-Known Sockets and the Application Layer 89
  UDP and ICMP 90
The Domain Name System 92
  Mapping Domain Names to Addresses 92
  Domain Name Resolution 93
IP Routing 93
  Packet Fragmentation and Reassembly 95
  ARP 95
Multicasting 96
  Multicast Groups 96
  Multicast Addressing 97
  Internet Group Management Protocol (IGMP) 99
  IGMP Versions 1 and 2 99
Multicast Routing Algorithms 102
  Flooding 102

Multicast Spanning Trees 103
Reverse Path Broadcasting (RPB) 103
Reverse Path Multicasting (RPM) 104
Multicast Routing Protocols 105
Distance Vector Multicast Routing Protocol (DVMRP) 105
Protocol-Independent Multicast (PIM) 106
Protocol-Independent Multicast – Dense Mode (PIM-DM) ...107
Routing 107
Routing Information Protocol.....107
RIP Version 1 Message Format.....109
RIP 1 Message.....111
RIP 1 Route Interpretation 111
RIP Version 2 Extensions.....112
RIP2 Message Format 112

Configuring the Switch Using the Console Interface.....114

Before You Start 115
General Deployment Strategy.....115
VLAN Layout 116
Assigning IP Network Addresses and Subnet Masks to VLANs 117
Defining Static Routes.....118
Connecting to the Switch 118
Console Usage Conventions 119
Creating User Accounts.....121
User Accounts Management 123
Saving Changes.....124
Factory Reset 126
Logging Onto The Switch Console.....128
Updating or Deleting User Accounts.....128
Viewing Current User Accounts 130
Deleting a User Account.....131
Setting Up The Switch 132
Basic Setup.....132
Switch Information 133
Remote Management Setup 134
Setting Up Trap Receivers 137
Configure Ports 139

Serial Port Settings.....140
Switch Operation Mode.....141
Changing the Switch Operation Mode 142
Layer 2 Switch Settings.....146
Layer 3 IP Routing Protocol Settings 148
Layer 3 Switch Mode - Setup RIP.....149
Advanced Setup 152
Configuring VLANs 152
VLANs by Switch Operating Mode – Layer 2 Only and IP Routing 153
Setting Up IP Interfaces.....163
Multicasting 168
Layer 2 Multicast Setup 168
IGMP Snooping Settings – by VLAN.....168
IEEE 802.1Q Multicast Forwarding.....171
Static Router Port 173
Layer 3 Multicasting.....175
DVMRP.....180
PIM-DM.....182
Static Router Port 184
Port Mirroring.....186
Priority 189
Filtering.....190
Layer 2 Filtering 190
Layer 3 (IP Routing) Filtering 192
Forwarding.....195
Layer 2 Forwarding 195
IP Routing Forwarding.....197
MAC Address Forwarding.....197
Spanning Tree.....201
Switch Spanning Tree Settings.....201
Port Group Spanning Tree Settings 203
Link Aggregation 206
Switch Utilities 208
Layer 2 Switch Utilities.....208
Updating Firmware 209
Downloading a Configuration File.....210
Uploading a Settings File.....211

Uploading a History Log File 212
Testing Connectivity with Ping.....213
Layer 3 Utilities 214
BOOTP Relay 214
DNS Relay 217
Network Monitoring 219
Layer 2 Network Monitoring.....219
Port Utilization 219
Port Error Statistics.....220
Port Packet Analysis Table 221
MAC Address Forwarding Table.....222
GVRP Status Table 223
GMRP Status Table 224
IGMP Snooping Table.....225
Switch History Log 226
Layer 3 Network Monitoring.....227
IP Address Forwarding Table 228
IP Routing Table 229
ARP Table.....230
IP Multicast Forwarding Table.....231
DVMRP Routing Table 232
Factory Reset .....**Error! Bookmark not defined.**
Reboot 233

Web-Based Network Management 236

Introduction.....236
Before You Start 237
General Deployment Strategy.....237
VLAN Layout 239
Assigning IP Network Addresses and Subnet Masks to VLANs 239
Defining Static Routes.....240
Getting Started 240
Management 240
Configuring the Switch.....241
User Accounts Management 241
Saving Changes.....243
Factory Reset 244

USING WEB-BASED MANAGEMENT.....245
CONFIGURING AND MONITORING THE SWITCH 253

Technical Specifications 349

RJ-45 Pin Specification 352

Sample Configuration File 354

Runtime Switching Software Default Settings.....357

Understanding and Troubleshooting the Spanning Tree Protocol
.....359

Blocking State 360
Listening State.....362
Learning State 364
Forwarding State 366
Disabled State 368
Troubleshooting STP 370
Spanning Tree Protocol Failure 370
Full/Half Duplex Mismatch.....371
Unidirectional Link.....372
Packet Corruption.....374
Resource Errors.....374
Identifying a Data Loop.....375
Avoiding Trouble.....375

Brief Review of Bitwise Logical Operations.....381

Index.....383

ABOUT THIS GUIDE

This User's guide tells you how to install your DES-3326, how to connect it to your Ethernet network, and how to set its configuration using either the built-in console interface or Web-based management.

Overview of this User's Guide

- Chapter 1, *Introduction*. Describes the Switch and its features.
- Chapter 2, *Unpacking and Setup*. Helps you get started with the basic installation of the Switch.
- Chapter 3, *Identifying External Components*. Describes the front panel, rear panel, optional plug-in modules, and LED indicators of the Switch.
- Chapter 4, *Connecting the Switch*. Tells how you can connect the DES-3326 to your Ethernet network.
- Chapter 5, *Switch Management*. Talks about Local Console Management via the RS-232 DCE console port and other aspects about how to manage the Switch.
- Chapter 6, *Using the Console Interface*. Tells how to use the built-in console interface to change, set, and monitor Switch performance and security.

- Chapter 7, *Web-Based Network Management*. Tells how to manage the Switch through an Internet browser.
- Appendix A, *Technical Specifications*. Lists the technical specifications of the DES-3326.
- Appendix B, *RJ-45 Pin Specifications*. Shows the details and pin assignments for the RJ-45 receptacle/connector.
- Appendix C, *Factory Default Settings*.
- Appendix D, *Sample Configuration File.*

1

INTRODUCTION

This section describes the Layer 3 functionality and Layer 2 and Layer 3 features of the DES-3326. Some background information about Ethernet/Fast Ethernet, Gigabit Ethernet, and switching technology is presented. This is intended for readers who may not be familiar with the concepts of layered switching and routing but is not intended to be a complete or in-depth discussion.

Layer 3 Switching

Layer 3 switching is the integration of two proven technologies: switching and routing. In fact, Layer 3 switches are running the same routing routines and protocols as traditional routers. The main difference between traditional routing and Layer 3 switching is the addition of a group of Layer 2 switching domains and the execution of routing routines for most packets via an ASIC – in hardware instead of software.

Where a traditional router would have one, or at best a few, Fast Ethernet ports, the DES-3326 Layer 3 switch has 24 Fast Ethernet ports and optionally, 2 Gigabit Ethernet ports. Where a traditional router would have one or two high-speed serial WAN connections, the DES-3326 relies upon a Fast Ethernet port to connect to a separate device, which in turn, connects the network to a WAN or the Internet.

The DES-3326 can be thought of as 24 Fast Ethernet Layer 2 switching domains with a wire-speed router between each domain. It can be deployed in a network between a traditional router and the intranetwork. The traditional router and its associated WAN interface would then handle routing between the intranetwork and the WAN (the Internet, for example) while the Layer 3 switch would handle routing within the LAN (between the Fast Ethernet Layer 2 domains). Any installed Layer 2 switches, and indeed the entire subnetting scheme, would remain in place.

The DES-3326 can also replace key traditional routers for data centers and server farms, routing between these locations and the rest of the network, and providing 24 ports of Layer 2 switching performance combined with wire-speed routing.

Backbone routers can also be replaced with DES-3326 and a series of DES-3326 could be linked via the optional Gigabit Ethernet ports. Routers that service WAN connections would remain in place, but would now be removed from the backbone and connected to the DES-3326 via an Ethernet/Fast Ethernet port. The backbone itself could be migrated to Gigabit Ethernet, or faster technologies as they become available.

The DES-3326 accomplishes two objectives. First as a tool to provide high-performance access to enterprise data servers and infrastructure, and second, to enhance the performance of network equipment already installed. Many network segments display poor performance, but the Ethernet wire is only carrying a fraction of its total traffic capacity. The problem is not the network, but the ability of the connected devices utilize the full capacity of the network. The DES-3326 can eliminate network bottlenecks to high-traffic areas, and improve the utilization of the network's installed bandwidth.

The Functions of a Layer 3 Switch

Traditional routers, once the core components of large networks, became an obstacle to the migration toward next-generation networks. Attempts to make software-based routers forward packets more quickly were inadequate.

A layer 3 switch does everything to a packet that a traditional router does:

- Determines forwarding path based on Layer 3 information
- Validates the integrity of the Layer 3 header via checksum
- Verifies packet expiration and updates accordingly
- Processes and responds to any optional information
- Updates forwarding statistics in the Management Information Base

A Layer 3 switch can be placed anywhere within a network core or backbone, easily and cost-effectively replacing the traditional collapsed backbone router. The DES-3326 Layer 3 switch communicates with a WAN router using a standard Ethernet/Fast Ethernet port. Multiple DES-3326 switches can be linked via the optional, 2-port Gigabit Ethernet module.

Features

The DES-3326 Switch was designed for easy installation and high performance in an environment where traffic on the network and the number of users increase continuously.

Switch features include:

Ports

- 24 high performance NWay ports all operating at 10/100 Mbps for connecting to end stations, servers and hubs (23 MDI-X 10/100 Ethernet UTP ports and one MDI-II/MDI-X port. The MDI-II/MDI-X port can be switched between the two modes from the front panel.)
- All ports can auto-negotiate (NWay) between 10Mbps/ 100Mbps, half-duplex or full duplex and flow control for half-duplex ports.
- One front panel slide-in module interface for a 2-port 1000BASE-SX, 1000BASE-LX, 1000BASE-T, or GBIC Gigabit Ethernet module.
- RS-232 DCE Diagnostic port (console port) for setting up and managing the Switch via a connection to a console terminal or PC using a terminal emulation program.

Performance Features

Layer 2 Features

- 8.8 Gbps switching fabric capacity
- Store and forward switching scheme.
- Full and half-duplex for both 10Mbps and 100Mbps connections. The front-port Gigabit Ethernet module operates at full-duplex only. Full-duplex allows the switch port to simultaneously transmit and receive data, and only works with connections to full-duplex capable end stations

and switches. Connections to hubs must take place at half-duplex.

- Supports IEEE 802.3x flow control for full-duplex mode ports.
- Supports Back-pressure flow control for half-duplex mode ports.
- Auto-polarity detection and correction of incorrect polarity on the transmit and receive twisted-pair at each port.
- IEEE 802.3z compliant for all Gigabit ports (optional module).
- IEEE 802.3x compliant Flow Control support for all Gigabit ports (optional module).
- IEEE 802.3ab compliant for 1000BASE-T (Copper) Gigabit ports (optional module).
- Data forwarding rate 14,880 pps per port at 100% of wire-speed for 10Mbps speed.
- Data forwarding rate 148,800 pps per port at 100% of wire-speed for 100Mbps speed.
- Data filtering rate eliminates all error packets, runts, etc. at 14,880 pps per port at 100% of wire-speed for 10Mbps speed.
- Data filtering rate eliminates all error packets, runts, etc. at 148,800 pps per port at 100% of wire-speed for 100Mbps speed.
- 8K active MAC address entry table per device with automatic learning and aging (10 to 9999 seconds).
- 16 MB packet buffer per device.
- Broadcast and Multicast storm filtering.

- Supports Port Mirroring.
- Supports Port Trunking – up to six trunk groups (each consisting of up to eight ports) may be set up.
- 802.1D Spanning Tree support.
- 802.1Q Tagged VLAN support – up to 63 User-defined VLANs per device (one VLAN is reserved for internal use).
- GVRP – (GARP VLAN Registration Protocol) support for dynamic VLAN registration.
- 802.1p Priority support with 4 priority queues.
- IGMP Snooping support.
- Layer 2 Multicast support – GMRP (GARP Multicast Registration Protocol).

Layer 3 Switch Features

- Wire speed IP forwarding.
- Hardware-based Layer 3 IP switching.
- IP packet forwarding rate of 6.6 Mpps.
- 2K active IP address entry table per device.
- Supports RIP – (Routing Information Protocol) version I and II.
- Supports IP version 4.
- IGMP version 1 and 2 support (RFC 1112 and RFC 2236).
- Supports PIM Dense Mode.

- Supports DVMRP.
- Supports IP multi-netting.
- Supports IP packet de-fragmentation.
- Supports Path MTU discovery.
- Supports 802.1D frame support.

Traffic Classification and Prioritization

- Based on 802.1p priority bits
- 4 priority queues

Management

- RS-232 console port for out-of-band network management via a console terminal or PC.
- Spanning Tree Algorithm Protocol for creation of alternative backup paths and prevention of network loops.
- SNMP v.1 Agent.
- Fully configurable either in-band or out-of-band control via SNMP based software.
- Flash memory for software upgrades. This can be done in-band via TFTP or out-of-band via the console.
- Built-in SNMP management:
    - Bridge MIB (RFC 1493)
    - MIB-II (RFC 1213)

  - Mini-RMON MIB (RFC 1757) – 4 groups
  - CIDR MIB (RFC 2096), except IP Forwarding Table.
  - 802.1p MIB (RFC 2674).
  - RIP MIB v2 (RFC 1724).
- Supports Web-based management.
- TFTP support.
- BOOTP support.
- BOOTP Relay Agent.
- IP filtering on the management interface.
- DCHP Client support.
- DCHP Relay Agent.
- DNS Relay Agent.
- Password enabled.

Optional Redundant Power Supply

The DES-3326 24+2 Fast Ethernet Layer 3 Switch supports the optional DPS-1000 (Redundant Power Supply) to provide automatic power supply monitoring and switchover to a redundant power supply (located in the chassis of the DPS-1000) in case of a failure in the DES-3326's internal power supply.

Fast Ethernet Technology

100Mbps Fast Ethernet (or 100BASE-T) is a standard specified by the IEEE 802.3 LAN committee. It is an extension of the 10Mbps Ethernet standard with the ability to transmit and receive data at 100Mbps, while maintaining the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Ethernet protocol.

Gigabit Ethernet Technology

Gigabit Ethernet is an extension of IEEE 802.3 Ethernet utilizing the same packet structure, format, and support for CSMA/CD protocol, full duplex, flow control, and management objects, but with a tenfold increase in theoretical throughput over 100Mbps Fast Ethernet and a one hundred-fold increase over 10Mbps Ethernet. Since it is compatible with all 10Mbps and 100Mbps Ethernet environments, Gigabit Ethernet provides a straightforward upgrade without wasting a company's existing investment in hardware, software, and trained personnel.

Gigabit Ethernet enables fast optical fiber connections and Unshielded Twisted Pair connections to support video conferencing, complex imaging, and similar data-intensive applications. Likewise, since data transfers occur 10 times faster than Fast Ethernet, servers outfitted with Gigabit Ethernet NIC's are able to perform 10 times the number of operations in the same amount of time.

2

UNPACKING AND SETUP

This chapter provides unpacking and setup information for the Switch.

Unpacking

Open the shipping carton of the Switch and carefully unpack its contents. The carton should contain the following items:

- One DES-3226 24-port Fast Ethernet Layer 3 Switch
- Mounting kit: 2 mounting brackets and screws
- Four rubber feet with adhesive backing
- One AC power cord
- This User's Guide with Registration Card

If any item is found missing or damaged, please contact your local D-Link reseller for replacement.

Installation

Use the following guidelines when choosing a place to install the Switch:

- The surface must support at least 3 kg.
- The power outlet should be within 1.82 meters (6 feet) of the device.
- Visually inspect the power cord and see that it is secured to the AC power connector.
- Make sure that there is proper heat dissipation from and adequate ventilation around the switch. Do not place heavy objects on the switch.

Desktop or Shelf Installation

When installing the Switch on a desktop or shelf, the rubber feet included with the device should first be attached. Attach these cushioning feet on the bottom at each corner of the device. Allow adequate space for ventilation between the device and the objects around it.

Figure 2-1. Installing rubber feet for desktop installation

Rack Installation

The DES-3326 can be mounted in an EIA standard-sized, 19-inch rack, which can be placed in a wiring closet with other equipment. To install, attach the mounting brackets on the switch's side panels (one on each side) and secure them with the screws provided.

Figure 2- 2A. Attaching the mounting brackets to the switch

Then, use the screws provided with the equipment rack to mount the switch on the rack.

Figure 2-2B. Installing the switch on an equipment rack

Power on

The DES-3326 switch can be used with AC power supply 100-240 VAC, 50 - 60 Hz. The power switch is located at the rear of the unit adjacent to the AC power connector and the system fan. The switch's power supply will adjust to the local power source automatically and may be turned on without having any or all LAN segment cables connected.

After the power switch is turned on, the LED indicators should respond as follows:

- All LED indicators will momentarily blink. This blinking of the LED indicators represents a reset of the system.
- The power LED indicator will blink while the Switch loads onboard software and performs a self-test. After approximately 20 seconds, the LED will light again to indicate the switch is in a ready state.
- The console LED indicator will remain ON if there is a connection at the RS-232 port, otherwise this LED indicator is OFF.
- The 100M LED indicator may remain ON or OFF depending on the transmission speed.

Power Failure

As a precaution in the event of a power failure, unplug the switch. When power is resumed, plug the switch back in.

3

IDENTIFYING EXTERNAL COMPONENTS

This chapter describes the front panel, rear panel, optional plug-in modules, and LED indicators of the DES-3326.

Front Panel

The front panel of the Switch consists of LED indicators, an RS-232 communication port, a slide-in module slot, one switched MDI-X/MDI-II uplink port, and 23 (10/100 Mbps) Ethernet/Fast Ethernet ports.

Figure 3-1. Front panel view of the Switch

- Comprehensive LED indicators display the status of the switch and the network (see the *LED Indicators* section below).
- An RS-232 DCE console port for setting up and managing the switch via a connection to a console terminal or PC using a terminal emulation program.

- A front-panel slide-in module slot for Gigabit Ethernet ports can accommodate a 2-port 1000BASE-T Gigabit Ethernet module, a 2-port 1000BASE-SX Gigabit Ethernet module, a 2-port 1000BASE-LX Gigabit Ethernet module, or a 2-port GBIC-based Gigabit Ethernet module.

- One switched MDI-X/MDI-II Uplink port that can be used to connect a straight-through cable or a crossed cable to a normal (non-Uplink) port on a switch or hub. This port is identical to the other 23 ports except for the ability to use a crossed or a straight-through cable.

- Twenty-three high-performance, NWay Ethernet ports all of which operate at 10/100 Mbps for connections to end stations, servers and hubs. All ports can auto-negotiate between 10Mbps or 100Mbps, full or half duplex, and flow control.

Rear Panel

The rear panel of the switch consists of a slot for the optional DPS-1000 (Redundant Power Supply) and an AC power connector.

Figure 3-2. Rear panel view of the Switch

- The AC power connector is a standard three-pronged connector that supports the power cord. Plug-in the female connector of the provided power cord into this socket, and the male side of the cord into a power outlet. Supported input voltages range from 100 ~ 240 VAC at 50 ~ 60 Hz.

Side Panels

The right side panel of the Switch contains two system fans (see the top part of the diagram below). The left side panel contains heat vents.

Figure 3-4. Side panel views of the Switch

- The system fans are used to dissipate heat. The sides of the system also provide heat vents to serve the same purpose. Do not block these openings, and leave at least 6 inches of space at the rear and sides of the switch for proper ventilation. Be reminded that without proper heat dissipation and air circulation, system components might overheat, which could lead to system failure.

Optional Plug-in Modules

The DES 3326 24-port Fast Ethernet Layer 3 Switch is able to accommodate a range of optional plug-in modules in order to increase functionality and performance. These modules must be purchased separately.

1000BASE-T Module

Figure 3-5. 1000BASE-TX two-port module

- Front-panel module.
- Connects to 1000BASE-T devices.
- Supports Category 5e UTP or STP cable connections of up to 100 meters.

1000BASE-SX Fiber Module

Figure 3-6. 1000BASE-SX two-port module

- Front-panel module.

- Connects to 1000BASE-SX devices at full-duplex.
- Allows connections using multi-mode fiber optic cable in the following configurations:

	62.5µm	62.5µm	50µm	50µm
Modal bandwidth (min. overfilled launch) Unit: MHz*km	160	200	400	500
Operating distance Unit: meters	220	275	500	550
Channel insertion loss Unit: dB	2.33	2.53	3.25	3.43

1000BASE-LX Fiber Module

Figure 3-7. 1000BASE-LX two-port module

- Front-panel module.
- Connects to 1000BASE-LX devices at full-duplex.

- Supports multi-mode fiber-optic cable connections of up to 550 meters or 5 km single-mode fiber-optic cable connections.

GBIC Two-Port Module

Figure 3-8. GBIC two-port module

- Front-panel module.
- Connects to GBIC devices at full duplex only.
- Allows multi-mode fiber optic connections of up to 550 m (SX and LX) and single-mode fiber optic connections of up to 5 km (LX only). GBIC modules are available in –SX and –LX fiber optic media.

LED Indicators

The LED indicators of the Switch include Power, Console, and Link/Act. The following shows the LED indicators for the Switch along with an explanation of each indicator.

Figure 3-9. The LED indicators

- **Power** This indicator on the front panel should be lit during the Power-On Self Test (POST). It will light green approximately 2 seconds after the switch is powered on to indicate the ready state of the device.

- **Console** This indicator is lit green when the switch is being managed via out-of-band/local console management through the RS-232 console port using a straight-through serial cable.

- **Act/Link** These indicators are located to the left and right of each port. They are lit when there is a secure connection (or link) to a device at any of the ports. The LEDs blink whenever there is reception or transmission (i.e. Activity--Act) of data occurring at a port.

4

CONNECTING THE SWITCH

This chapter describes how to connect the DES 3226 to your Fast Ethernet network.

Switch to End Node

End nodes include PCs outfitted with a 10, 100 or 10/100 Mbps RJ-45 Ethernet/Fast Ethernet Network Interface Card (NIC) and most routers. The RJ-45 UTP ports on NICs and most routers are MDI-II. When using a normal straight-through cable, an MDI-II port must connect to an MDI-X port.

An end node can be connected to the Switch via a two-pair Category 3, 4, 5 UTP/STP straight cable (be sure to use Category 5e UTP or STP cabling for 100 Mbps Fast Ethernet connections). The end node should be connected to any of the twenty-three ports (2x - 24x) of the DES-3226 or to either of the two 100BASE-TX ports on the front-panel module that came preinstalled on the switch. Port 1x can be used as an uplink port to connect to another switch using either a crossed or a straight-through cable. This port is switched between MDI-X and MDI-II to accommodate either type of cable.

Figure 4-1. Switch connected to an End Node

The LED indicators for the port the end node is connected to are lit according to the capabilities of the NIC. If LED indicators are not illuminated after making a proper connection, check the PC's LAN card, the cable, switch conditions, and connections.

The following LED indicator states are possible for an end node to switch connection:

1. The 100 LED indicator comes *ON* for a 100 Mbps and stays *OFF* for 10 Mbps.

2. The Link/Act LED indicator lights up upon hooking up a PC that is powered on.

Switch to Hub or Switch

These connections can be accomplished in a number of ways. The most important consideration is that when using a normal, straight-through cable, the connection should be made between a normal crossed port (Port 2x, 3x, etc.) and an Uplink (MDI-II) port. If you are using a crossover cable, the connection must be made from Uplink to Uplink (port 1x on the DES-3326), or from a crossed port to another crossed port.

- A 10BASE-T hub or switch can be connected to the Switch via a two-pair Category 3, 4 or 5 UTP/STP straight cable.

- A 100BASE-TX hub or switch can be connected to the Switch via a two-pair Category 5e UTP/STP straight cable.

If the other switch or hub contains an unused Uplink port, we suggest connecting the other device's Uplink (MDI-II) port to any of the switch's (MDI-X) ports (1x - 22x, or one of the optional Gigabit module ports) using a normal straight-through cable, as shown below.

If the other device does not have an unused Uplink port, make the connection with a normal straight-through cable from the Uplink port on the switch to any normal crossed port on the hub. Alternatively, if you have a crossover cable you can save the Uplink ports for other connections and make this one from a crossed port to another crossed port.

Figure 4-2. Switch connected to a normal (non-Uplink) port on a hub or switch using a straight or crossover cable

10BASE-T Device

For a 10BASE-T device, the Switch's LED indicators should display the following:

- 100 LED speed indicator is *OFF*.
- Link/Act indicator is *ON*.

100BASE-TX Device

For a 100BASE-TX device, the Switch's LED indicators should display the following:

- 100 LED speed indicator is *ON*.
- Link/Act is *ON*.

5

SWITCH MANAGEMENT AND OPERATING CONCEPTS

This chapter discusses many of the concepts and features used to manage the switch, as well as the concepts necessary for the user to understand the functioning of the switch. Further, this chapter explains many important points regarding these features.

Configuring the switch to implement these concepts and make use of its many features is discussed in detail in the next chapters.

Local Console Management

A local console is a terminal or a workstation running a terminal emulation program that is connected directly to the switch via the RS-232 console port on the front of the switch. A console connection is referred to as an 'Out-of-Band' connection, meaning that console is connected to the switch using a different circuit than that used for normal network communications. So, the console can be used to set up and manage the switch even if the network is down.

Local console management uses the terminal connection to operate the console program built-in to the switch (see Chapter 6 – Using the Console Interface). A network administrator can manage, control and monitor the switch from the console program.

The DES-3326 contains a CPU, memory for data storage, flash memory for configuration data, operational programs, and SNMP agent firmware. These components allow the switch to be actively managed and monitored from either the console port or the network itself (out-of-band, or in-band).

Diagnostic (console) port (RS-232 DCE)

Out-of-band management requires connecting a terminal, such as a VT-100 or a PC running a terminal emulation program (such as HyperTerminal, which is automatically installed with Microsoft Windows) a to the RS-232 DCE console port of the Switch. Switch management using the RS-232 DCE console port is called *Local Console Management* to differentiate it from management performed via management platforms, such as D-View, HP OpenView, etc. *Web-based Management* describes management of the switch performed over the network (in-band) using the switch's built-in Web-based management program (see Chapter 7 – Web-based Network Management). The operations to be performed and the facilities provided by these two built-in programs are identical.

The console port is set at the factory for the following configuration:

- Baud rate: 9,600
- Data width: 8 bits
- Parity: none
- Stop bits: 1
- Flow Control None

Make sure the terminal or PC you are using to make this connection is configured to match these settings.

If you are having problems making this connection on a PC, make sure the emulation is set to VT-100. If you still don't see anything, try hitting <Ctrl> + r to refresh the screen.

IP Addresses and SNMP Community Names

Each Switch must be assigned its own IP Address, which is used for communication with an SNMP network manager or other TCP/IP application (for example BOOTP, TFTP). The switch's default IP address is 10.90.90.90. You can change the default Switch IP Address to meet the specification of your networking address scheme.

The switch is also assigned a unique MAC address by the factory. This MAC address cannot be changed, and can be found from the initial boot console screen – shown below.

Figure 5-1. Boot Screen

The switch's MAC address can also be found from the console program under the Switch Information menu item, as shown below.

Figure 5-2. Switch Information Screen

In addition, you can also set an IP Address for a gateway router. This becomes necessary when the network management station is located on a different IP network from the Switch, making it necessary for management packets to go through a router to reach the network manager, and vice-versa.

For security, you can set in the Switch a list of IP Addresses of the network managers that you allow to manage the Switch. You can also change the default SNMP Community Strings in the Switch and set the access rights of these Community Strings. In addition, a VLAN may be designated as a Management VLAN.

Traps

Traps are messages that alert you of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned OFF the Switch), or less serious like a port status change. The Switch generates traps and sends them to the network manager (trap recipient).

Trap recipients are special users of the network who are given certain rights and access in overseeing the maintenance of the network. Trap recipients will receive traps sent from the Switch; they must immediately take certain actions to avoid future failure or breakdown of the network.

You can also specify which network managers may receive traps from the Switch by entering a list of the IP addresses of authorized network managers. Up to four trap recipient IP addresses, and four corresponding SNMP community strings can be entered.

SNMP community strings function like passwords in that the community string entered for a given IP address must be used in the management station software, or a trap will be sent.

The following are trap types the switch can send to a trap recipient:

- **Cold Start** This trap signifies that the Switch has been powered up and initialized such that software settings are reconfigured and hardware systems are rebooted. A cold start is different from a factory reset in that configuration settings saved to non-volatile RAM used to reconfigure the switch.

- **Warm Start** This trap signifies that the Switch has been rebooted, however the POST (Power On Self-Test) is skipped.

- **Authentication Failure** This trap signifies that someone has tried to logon to the switch using an invalid SNMP community string. The switch automatically stores the source IP address of the unauthorized user.

- **New Root** This trap indicates that the Switch has become the new root of the Spanning Tree, the trap is sent by the switch soon after its election as the new root. This implies that upon expiration of the Topology Change Timer the new root trap is sent out immediately after the Switch's election as the new root.

- **Topology Change (STP)** A Topology Change trap is sent by the Switch when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a new root trap is sent for the same transition.

- **Link Up** This trap is sent whenever the link of a port changes from link down to link up.

- **Link Down** This trap is sent whenever the link of a port changes from link up to link down.

MIBs

Management and counter information are stored in the Switch in the Management Information Base (MIB). The Switch uses the standard MIB-II Management Information Base module. Consequently, values for MIB objects can be retrieved from any SNMP-based network management software. In addition to the standard MIB-II, the Switch also supports its own proprietary enterprise MIB as an extended Management Information Base. These MIBs may also be retrieved by specifying the MIB's Object-

Identity (OID) at the network manager. MIB values can be either read-only or read-write.

Read-only MIBs variables can be either constants that are programmed into the Switch, or variables that change while the Switch is in operation. Examples of read-only constants are the number of port and type of ports. Examples of read-only variables are the statistics counters such as the number of errors that have occurred, or how many kilobytes of data have been received and forwarded through a port.

Read-write MIBs are variables usually related to user-customized configurations. Examples of these are the Switch's IP Address, Spanning Tree Algorithm parameters, and port status.

If you use a third-party vendors' SNMP software to manage the Switch, a diskette listing the Switch's propriety enterprise MIBs can be obtained by request. If your software provides functions to browse or modify MIBs, you can also get the MIB values and change them (if the MIBs' attributes permit the write operation). This process however can be quite involved, since you must know the MIB OIDs and retrieve them one by one.

SNMP

The Simple Network Management Protocol (SNMP) is an OSI layer 7 (the application layer) protocol for remotely monitoring and configuring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. SNMP can be used to perform many of the same functions as a directly connected console, or can be used within an integrated network management software package such as DView.

SNMP performs the following functions:

- Sending and receiving SNMP packets through the IP protocol.
- Collecting information about the status and current configuration of network devices.
- Modifying the configuration of network devices.

The DES-3326 has a software program called an 'agent' that processes SNMP requests, but the user program that makes the requests and collects the responses runs on a management station (a designated computer on the network). The SNMP agent and the user program both use the UDP/IP protocol to exchange packets.

Authentication

The authentication protocol ensures that both the router SNMP agent and the remote user SNMP application program discard packets from unauthorized users. Authentication is accomplished using 'community strings', which function like passwords. The remote user SNMP application and the router SNMP must use the same community string. SNMP community strings of up to 20 characters may be entered under the *Remote Management Setup* menu of the console program.

Packet Forwarding

The Switch enters the relationship between destination MAC or IP addresses and the Ethernet port or gateway router the destination resides on into its forwarding table. This information is then used to forward packets. This reduces the traffic congestion on the network, because packets, instead of being transmitted to all ports, are transmitted to the destination port only. Example: if Port 1

receives a packet destined for a station on Port 2, the Switch transmits that packet through Port 2 only, and transmits nothing through the other ports. This process is referred to as 'learning' the network topology.

MAC Address Aging Time

The Aging Time affects the learning process of the Switch. Dynamic forwarding table entries, which are made up of the source and destination MAC addresses and their associated port numbers, are deleted from the table if they are not accessed within the aging time.

The aging time can be from 10 to 1,000,000 seconds with a default value of 300 seconds. A very long aging time can result in dynamic forwarding table entries that are out-of-date or no longer exist. This may cause incorrect packet forwarding decisions by the switch.

If the Aging Time is too short however, many entries may be aged out too soon. This will result in a high percentage of received packets whose source addresses cannot be found in the forwarding table, in which case the switch will broadcast the packet to all ports, negating many of the benefits of having a switch.

Static forwarding entries are not affected by the aging time.

Filtering

The switch uses a filtering database to segment the network and control communication between segments. It can also filter packets off the network for intrusion control. Static filtering entries can be made by MAC Address or IP Address filtering.

Each port on the switch is a unique collision domain and the switch filters (discards) packets whose destination lies on the same port as where it originated. This keeps local packets from disrupting communications on other parts of the network.

For intrusion control, whenever a switch encounters a packet originating from or destined to a MAC address or an IP Address entered into the filter table, the switch will discard the packet.

Some filtering is done automatically by the switch:

- Dynamic filtering – automatic learning and aging of MAC addresses and their location on the network. Filtering occurs to keep local traffic confined to its segment.
- Filtering done by the Spanning Tree Protocol, which can filter packets based on topology, making sure that signal loops don't occur.
- Filtering done for VLAN integrity. Packets from a member of a VLAN (VLAN 2, for example) destined for a device on another VLAN (VLAN 3) will be filtered.

Some filtering requires the manual entry of information into a filtering table:

- MAC address filtering – the manual entry of specific MAC addresses to be filtered from the network. Packets sent from one manually entered MAC address can be filtered from the network. The entry may be specified as either a source, a destination, or both.
- IP address filtering – the manual entry of specific IP addresses to be filtered from the network (switch must be in IP Routing mode). Packets sent from one manually entered IP address to another can be filtered from the network. The entry may specified as either a

source, a destination, or either (switch must be in IP Routing mode).

Spanning Tree Protocol

The IEEE 802.1D Spanning Tree Protocol allows for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows for the duplicate links to be used in the event of a failure of the primary link. Once the Spanning Tree Protocol is configured and enabled, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically – without operator intervention.

This automatic network reconfiguration provides maximum uptime to network users. However, the concepts of the Spanning Tree Algorithm and protocol are a complicated and complex subject and must be fully researched and understood. It is possible to cause serious degradation of the performance of the network if the Spanning Tree is incorrectly configured. Please read the following before making any changes from the default values.

The DES-3326 STP allows two levels of spanning trees to be configured. The first level constructs a spanning tree on the links between switches. This is referred to as the **Switch** or **Global** level. The second level is on a port group basis. Groups of ports are configured as being members of a spanning tree and the algorithm and protocol are applied to the group of ports. This is referred to as the **Port** or **VLAN** level.

The DES-3326 switch STP performs the following functions:

- Creates a single spanning tree from any combination of switching or bridging elements.
- Creates multiple spanning trees – from any combination of ports contained within a single switch, in user-specified groups.
- Automatically reconfigures the spanning tree to compensate for the failure, addition, or removal of any element in the tree.
- Reconfigures the spanning tree without operator intervention.

STP Operation Levels

The DES-3326 switch allows for two levels of operation: the switch level and the port level. The switch level forms a spanning tree consisting of links between one or more switches. The port level constructs a spanning tree consisting of groups of one or more ports. The STP operates in much the same way for both levels.

On the switch level, STP calculates the Bridge Identifier for each switch and then sets the Root Bridge and the Designated Bridges.

On the port level, STP sets the Root Port and the Designated Ports.

The following are the user-configurable STP parameters for the switch level:

Parameter	Description	Default Value
Bridge Identifier (Not user-configurable except by setting priority below)	A combination of the User-set priority and the switch's MAC address. The Bridge Identifier consists of two parts: a 16-bit priority and a 48-bit Ethernet MAC address.	32768 + MAC

	address	
Priority	A relative priority for each switch – lower numbers give a higher priority and a greater chance of a given switch being elected as the root bridge	32768
Hello Time	The length of time between broadcasts of the hello message by the switch	2 seconds
Maximum Age Timer	Measures the age of a received BPDU for a port and ensures that the BPDU is discarded when its age exceeds the value of the maximum age timer.	20 seconds
Forward Delay Timer	The amount time spent by a port in the learning and listening states waiting for a BPDU that may return the port to the blocking state.	15 seconds

Table 5-1. STP Parameters – Switch Level

The following are the user-configurable STP parameters for the port or port group level:

Variable	Description	Default Value
Port Priority	A relative priority for each port – lower numbers give a higher priority and a greater chance of a given port being elected as the root port	32768
Port Cost	A value used by STP to evaluate paths – STP calculates path costs and selects the path with the minimum cost as the active path.	19 – 100Mbps Fast Ethernet ports 4 – 1000Mbps Gigabit Ethernet ports

Table 5-2. STP Parameters – Port Group Level

Bridge Protocol Data Units

For STP to arrive at a stable network topology, the following information is used:

- The unique switch identifier
- The path cost to the root associated with each switch port
- The port identifier

STP communicates between switches on the network using Bridge Protocol Data Units (BPDUs). Each BPDU contains the following information:

- The unique identifier of the switch that the transmitting switch currently believes is the root switch
- The path cost to the root from the transmitting port
- The port identifier of the transmitting port

The switch sends BPDUs to communicate and construct the spanning-tree topology. All switches connected to the LAN on which the packet is transmitted will receive the BPDU. BPDUs are not directly forwarded by the switch, but the receiving switch uses the information in the frame to calculate a BPDU, and, if the topology changes, initiates a BPDU transmission.

The communication between switches via BPDUs results in the following:

- One switch is elected as the root switch
- The shortest distance to the root switch is calculated for each switch

- A designated switch is selected. This is the switch closest to the root switch through which packets will be forwarded to the root.
- A port for each switch is selected. This is the port providing the best path from the switch to the root switch.
- Ports included in the STP are selected.

Creating a Stable STP Topology

If all switches have STP enabled with default settings, the switch with the lowest MAC address in the network will become the root switch. By increasing the priority (lowering the priority number) of the best switch, STP can be forced to select the best switch as the root switch.

When STP is enabled using the default parameters, the path between source and destination stations in a switched network might not be ideal. For instance, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change. The goal is to make the fastest link the root port.

STP Port States

The BPDUs take some time to pass through a network. This propagation delay can result in topology changes where a port that transitioned directly from a Blocking state to a Forwarding state could create temporary data loops. Ports must wait for new network topology information to propagate throughout the network before starting to forward packets. They must also wait for the packet lifetime to expire for BPDU packets that were forwarded based on the old topology. The forward delay timer is used to allow the network topology to stabilize after a topology change. In addition, STP specifies a series of states a port must transition

through to further ensure that a stable network topology is created after a topology change.

Each port on a switch using STP exists is in one of the following five states:

- Blocking – the port is blocked from forwarding or receiving packets
- Listening – the port is waiting to receive BPDU packets that may tell the port to go back to the blocking state
- Learning – the port is adding addresses to its forwarding database, but not yet forwarding packets
- Forwarding – the port is forwarding packets
- Disabled – the port only responds to network management messages and must return to the blocking state first

A port transitions from one state to another as follows:

- From initialization (switch boot) to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled
- From disabled to blocking

Figure 5-3. STP Port State Transitions

When you enable STP, every port on every switch in the network goes through the blocking state and then transitions through the states of listening and learning at power up. If properly configured, each port stabilizes to the forwarding or blocking state.

No packets (except BPDUs) are forwarded from, or received by, STP enabled ports until the forwarding state is enabled for that port.

Default Spanning-Tree Configuration

Feature	Default Value
Enable state	STP enabled for all ports
Port priority	128
Port cost	19
Bridge Priority	32,768

Table 5-3. Default STP Parameters

User-Changeable STA Parameters

The factory default setting should cover the majority of installations. However, it is advisable to keep the default settings as set at the factory; unless, it is absolutely necessary. The user changeable parameters in the Switch are as follows:

- **Priority** A Priority for the switch can be set from 0 to 65535. 0 is equal to the highest Priority.

- **Hello Time** The Hello Time can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other Switches that it is indeed the Root Bridge. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge.

  Note: *The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.*

- **Max. Age** The Max. Age can be from 6 to 40 seconds. At the end of the Max. Age, if a BPDU has still not been received from the Root Bridge, your Switch will start sending its own BPDU to all other Switches for

permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.

- **Forward Delay Timer** The Forward Delay can be from 4 to 30 seconds. This is the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state.

  Note: *Observe the following formulas when setting the above parameters:*

  Max. Age ≤ 2 x (Forward Delay - 1 second)
  Max. Age ≥ 2 x (Hello Time + 1 second)

- **Port Priority** A Port Priority can be from 0 to 255. The lower the number, the greater the probability the port will be chosen as the Root Port.

- **Port Cost** A Port Cost can be set from 1 to 65535. The lower the number, the greater the probability the port will be chosen to forward packets.

Illustration of STP

A simple illustration of three Bridges (or three switches) connected in a loop is depicted in **Figure 5-3**. In this example, you can anticipate some major network problems if the STP assistance is not applied. If Bridge A broadcasts a packet to Bridge B, Bridge B will broadcast it to Bridge C, and Bridge C will broadcast it to back to Bridge A ... and so on. The broadcast packet will be passed indefinitely in a loop, potentially causing a network failure.

STP can be applied as shown in **Figure 5-4**. In this example, STP breaks the loop by blocking the connection between Bridge B and C. The decision to block a particular connection is based on the STP calculation of the most current Bridge and Port settings. Now, if

Bridge A broadcasts a packet to Bridge C, then Bridge C will drop the packet at port 2 and the broadcast will end there.

Setting-up STP using values other than the defaults, can be complex. Therefore, you are advised to keep the default factory settings and STP will automatically assign root bridges/ports and block loop connections. Influencing STP to choose a particular switch as the root bridge using the **Priority** setting, or influencing STP to choose a particular port to block using the **Port Priority** and **Port Cost** settings is, however, relatively straight forward.

Figure 5-4. Before Applying the STA Rules

In this example, only the default STP values are used.

Figure 5-5. After Applying the STA Rules

The switch with the lowest Bridge ID (switch C) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C. The two (optional) Gigabit ports (default port cost = 4) on switch A are connected to one (optional) Gigabit port on both switch B and C. The redundant link between switch B and C is deliberately chosen as a 100 Mbps Fast Ethernet link (default port cost = 19). Gigabit ports could be used, but the port cost should be increased from the default to ensure that the link between switch B and switch C is the blocked link.

Note also that the example network topology is intended to provide redundancy to protect the network against a link or port failure –

not a switch failure or removal. For example, a failure of switch A would isolate LAN 1 from connecting to LAN 2 or LAN 3.

Port Aggregation

Port aggregation is used to combine a number of ports together to make a single high-bandwidth data pipeline. The participating parts are called members of a link aggregation group, with one port designated as the **master port** of the group. Since all members of the link aggregation group must be configured to operate in the same manner, the configuration of the master port is applied to all members of the link aggregation group. Thus, when configuring the ports in a link aggregation group, you only need to configure the master port.

The DES-3326 supports 6 link aggregation groups, which may include from 2 to 8 switch ports each, except for a Gigabit link aggregation group which consists of the 2 (optional) Gigabit Ethernet ports of the front panel. These ports are the two 1000BASE-SX, -LX –TX or GBIC ports contained in a front-panel mounted module.

The DES-3326 allows the creation of up to 6 link aggregation groups, each group consisting of up to 8 links (ports). The aggregated links must be contiguous (they must have sequential port numbers), except the two (optional) Gigabit ports – which can only belong to a single link aggregation group.

Figure 5-6. 800 Mbps Link Aggregation Group

Data transmitted to a specific host (destination address) will always be transmitted over the same port in a trunk group. This

allows packets in a data stream to arrive in the same order they were sent. A trunk connection can be made with any other switch that maintains host-to-host data streams over a single trunk port. Switches that use a load-balancing scheme that sends the packets of a host-to-host data stream over multiple trunk ports cannot have a trunk connection with the DES-3326 switch.

Setting Up IP Interfaces

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLANs can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLANs also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLANs can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.

Notes About VLANs on the DES-3326

1. *No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets* ***cannot*** *cross VLANs without*

a network device performing a routing function between the VLANs.

2. *The DES-3326 supports only IEEE 802.1Q VLANs. The port untagging function can be used to remove the 802.1Q tag from packet headers to maintain compatibility with devices that are tag-unaware.*

3. *The switch's default - in both* **Layer 2 Only** *mode and* **IP Routing** *mode - is to assign all ports to a single 802.1Q VLAN named* DEFAULT_VLAN*.*

4. *The* DEFAULT_VLAN *has a VID = 1. An IP interface called* **System** *in the IP interface entry menu also has a VID = 1, and therefore corresponds to the* DEFAULT_VLAN.

5. *There is no difference in the creation, deletion, configuration, or editing of 802.1Q VLANs whether the switch is in* **Layer 2 Only**, *or* **IP Routing** *mode, except that once assigned an IP interface, a VLAN cannot be deleted until the IP interface is deleted.*

6. *There is a difference in the* ***behavior*** *of VLANs when the switch is in* **Layer 2 Only** *or* **IP Routing** *mode. In* **Layer 2 Only** *mode, network resources cannot be shared across VLANs. In* **IP Routing** *mode, network resources are shared via routing.*

7. *The switch allows the assignment of an IP interface to each VLAN, in* **IP Routing** *mode. The VLANs must be configured before setting up the IP interfaces. In addition, an IP addressing scheme must be determined.*

8. *A VLAN that is not assigned an IP interface will behave as a layer 2 VLAN – and IP routing will not*

be possible on this VLAN regardless of the switch's operating mode.

IEEE 802.1Q VLANs

Some relevant terms:

Tagging - The act of putting 802.1Q VLAN information into the header of a packet.

Untagging - The act of stripping 802.1Q VLAN information out of the packet header.

Ingress port - A port on a switch where packets are flowing into the switch and VLAN decisions must be made.

Egress port - A port on a switch where packets are flowing out of the switch, either to another switch or to an end station, and tagging decisions must be made.

IEEE 802.1Q (tagged) VLANs are implemented on the DES-3326 Layer 3 switch. 802.1Q VLANs require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

VLANs allow a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast and unicast packets from unknown sources.

VLANs can also provide a level of security to your network. IEEE 802.1Q VLANs will only deliver packets between stations that are members of the VLAN.

Any port can be configured as either *tagging* or *untagging*. The *untagging* feature of IEEE 802.1Q VLANs allow VLANs to work with legacy switches that don't recognize VLAN tags in packet

headers. The *tagging* feature allows VLANs to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

The IEEE 802.1Q standard restricts the forwarding of untagged packets to the VLAN the receiving port is a member of.

The main characteristics of IEEE 802.1Q are as follows:

- Assigns packets to VLANs by filtering.
- Assumes the presence of a single global spanning tree.
- Uses an explicit tagging scheme with one-level tagging.

802.1Q VLAN Packet Forwarding

Packet forwarding decisions are made based upon the following three types of rules:

- Ingress rules – rules relevant to the classification of received frames belonging to a VLAN.
- Forwarding rules between ports – decides filter or forward the packet
- Egress rules – determines if the packet must be sent tagged or untagged.

Figure 5-7. IEEE 802.1Q Packet Forwarding

802.1Q VLAN Tags

The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of 0x8100 in the EtherType field. When a packet's EtherType field is equal to 0x8100, the packet

carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits or user priority, 1 bit of Canonical Format Identifier (CFI – used for encapsulating Token Ring packets so they can be carried across Ethernet backbones) and 12 bits of VLAN ID (VID). The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLANs can be identified.

The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information contained in the packet originally is retained.

Figure 5-8. IEEE 802.1Q Tag

The EtherType and VLAN ID are inserted after the MAC source address, but before the originial EtherType/Length or Logical Link

Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

Figure 5-9. Adding an IEEE 802.1Q Tag

Port VLAN ID

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLANs to span network devices (and indeed, the entire network – if all network devices are 802.1Q compliant).

Unfortunately, not all network devices are 802.1Q compliant. These devices are referred to as *tag-unaware.* 802.1Q devices are referred to as *tag-aware.*

Prior to the adoption 802.1Q VLANs, port-based and MAC-based VLANs were in common use. These VLANs relied upon a Port VLAN ID (PVID) to forward packets. A packet received on a given port would be assigned that port's PVID and then be forwarded to

the port that corresponded to the packet's destination address (found in the switch's forwarding table). If the PVID of the port that received the packet is different from the PVID of the port that is to transmit the packet, the switch will drop the packet.

Within the switch, different PVIDs mean different VLANs. (remember that two VLANs cannot communicate without an external router). So, VLAN identification based upon the PVIDs cannot create VLANs that extend outside a given switch (or switch stack).

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the switch. If no VLANs are defined on the switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, in so far as VLANs are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet forwarding decisions, the VID is.

Tag-aware switches must keep a table to relate PVIDs within the switch to VIDs on the network. The switch will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VIDs are different, the switch will drop the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can have only one PVID, but can have as many VIDs as the switch has memory in its VLAN table to store them.

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted – should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device,

the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

Tagging and Untagging

Every port on an 802.1Q compliant switch can be configured as *tagging* or *untagging.*

Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into and out of it. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet forwarding decisions.

Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into and out of those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Ingress Filtering

A port on a switch where packets are flowing into the switch and VLAN decisions must be made is referred to as an *ingress port*. If ingress filtering is enabled for a port, the switch will examine the VLAN information in the packet header (if present) and decide whether or not to forward the packet.

If the packet is tagged with VLAN information, the ingress port will first determine if the ingress port itself is a member of the tagged VLAN. If it is not, the packet will be dropped. If the

ingress port is a member of the 802.1Q VLAN, the switch then determines if the destination port is a member of the 802.1Q VLAN. If it is not, the packet is dropped. If the destination port is a member of the 802.1Q VLAN, the packet is forwarded and the destination port transmits it to its attached network segment.

If the packet is not tagged with VLAN information, the ingress port will tag the packet with its own PVID as a VID (if the port is a tagging port). The switch then determines if the destination port is a member of the same VLAN (has the same VID) as the ingress port. If it does not, the packet is dropped. If it has the same VID, the packet is forwarded and the destination port transmits it on its attached network segment.

This process is referred to as *ingress filtering* and is used to conserve bandwidth within the switch by dropping packets that are not on the same VLAN as the ingress port at the point of reception. This eliminates the subsequent processing of packets that will just be dropped by the destination port.

Layer 3-Based VLANs

Layer 3-based VLANs use network-layer addresses (subnet address for TCP/IP) to determine VLAN membership. These VLANs are based on layer 3 information, but this does not constitute a 'routing' function.

The DES-3326 allows an IP subnet to be configured for each 802.1Q VLAN that exists on the switch.

Even though a switch inspects a packet's IP address to determine VLAN membership, no route calculation is performed, the RIP protocol is not employed, and packets traversing the switch are bridged using the Spanning Tree algorithm.

A switch that implements layer 3 (or 'subnet') VLANs without performing any routing function between these VLANs is referred to as performing 'IP Switching'.

> ***Note:*** *IP switching does not allow packets to cross VLANs without a network device performing a routing function between the VLANs (IP subnets).*

VLANs in Layer 2 Only Mode

The switch initially configures one VLAN, VID = 1, called the DEFAULT_VLAN. The factory default setting assigns all ports on the switch to the DEFAULT_VLAN. As new VLANs are configured, there respective member ports are removed from the DEFAULT_VLAN.

Packets cannot cross VLANs if the switch is in **Layer 2 Only** mode. If a member of one VLAN wants to connect to another VLAN, the link must be through an external router.

When the switch is in **Layer 2 Only** mode, 802.1Q VLANs are supported.

> ***Note:*** *If no VLANs are configured on the switch and the switch is in* **Layer 2 Only** *mode, then all packets will be forwarded to any destination port. Packets with unknown source addresses will be flooded to all ports. Broadcast and multicast packets will also be flooded to all ports.*
>
> ***Note****: Each IP interface on the switch corresponds to a VLAN. The VLAN must be configured before the IP interface can be setup. The IP interface must have the same name (and the same VID number) as its corresponding VLAN.*
>
> ***Note****: A VLAN that does not have a corresponding IP interface defined for it, will function as a* **Layer 2 Only** *VLAN – regardless of the* **Switch Operation** *mode.*

> ***Note***: *An IP addressing scheme must be determined before the IP interfaces can be setup on the switch. Some consideration is required to arrive at an addressing scheme that will suit the needs of a given network. Please see the section titled* **IP Addressing and Subnetting** *in Chapter 5 for more information.*

The Layer 3 switch allows ranges of IP addresse to be assigned to VLANs. Each VLAN must be configured prior to setting up the corresponding IP interface. An IP addressing scheme must then be established, and implemented when the IP interfaces are set up on the switch.

An example is presented below:

VLAN Name	VID	Switch Ports
System (default)	1	5, 6, 7, 8, 21, 22, 23, 24
Engineering	2	9, 10, 11, 12
Marketing	3	13, 14, 15, 16
Finance	4	17, 18, 19, 20
Sales	5	1, 2, 3, 4
Backbone	6	25, 26

Table 5-4. VLAN Example – Assigned Ports

In this case, 6 IP interfaces (or 6 subnets) are required, so a CIDR notation of 10.32.0.0/3 (or a 3-bit) addressing scheme will work. This addressing scheme will give a subnet mask of 11111111.11100000.00000000.00000000 (binary) or 255.224.0.0 (decimal).

Using a 10.xxx.xxx.xxx IP address notation would give 6 network addresses:

VLAN Name	VID	Network Address
System (default)	1	10.32.0.0
Engineering	2	10.64.0.0
Marketing	3	10.96.0.0
Finance	4	10.128.0.0
Sales	5	10.160.0.0
Backbone	6	10.192.0.0

Table 5-5. VLAN Example – Assigned Network Addresses

The 6 IP interfaces, each with an IP address (or network) address (listed in the table above), and a subnet mask of 255.224.0.0 can be entered into the **Setup IP Interface** menu.

> ***Note:*** *IP interfaces consist of two parts – a subnet mask and a network address.*
>
> ***Note****: Each IP interface listed above will give a maximum of 2,080,800 unique IP addresses per interface (assuming the 10.xxx.xxx.xxx notation).*

DHCP Servers

The Dynamic Host Configuration Protocol (DHCP) can reduce the administrative burden of assigning and maintaining IP address information. DHCP provides reliable and simple TCP/IP network

configuration, ensures that address conflicts do not occur, and helps to conserve the use of IP addresses through the centralized management of address allocation.

> ***Note:*** *For multiple DHCP servers on different subnets to communicate, the* **BOOTP Relay** *function on the DES-3326 must be used to provide a path for the servers to communicate. Servers are identified by IP address.*

Dynamic address allocation enables a client to be assigned an IP address from a pool of free addresses. Each address is assigned with a lease and a lease expiration period. The client must renew the lease to continue using the assigned address. Dynamically assigned addresses can be returned to the free address pool if the computer is not being used, if it is moved to another subnet, of if its lease expires. Usually, network policy ensures that the same IP address is assigned to a client each time and that addresses returned to the free address pool are reassigned.

When the address lease expires, the DHCP client enters the renewing state. The client sends a request message to the DHCP server that provided the address. The DHCP server sends an acknowledgement that contains the new lease and configuration parameters. The client then updates its configuration values and returns to the bound state.

When the DHCP client is in the renewing state, it must release its address immediately in the rare event that the DHCP server sends a negative acknowledgment. The DHCP server sends this message to inform a client that it has incorrect configuration information, forcing it to release its current address and acquire new information.

If the DHCP client cannot successfully renew its lease, the client enters a rebinding state. The client then sends a request message to all DHCP servers in its range, attempting to renew its lease. Any DHCP server that can extend the lease sends and acknowledgement containing the extended lease and updated

configuration information. IF the lease expires or if a DHCP server responds with a negative acknowledgement, the client must release its current configuration, and then return to the initializing state.

If the DHCP client uses more than one network adapter to connect to multiple networks, this protocol is followed for each adapter that the user wants to configure for TCP/IP. Multi-homed systems are selectively configured for any combination of the system's interfaces.

When a DHCP-enabled computer is restarted, it sends a message to the DHCP server with its current configuration information. The DHCP server either confirms this configuration or sends a negative reply so that the client must begin the initializing state again. System startup mignt, therefore, result in a new IP address for a client computer, but neither the user nor the network administrator has to take any action in the configuration process.

Before loading TCP/IP with an address acquired from the DHCP server, DHCP clients check for an IP address conflict by sending an Address Resolution Protocol (ARP) request containing the address. If a conflict is found, TCP/IP does not start, and the user receives an error message. The conflicting address should be removed for the list of active leases or it should be excluded until the conflict is identified and resolved.

Broadcast Storms

Broadcast storms consist of broadcast packets that flood and/or are looped on a network causing noticeable performance degradation and in extreme cases, network failure. Broadcast storms can be caused by malfunctioning NICs, bad cable connections and applications or protocols that generate broadcast traffic, among others.

Broadcast storms have long been a concern for network administrators with routers traditionally being used to prevent their occurrence, and if that failed, limit their scope. However, with the advent of VLANs, switches are now able to limit broadcast domains better and cheaper than routers. Also, many switches, including the DES-3226, have broadcast sensors and filters built into each port to further control broadcast storms.

Segmenting Broadcast Domains

VLANs can be used to segment broadcast domains. They do this by forwarding packets only to ports that are members of the same VLAN. Other parts of the network are effectively shielded. Thus, the smaller the broadcast domain, the smaller effect a broadcast storm will have. Because VLANs are implemented at each switch port, they can be quite effective in limiting the scope of broadcast storms.

Eliminating Broadcast Storms

SNMP agents can be programmed to monitor the number of broadcast packets on switch ports and act on the data. When the number of broadcast packets on a given port rise past an assigned threshold, an action can be triggered. When enabled, the usual action is to block the port from receiving broadcast packets. This will discard all broadcast frames arriving at the port from the attached segment. Not only does this isolate the broadcast domain, but it actually starts removing broadcast packets from the affected segment. When the number of broadcast packets falls to an acceptable level (below the trigger level), the SNMP agent can remove the blocking condition, returning the port to its normal operational state.

In the DES-3326, the default trigger threshold is set to 128,000 broadcast packets per second (128 Kpps) for both 100 Mbps Fast Ethernet ports and the optional 1000 Mbps Gigabit Ethernet ports.

The thresholds can be set separately for the two types of ports and can easily be modified by using a normal SNMP management program or through the console interface.

IP Addressing and Subnetting

This section gives basic information needed to configure your Layer 3 switch for IP routing. The information includes how IP addresses are broken down and how subnetting works. You will learn how to assign each interface on the router an IP address with an unique subnet.

Definitions

- **IP Address** – the unique number ID assigned to each host or interface on a network. IP addresses have the form xxx.xxx.xxx.xxx.
- **Subnet** – a portion of a network sharing a particular network address.
- **Subnet mask** – a 32-bit number used to describe which portion of a Network Address refers to the subnet and which portion refers to the host. Subnet masks have the form xxx.xxx.xxx.xxx.
- **Interface** – a network connection
- **IP Interface** – a network connection that is assigned an IP address.
- **Network Address** – the resulting 32-bit number from a bitwise logical AND operation performed between an IP address and a subnet mask.
- **Subnet Address** – another name for network address.
- **Netmask** – another name for a subnet mask.

In a subnetted network, all addresses consist of ***two*** *parts: an IP address and a subnet mask. The two are used together and one is meaningless without the other.*

IP Addresses

The Internet Protocol (IP) was originally designed to allow communication across network sites comprising the Internet. It was later adapted to allow routing between subnets within a site (within an intranet). The IP includes a system by which an unique number is assigned to each network and to each computer within each network. This number is called the IP address.

IP addresses are written in a 'dotted decimal' notation to make them easier to work with. Some examples follow:

1. 210.202.204.205
2. 189.21.241.56
3. 125.87.0.1

The four decimal (base 10) values in an IP address represent four eight bit binary (base 2) numbers. A computer can only interpret the binary numbers. The dots are simply visual separators, a computer interprets an IP address as a series of 32 binary digits (as a 32 bit number).

The same three IP address, from above, are written below in binary form. The dots are retained for clarity.

1. 11010010.11001010.11001100.11001101
2. 10111101.00010101.11110001.00111000
3. 01111101.01010111.00000000.00000001

Note that in the third value of the third IP address, '0' is represented in binary form as '00000000' and that the forth value, '1' is represented in binary form as '00000001'.

Eight bit numbers are called a 'byte' or an 'octet'. An octet can represent any decimal value between '0' (00000000) and '255' (11111111). IP address values represented in decimal form have four numbers ranging in value from '0' to '255'. The maximum range an IP address can have is then:

Lowest possible IP address -	0.0.0.0
Highest possible IP address -	255.255.255.255

This would allow a maximum of 4,228,250,624 individual IP addresses to be assigned. This number is substantially reduced in practice, however because many of these addresses are reserved.

The following chart can be used to convert octets in binary to decimal:

Binary Octet Digit	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Decimal Equivalent	128	64	32	16	8	4	2	1
Binary Number 128+64+32+16+8+4+2+1= **255**	1	1	1	1	1	1	1	1

Table 5-6. Binary to Decimal Conversion

Each bit in an 8-bit binary number (an octet) represents a power of two. The left-most bit represents 2 raised to the 7th power (2x2x2x2x2x2x2=128), while the right-most digit represents 2 raised to the 0th power, which equals 1 (any number raised to the 0th power equals one, by definition).

IP addresses consist of two parts, one that identifies the network, and one that identifies the destination within the network. In a 'classed' addressing scheme, the class of the IP address determines

which part belongs to the destination and which part belongs to the network.

Address Classes

An IP addressing scheme using 'classes' of IP addresses was developed to make the task of subnetting networks easier. This scheme is consistent and easy to deploy, but is wasteful of IP address space. A new scheme was introduced called Classless Interdomain Routing (CIDR), as an extension of the classed addressing scheme. CIDR allows greater control over the number of IP addresses assigned to a subnet.

The classed IP addressing scheme will be discussed first.

IP addresses used within an intranetwork (within a company network, for instance) have two parts – a network part and a node part. The classed addressing scheme provides a method of determining the information necessary to forward packets to and from the subnetwork.

The classed scheme defines 5 address classes. The first 4 bits in the IP address determine which class the IP address falls in.

- Class A addresses begin with 0xxx, or 1 to 126 decimal.
- Class B addresses begin with 10xx, or 128 to 191 decimal.
- Class C addresses begin with 110x, or 192 to 223 decimal.
- Class D addresses begin with 1110, or 224 to 239 decimal.
- Class E addresses begin with 1111, or 240 to 254 decimal.

Addresses beginning with 01111111, or 127 decimal, are reserved for loopback and internal testing on a local machine. (The address 127.0.0.1 always points loops back to the local computer – so you can always ping this address, if the network is working). Class D addresses are reserved for multicasting. Class E Addresses are reserved for future use.

So there are three classes available for the classed IP addressing scheme. The classed IP addresses are divided into the network part and the node (end station) part:

- Class A NETWORK.node.node.node
- Class B NETWORK.NETWORK.node.node
- Class C NETWORK.NETWORK.NETWORK.node

For example, the IP address 10.42.73.210 is a Class A address (the first number is between 1 and 126), so the first octet (10) belongs to the network, and the remaining three octets belong to the node (42.73.210). Since these numbers are not valid IP addresses, some rules have been developed to make valid (and unique) IP addresses from the network and note part of an IP address.

To specify the network address that corresponds to 10.42.73.210, the first octet – 10 is made into a valid IP address by adding three octets of zeros to give a network address of 10.0.0.0. This method is followed for all classes of a classed subnet.

Additional IP addresses for the subnetwork can be similarly determined. When the remaining octets are set to all binary ones, the broadcast address for the subnetwork is specified. For our example, 10.255.255.255 would be the broadcast address for the subnetwork (remember that eight 1's in binary form is 255 in decimal form).

Note that for Class C networks, only the last octet is set to zeros for the network address, and all ones for the broadcast address. For Class B networks, the last two octets are set to zeros for the network address and all ones for the broadcast address.

To specify the network address for a given IP address, the node section is set to all "0"s. In our example, 10.0.0.0 specifies the network address for 10.42.73.210. When the node section is set to all "1"s, the address specifies a broadcast address that is sent to all hosts on the network. So, 10.255.255.255 is the broadcast address for the network 10.0.0.0. Note that for a Class C networks, only

the last octet is set to "1"s for the broadcast address and that for a Class A networks, the last three octets are set to "1"s for the broadcast address.

Subnet Masking

A subnet mask can be applied to an IP address to identify the network and the node parts of the address. A bitwise logical AND operation between the IP address and the subnet mask results in the *Network Address* (sometimes called the "*Network Number*").

For our example:

00001010.00101010.01001001.11010010 Class A IP address	10.42.73.210
11111111.00000000.00000000.00000000 Class A Subnet Mask	255.0.0.0
00001010.00000000.00000000.00000000 Network Address	10.0.0.0

The Default subnet masks are:

- Class A – 11111111.00000000.00000000.00000000
  255.0.0.0
- Class B – 11111111.11111111.00000000.00000000
  255.255.0.0
- Class C – 1111111.11111111.11111111.00000000
  255.255.255.0

Additional bits can be added to the default subnet mask for a given Class to further subnet a network. This has the effect of making the subnet mask 'longer'. When a bitwise logical AND operation is performed between the subnet mask and the IP address, the result defines the network. Some restrictions apply to the network

address. Addresses of all "0"s and all "1"s are reserved for the local network (when a host does not know it's network address) and for all hosts on the network (the broadcast address). This also applies to subnets. A subnet address cannot be all "0"s or all "1"s. A 1-bit subnet mask is also generally not allowed.

It is important to know how many subnet addresses and how many node addresses within a subnet will be available when implementing an address scheme.

Calculating the Number of Subnets and Nodes

The number of subnet and node addresses available for a given addressing scheme can be calculated using the formula:

$$2^n-2 = \text{Number of nodes or subnets}$$

Where n = the number of bits in either the subnet mask (to determine the number of subnets) or the number of bits in the node part of the IP address (to determine the number of nodes). Multiplying the number of subnets by the number of nodes gives the total number of IP addresses available for the entire network.

Note: *Subnet masks with non-contiguous mask bits are allowed, but not recommended.*

For example:

00001010.00101010.01001001.11010010 Class A IP address	10.42.73.210
11111111.11100000.00000000.00000000 Subnet Mask	255.224.0.0
00001010.00100000.00000000.00000000 Network Address	10.32.0.0

00001010.00101010.11111111.11111111 10.32.255.255
Broadcast Address

This example uses a 3-bit subnet mask. (There are 3 additional bits added to the default Class A subnet mask of 8 bits). So the number of subnets is:

$2^3 – 2 = 8 – 2 = 6$

Subnets of all "0"s and all "1"s are not allowed, so 2 subnets are subtracted from the total.

The number of bits used in the node part of the address is 32 – 11 = 21 bits, so the total number of nodes is:

$2^{21} – 2 = 2{,}097{,}152 – 2 = 2{,}097{,}150$

Multiplying the number of subnets times the number of nodes gives 12,582,900 possible nodes. This is less than the 16,777,214 possible nodes that an unsubnetted Class A network would have.

Subnetting reduces the number of possible nodes for a given network, but increases the segmentation of the network.

Classless InterDomain Routing – CIDR

The classed IP addressing scheme is somewhat wasteful of IP address space. Medium-sized networks were assigned Class B addresses (65533 nodes), and Class A IP addresses (over 16 million nodes) were assigned to large networks. Even a small network was given a Class C IP address that allowed 254 nodes. Most of these assigned addresses were never used.

CIDR allows IP address space to be assigned in a way that the total number of available IP addresses in the assigned space more closely matches the network's actual needs. This method has been adapted for use in intranetworks from the Internet.

Under CIDR, the subnet mask notation is reduced to a simplified shorthand. Instead of spelling out the bits of the subnet mask, it is simply listed as the number of "1"s (bits) in the network portion of the address. The subnet mask of the above example looks like this in binary - 11111111.11100000.00000000.00000000 – and there are 11 "1"s or 11 bits used to mask the network address from the node address. So the example written in CIDR notation becomes:

10.32.0.0/11

This is the reason that non-contiguous bits are not recommended in subnet masks.

CIDR notation can also be used for classed addresses: Class A = /8, Class B = /16, and Class C = /24.

# of Bits	Subnet Mask	CIDR Notation	# of Subnets	# of Hosts	Total Hosts
2	255.192.0.0	/10	2	4194302	8388604
3	255.224.0.0	/11	6	2097150	12582900
4	255.240.0.0	/12	14	1048574	14680036
5	255.248.0.0	/13	30	524286	15728580
6	255.252.0.0	/14	62	262142	16252804
7	255.254.0.0	/15	126	131070	16514820
8	255.255.0.0	/16	254	65534	16645636
9	255.255.128.0	/17	510	32766	16710660
10	255.255.192.0	/18	1022	16382	16742404
11	255.255.224.0	/19	2046	8190	16756740
12	255.255.240.0	/20	4094	4094	16760836
13	255.255.248.0	/21	8190	2046	16756740
14	255.255.252.0	/22	16382	1022	16742404
15	255.255.254.0	/23	32766	510	16710660
16	255.255.255.0	/24	65534	254	16645636

17	255.255.255.128	/25	131070	126	16514820
18	255.255.255.192	/26	262142	62	16252804
19	255.255.255.224	/27	525286	30	15728580
20	255.255.255.240	/28	1048574	14	14680036
21	255.255.255.248	/29	2097150	6	12582900
22	255.255.255.252	/30	4194302	2	8388604

Table 5-7. Class A Subnet Masks

# of Bits	Subnet Mask	CIDR Notation	# of Subnets	# of Hosts	Total Hosts
2	255.255.192	/18	2	16382	32764
3	255.255.224.0	/19	6	8190	49140
4	255.255.240.0	/20	14	4094	57316
5	255.255.248.0	/21	30	2046	61380
6	255.255.252.0	/22	62	1022	63364
7	255.255.254.0	/23	126	510	64260
8	255.255.255.0	/24	254	254	64516
9	255.255.255.128	/25	510	126	64260
10	255.255.255.192	/26	1022	62	63364
11	255.255.255.224	/27	2046	30	61380
12	255.255.255.240	/28	4094	14	57316
13	255.255.255.248	/29	8190	6	49140
14	255.255.255.252	/30	16382	2	32764

Figure 5-8. Class B Subnet Masks

# of Bits	Subnet Mask	CIDR Notation	# of Subnets	# of Hosts	Total Hosts
2	255.255.255.192	/26	2	62	124
3	255.255.255.224	/27	6	30	180
4	255.255.255.240	/28	14	14	196
5	255.255.255.248	/29	30	6	180
6	255.255.255.252	/30	62	2	124

Figure 5-9. Class C Subnet Masks

Internet Protocols

This is a brief introduction to the suite of Internet Protocols frequently referred to as TCP/IP. It is intended to give the reader a reasonable understanding of the available facilities and some familiarity with terminology. It is not intended to be a complete description.

Protocol Layering

The Internet Protocol (IP) divides the tasks necessary to route and forward packets across networks by using a layered approach. Each layer has clearly defined tasks, protocol, and interfaces for communicating with adjacent layers, but the exact way these tasks are accomplished is left to individual software designers. The Open Systems Interconnect (OSI) seven-layer model has been adopted as the reference for the description of modern networking, including the Internet.

A diagram of the OSI model is shown below (note that this is not a complete listing of the protocols contained within each layer of the model):

Figure 5-10. OSI Seven Layer Network Model

Each layer is a distinct set of programs executing a distinct set of protocols designed to accomplish some necessary tasks. They are separated from the other layers within the same system or network, but must communicate and interoperate. This requires very well-defined and well-known methods for transferring messages and data. This is accomplished through the protocol stack.

Protocol layering as simply a tool for visualizing the organization of the necessary software and hardware in a network. In this view, Layer 2 represents switching and Layer 3 represents routing. Protocol layering is actually a set of guidelines used in writing programs and designing hardware that delegate network functions and allow the layers to communicate. How these layers

communicate within a stack (for example, within a given computer) is left to the operating system programmers.

Figure 5-11. The Protocol Stack

Between two protocol stacks, members of the same layer are known as peers and communicate by well-known (open and published) protocols. Within a protocol stack, adjacent layers communicate by an internal interface. This interface is usually not publicly documented and is frequently proprietary. It has some of the same characteristics of a protocol and two stacks from the same software vendor may communicate in the same way. Two stacks from different software vendors (or different products from the same vendor) may communicate in completely different ways. As

long as peers can communicate and interoperate, this has no impact on the functioning of the network.

The communication between layers within a given protocol stack can be both different from a second stack and proprietary, but communication between peers on the same OSI layer is open and consistent.

A brief description of the most commonly used functional layers is helpful to understand the scope of how protocol layering works.

Layer 1

This is referred to as the physical layer. It handles the electrical connections and signaling required to make a physical link from one point in the network to another. It is on this layer that the unique Media Access Control (MAC) address is defined.

Layer 2

This layer, commonly called the switching layer, allows end station addressing and the establishment of connections between them.

Layer 2 switching forwards packets based on the unique MAC address of each end station and offers high-performance, dedicated-bandwidth of Fast or Gigibit Ethernet within the network.

Layer 2 does not ordinarily extend beyond the intranet. To connect to the Internet usually requires a router and a modem or other device to connect to an Internet Service Provider's WAN. These are Layer 3 functions.

Layer 3

Commonly referred to as the routing layer, this layer provides logical partitioning of networks (subnetting), scalability, security, and Quality of Service (QoS).

The backbone of the Internet is built using Layer 3 functions. IP is the premier Layer 3 protocol.

IP is itself, only one protocol in the IP protocol suite. More extensive capabilities are found in the other protocols of the IP suite. For example; the Domain Name System (DNS) associates IP addresses with text names, the Dynamic Host Configuration Protocol (DCHP) eases the administration of IP addresses, and routing protocols such as the Routing Information Protocol (RIP), the Open Shortest Path First (OSPF), and the Border Gateway Protocol (BGP) enable Layer 3 devices to direct data traffic to the intended destination. IP security allows for authentication and encryption. IP not only allows for user-to-user communication, but also for transmission from point-to-multipoint (known as IP multicasting).

Layer 4

This layer, known as the transport layer, establishes the communication path between user applications and the network infrastructure and defines the method of communicating. TCP and UDP are well-known protocols in the transport layer. TCP is a "connection-oriented" protocol, and requires the establishment of parameters for transmission prior to the exchange of data. Web technology is based on TCP. UDP is "connectionless" and requires no connection setup. This is important for multicast traffic, which cannot tolerate the overhead and latency of TCP. TCP and UDP also differ in the amount of error recovery provided and whether or not it is visible to the user application. Both TCP and UDP are layered on IP, which has minimal error recovery and detection.

TCP forces retransmission of data that was lost by the lower layers, UDP does not.

Layer 7

This layer, known as the application layer, provides access to either the end user application software such as a database. Users communicate with the application, which in turn delivers data to the transport layer. Applications do not usually communicate directly with lower layers They are written to use a specific communication library, like the popular WinSock library.

Software developers must decide what type of transport mechanism is necessary. For example, Web access requires reliable, error-free access and would demand TCP, Multimedia, on the other hand, requires low overhead and latency and commonly uses UDP.

TCP/IP

The TCP/IP protocol suite is a set of protocols that allow computers to share resources across a network. TCP and IP are only two of the Internet suite of protocols, but they are the best known and it has become common to refer the entire family of Internet protocols as TCP/IP.

TCP/IP is a layered set of protocols. An example, such as sending e-mail, can illustrate this. There is first a protocol for sending and receiving e-mail. This protocol defines a set of commands to identify the sender, the recipient, and the content of the e-mail. The e-mail protocol will not handle the actual communication between the two computers, this is done by TCP/IP. TCP/IP handles the actual sending and receiving of the packets that make up the e-mail exchange.

TCP makes sure the e-mail commands and messages are received by the appropriate computers. It keeps track of what is sent and what is received, and retransmits any packets that are lost or dropped. TCP also handles the division of large messages into several Ethernet packets, and makes sure these packets are received and reassembled in the correct order.

Because these functions are required by a large number of applications, they are grouped into a single protocol, rather than being the part of the specifications for just sending e-mail. TCP is then a library of routines that application software can use when reliable network communications are required.

IP is also a library of routines, but with a more general set of functions. IP handles the routing of packets from the source to the destination. This may require the packets to traverse many different networks. IP can route packets through the necessary gateways and provides the functions required for any user on one network to communicate with any user on another connected network.

The communication interface between TCP and IP is relatively simple. When IP received a packet, it does not know how this packet is related to others it has sent (or received) or even which connection the packet is part of. IP only knows the address of the source and the destination of the packet, and it makes its best effort to deliver the packet to its destination.

The information required for IP to do its job is contained in a series of octets added to the beginning of the packet called headers. A header contains a few octets of data added to the packet by the protocol in order to keep track of it.

Other protocols on other network devices can add and extract their own headers to and from packets as they cross networks. This is analogous to putting data into an envelope and sending the envelope to a higher-level protocol, and having the higher-level

protocol put the entire envelope into it's own, larger envelope. This process is referred to as encapsulation.

Many levels of encapsulation are required for a packet to cross the Internet.

Packet Headers

TCP Level

Most data transmissions are much longer that a single packet. The data must then be divided up among a series of packets. These packets must be transmitted, received and then reassembled into the original data. TCP handles these functions.

TCP must know how large a packet the network can process. To do this, the TCP protocols at each end of a connection state how large a packet they can handle and the smaller of the two is selected.

The TCP header contains at least 20 octets. The source and destination TCP port numbers are the most important fields. These specify the connection between two TCP protocols on two network devices.

The header also contains a sequence number that is used to ensure the packets are received in the correct order. The packets are not numbered, but rather the octets the packets contain are. If there are 100 octets of data in each packet, the first packet is numbered 0, the second 100, the third 200, etc.

To insure that the data in a packet is received uncorrupted, TCP adds the binary value of all the octets in the packet and writes the sum in the checksum field. The receiving TCP recalculates the checksum and if the numbers are different, the packet is dropped.

Figure 5-12. TCP Packet Header

When packets have been successfully received, TCP sends an acknowledgement. This is simply a packet that has the acknowledgement number field filled in.

An acknowledgement number of 1000 indicates that all of the data up to octet 1000 has been received. If the transmitting TCP does not receive an acknowledgement in a reasonable amount of time, the data is resent.

The window field controls the amount of data being sent at any one time. It would require too much time and overhead to acknowledge each packet received. Each end of the TCP connection declares how much data it is able to receive at any one time by writing this number of octets in the window field.

The transmitting TCP decrements the number in the window field and when it reaches zero, the transmitting TCP stops sending data. When the receiving TCP can accept more data, it increases the

number in the window field. In practice, a single packet can acknowledge the receipt of data and give permission for more data to be sent.

IP Level

TCP sends its packets to IP with the source and destination IP addresses. IP is only concerned with these IP addresses. It is not concerned with the contents of the packet or the TCP header.

IP finds a route for the packet to get to the other end of the TCP connection. IP adds its own header to the packet to accomplish this.

The IP header contains the source and destination addresses, the protocol number, and another checksum.

The protocol number tells the receiving IP which protocol to give the packet to. Although most IP traffic uses TCP, other protocols can be used (such as UDP).

The checksum is used by the receiving IP in the same way as the TCP checksum.

Figure 5-13. IP Packet Header

The flags and fragment offset are used to keep track of packets that must be divided among several smaller packets to cross networks for which they are too large.

The Time-to-Live (TTL) is the number of gateways the packet is allowed to cross between the source and destination. This number is decremented by one when the packet crosses a gateway and when the TTL reaches zero, the packet is dropped. This helps reduce network traffic if a loop develops.

Ethernet Level

Every active Ethernet device has its own Ethernet address (commonly called the MAC address) assigned to it by the manufacturer. Ethernet uses 48 bit addresses.

The Ethernet header is 14 octets that include the source and destination MAC address and a type code.

There is no relationship between the MAC address of a network node and its IP address. There must be a database of Ethernet addresses and their corresponding IP addresses.

Different protocol families can be in use on the same network. The type code field allows each protocol family to have its own entry.

A checksum is calculated and when the packet is received, the checksum is recalculated. If the two checksums are different, the packet is dropped.

Figure 5-14. Ethernet Packet Header

When a packet is received, the headers are removed. The Ethernet Network Interface Card (NIC) removes the Ethernet header and checks the checksum. It then looks at the type code. If the type code is for IP, the packet is given to IP. IP then removes the IP

header and looks at its protocol field. If the protocol field is TCP, the packet is sent to TCP. TCP then looks at the sequence number and uses this number and other data from the headers to reassemble the data into the original file.

Well-Known Sockets and the Application Layer

Application protocols run 'on top of' TCP/IP. When an application wants to send data or a message, it gives the data to TCP. Because TCP and IP take care of the networking details, the application can look at the network connection as a simple data stream.

To transfer a file across a network using the File Transfer Protocol (FTP), a connection must first be established. The computer requesting the file transfer must connect specifically to the FTP server on the computer that has the file.

This is accomplished using sockets. A socket is a pair of TCP port numbers used to establish a connection from one computer to another. TCP uses these port numbers to keep track of connections. Specific port numbers are assigned to applications that wait for requests. These port numbers are referred to as 'well-known' ports.

TCP will open a connection to the FTP server using some random port number, 1234 for example, on the local computer. TCP will specify port 21 for the FTP server. Port 21 is the well-known port number for FTP servers. Note that there are two different FTP programs running in this example – an FTP client that requests the file to be transferred, and an FTP server that sends the file to the FTP client. The FTP server accepts commands from the client, so the FTP client must know how to connect to the server (must know the TCP port number) in order to send commands. The FTP Server can use any TCP port number to send the file, so long as it is sent as part of the connection setup.

A TCP connection is then described by a set of four numbers – the IP address and TCP port number for the local computer, and the IP address and TCP port number for the remote computer. The IP address is in the IP header and the TCP port number is in the TCP header.

No two TCP connection can have the same set of numbers, but only one number needs to be different. It is possible, for example, for two users to send files to the same destination at the same time. This could give the following connection numbers:

	Internet addresses	TCP ports
Connection 1	10.42.73.23, 10.128.12.1	1234, 21
Connection 2	10.42.73.23, 10.128.12.1	1235, 21

The same computers are making the connections, so the IP addresses are the same. Both computers are using the same well-known TCP port for the FTP server. The local FTP clients are using different TCP port numbers.

FTP transfers actually involve two different connections. The connection begins by the FTP sending commands to send a particular file. Once the commands are sent, a second connection is opened for the actual data transfer. Although it is possible to send data on the same connection, it is very convenient for the FTP client to be able to continue to send commands (such as 'stop sending this file').

UDP and ICMP

There are many applications that do not require long messages that cannot fit into a single packet. Looking up computer names is an example. Users wanting to make connections to other computers will usually use a name rather than the computer's IP or MAC address. The user's computer must be able to determine the remote computer's address before a connection can be made. A

designated computer on the network will contain a database of computer names and their corresponding IP and MAC addresses. The user's computer will send a query to the name database computer, and the database computer will send a response. Both the query and the response are very short. There is no need to divide the query or response between multiple packets, so the complexity of TCP is not required. If there is no response to the query after a period of time, the query can simply be resent.

The User Datagram Protocol (UDP) is designed for communications that do not require division among multiple packets and subsequent reassembly. UDP does not keep track of what is sent.

UDP uses port numbers in a way that is directly analogous to TCP. There are well-known UDP port numbers for servers that use UDP.

Figure 5-15. UDP Packet Header

The UDP header is shorter than a TCP header. UDP also uses a checksum to verify that data is received uncorrupted.

The Internet Control Message Protocol (ICMP) is also a simplified protocol used for error messages and messages used by TCP/IP. ICMP, like UDP, processes messages that will fit into a single

packet. ICMP does not, however use ports because its messages are processed by the network software.

The Domain Name System

Computer users usually prefer to use text names for computers they may want to open a connection with. Computers themselves, require 32 bit IP addresses. Somewhere, a database of network devices' text names and their corresponding IP addresses must be maintained.

The Domain Name System (DNS) is used to map names to IP addresses throughout the Internet and has been adapted for use within intranets.

For two DNS servers to communicate across different subnets, the **DNS Relay** of the DES-3326 must be used. The DNS servers are identified by IP addresses.

Mapping Domain Names to Addresses

Name-to-address translation is performed by a program called a Name server. The client program is called a Name resolver. A Name resolver may need to contact several Name servers to translate a name to an address.

The DNS servers are organized in a somewhat hierarchical fashion. A single server often holds names for a single network, which is connected to a root DNS server – usually maintained by an ISP.

Domain Name Resolution

The domain name system can be used by contacting the name servers one at a time, or by asking the domain name system to do the complete name translation. The client makes a query containing the name, the type of answer required, and a code specifying whether the domain name system should do the entire name translation, or simply return the address of the next DNS server if the server receiving the query cannot resolve the name.

When a DNS server receives a query, it checks to see if the name is in its subdomain. If it is, the server translates the name and appends the answer to the query, and sends it back to the client. If the DNS server cannot translate the name, it determines what type of name resolution the client requested. A complete translation is called recursive resolution and requires the server to contact other DNS servers until the name is resolved. Iterative resolution specifies that if the DNS server cannot supply an answer, it returns the address of the next DNS server the client should contact.

Each client must be able to contact at least one DNS server, and each DNS server must be able to contact at least one root server.

The address of the machine that supplies domain name service is often supplied by a DCHP or BOOTP server, or can be entered manually and configured into the operating system at startup.

IP Routing

IP handles the task of determining how packets will get from their source to their destination. This process is referred to as routing.

For IP to work, the local system must be attached to a network. It is safe to assume that any system on this network can send packets

to any other system, but when packets must cross other networks to reach a destination on a remote network, these packets must be handled by gateways (also called routers).

Gateways connect a network with one or more other networks. Gateways can be a computer with two network interfaces or a specialized device with multiple network interfaces. The device is designed to forward packets from one network to another.

IP routing is based on the network address of the destination IP address. Each computer has a table of network addresses. For each network address, a corresponding gateway is listed. This is the gateway to use to communicate with that network. The gateway does not have to be directly connected to the remote network, it simply needs to be the first place to go on the way to the remote network.

Before a local computer sends a packet, it first determines whether the destination address is on the local network. If it is, the packet can be sent directly to the remote device. If it is not, the local computer looks for the network address of the destination and the corresponding gateway address. The packet is then sent to the gateway leading to the remote network. There is often only one gateway on a network.

A single gateway is usually defined as a default gateway, if that gateway connects the local network to a backbone network or to the Internet. This default gateway is also used whenever no specific route is found for a packet, or when there are several gateways on a network.

Local computers can use default gateways, but the gateways themselves need a more complete routing table to be able to forward packets correctly. A protocol is required for the gateways to be able to communicate between themselves and to keep their routing tables updated.

Packet Fragmentation and Reassembly

TCP/IP can be used with many different types of networks, but not all network types can handle the same length packets.

When IP is transmitting large files, large packets are much more efficient than small ones. It is preferable to use the largest possible packet size, but still be able to cross networks that require smaller packets.

To do this, IP can 'negotiate' packet size between the local and remote ends of a connection. When an IP connection is first made, the IPs at both ends of the connection state the largest packet they can handle. The smaller of the two is selected.

When a IP connection crosses multiple networks, it is possible that one of the intermediate networks has a smaller packet size limit than the local or remote network. IP is not able to determine the maximum packet size across all of the networks that may make up the route for a connection. IP has, therefore, a method to divide packets into multiple, smaller packets to cross such networks. This division of large packets into smaller packets is referred to as fragmentation.

A field in the TCP header indicates that a packet has been fragmented, and other information aids in the reassembly of the packets into the original data.

Gateways that connect networks of different packet size limits split the large packets into smaller ones and forward the smaller packets on their attached networks.

ARP

The Address Resolution Protocol (ARP) determines the MAC address and IP address correspondence for a network device.

A local computer will maintain an ARP cache which is a table of MAC addresses and the corresponding IP addresses. Before a connection with another computer is made, the local computer first checks its ARP cache to determine whether the remote computer has an entry. If it does, the local computer reads the remote computer's MAC address and writes it into the destination field of the packets to be sent.

If the remote computer does not have an ARP cache entry, the local computer must send an ARP request and wait for a reply.

When the local computer receives the ARP reply packet, the local ARP reads the IP MAC address pair, and then checks the ARP cache for this entry. If there is an entry, it is updated with the new information. If there is no entry, a new entry is made.

There are two possible cases when an ARP packet is received by a local computer. First, the local computer is the target of the request. If it is, the local ARP replies by sending its MAC IP address pair back to the requesting system. Second, if the local computer is not the target of the request, the packet is dropped.

Multicasting

Multicasting is a group of protocols and tools that enable a single source point to send packets to groups of multiple destination points with persistent connections that last for some amount of time. The main advantage to multicasting is a decrease in the network load compared to broadcasting.

Multicast Groups

There are three types of IP v4 addresses: unicast, broadcast, and multicast. Unicast addresses are used to transmit messages from a

single network device to another, single network device. Broadcast packets are sent to all devices on the subnetwork. Multicast defines a group of network devices or computers that will receive the multicast packets. The members of this group are not necessarily on the same subnetwork. Multicast addresses are used to send multicast packets to the group members.

Multicast Addressing

Class D IP addresses are assigned to a group of network devices that comprise a multicast group. The four most significant four bits of a Class D address are set to "1110". The following 28 bits is referred to as the 'multicast group ID'. Some of the range of Class D addresses are registered with the Internet Assigned Numbers Authority (IANA) for special purposes. For example, the block of multicast addresses ranging from 224.0.0.1 to 224.0.0.225 is reserved for use by routing protocols and some other low-level topology discovery and maintenance protocols.

Figure 5-16. Class D Multicast Address

Some of the reserved IP multicast addresses are as follows:

Address	Meaning
224.0.0.0	Base Address (reserved)
224.0.0.1	All Systems on this subnet
224.0.0.2	All Routers on this subnet

224.0.0.3	Unassigned
224.0.0.4	DVMRP Routers
224.0.0.5	OSPF IGP Routers
224.0.0.6	OSPF IGP Designated Routers
224.0.0.7	ST Routers
224.0.0.8	ST Hosts
224.0.0.9	All RIP2 Routers
224.0.0.10	All IGRP Routers
224.0.0.11	Mobile Agents
224.0.0.12	DHCP Servers and Relay Agents
224.0.0.13	All PIM Routers
224.0.0.14	RSVP Encapsulation
224.0.0.15	All CBT Routers
224.0.0.16	Designated Sbm
224.0.0.17	All Sbms
224.0.0.18	VRRP
224.0.0.19	Unassigned
through	
224.0.0.225	
224.0.0.21	DVMRP on MOSPF

Table 5-10. Reserved Multicast Address Assignments

Internet Group Management Protocol (IGMP)

End users that want to receive multicast packets must be able to inform nearby routers that they want to become a multicast group member of the group these packets are being sent to. The Internet Group Management Protocol (IGMP) is used by multicast routers to maintain multicast group membership. IGMP is also used to coordinate between multiple multicast routers that may be present on a network by electing one of the multicast routers as the 'querier'. This router then keep track of the membership of multicast groups that have active members on the network. IGMP is used to determine whether the router should forward multicast packets it receives to the subnetworks it is attached to or not. A multicast router that has received a multicast packet will check to determine if there is at least one member of a multicast group that has requested to receive multicast packets from this source. If there is one member, the packet is forwarded. If there are no members, the packet is dropped.

IGMP Versions 1 and 2

Users that want to receive multicast packets need to be able to join and leave multicast groups. This is accomplished using IGMP.

Figure 5-17. IGMP Message Format

The IGMP Type codes are shown below:

Type	Meaning
0X11	Membership Query (if Group Address is 0.0.0.0)
0x11	Specific Group Membership Query (if Group Address is Present)
0x16	Membership Report (version 2)
0x17	Leave a Group (version 2)
0x12	Membership Report (version 1)

Table 5-11. IGMP Type Codes

Multicast routers use IGMP to manage multicast group memberships:

- An IGMP "report" is sent by a user's computer to join a group
- IGMP version 1 does not have an explicit 'leave' message. Group members have an expiration timer, and if this timer expires before a query response is returned, the member is dropped from the group.
- IGMP version 2 introduces an explicit "leave" report. When a user wants to leave a group, this report is sent to the multicast router (for IGMP version 2).
- Multicast routers send IGMP queries (to the all-hosts group address: 224.0.0.1) periodically to see whether any group members exist on their subnetworks. If there is no response from a particular group, the router assumes that there are no group members on the network, and multicast packets are not forwarded.

The TTL field of query messages is set to 1 so that the queries do not get forwarded to other subnetworks.

IGMP version 2 introduces a few extensions to IGMP version 1 such as, the election of a single multicast querier for each network, explicit 'leave' reports, and queries that are specific to a particular multicast group.

The router with the lowest IP address is elected as the querier. The explicit group leave message is added to decrease latency, and routers can ask for membership reports from a particular multicast group ID.

The transition states a host will go through to join or leave a multicast group are shown in the diagram below.

Figure 5-18. IGMP State Transitions

Multicast Routing Algorithms

An algorithm is not a program. An algorithm is a statement of how a problem can be solved. A program is written to implement an algorithm.

Multicast packets are delivered by constructing multicast trees where the multicast router is the trunk, the branches are the various subnetworks that may be present, and the leaves are end recipients of the multicast packets. Several algorithms have been developed to construct these trees and to prune branches that have no active mulitcast group members.

Flooding

The simplest algorithm for the delivery of multicast packets is for the multicast router to forward a multicast packet to all interfaces. This is referred to as flooding. An equally simple refinement of flooding is to have the router check to determine if a given multicast packet has been received before (in a certain amount of time). If it has, then the packet does not need to be forwarded at all and can be dropped. If the packet is being received for the first time, it should be flooded to all interface, except the interface on which it was received. This will ensure that all routers on the network will receive at least one copy of the multicast packet.

There are some obvious disadvantages to this simple algorithm. Flooding duplicates a lot of packets and uses a lot of network bandwidth. A multicast router must also keep a record of the multicast packets it has received (for a period of time) to determine if a given packet has been previously received. So flooding uses a lot of router memory.

Multicast Spanning Trees

A multicast delivery tree that spans the entire network with a single active link between routers (or subnetwork) is called a multicast spanning tree. Links (or branches) are chosen such that there is only one active path between any two routers. When a router receives a multicast packet, it forwards the packet on all links except the one on which it was received. This guarantees that all routers in the network will receive a copy of the packet. The only information the router needs to store is whether a link is a part of the spanning tree (leads to a router) or not.

Multicast spanning trees do not use group membership information when deciding to forward or drop a given multicast packet.

Reverse Path Broadcasting (RPB)

The Reverse Path Broadcasting (RPB) algorithm is an enhancement of the multicast spanning tree algorithm. RPB constructs a spanning tree for each multicast source. When the router receives a multicast packet, it then checks to determine if the packet was received on the shortest path back from the router to the source. If the packet was received on the shortest path back to the source, the packet is forwarded on all links except the link on which the packet was received. If the packet was not received on the shortest link back to the source, the packet is dropped.

If a link-state routing protocol is in use, RPB on a local router can determine if the path from the source through the local router to an immediately neighboring router. If it is not, the packet will be dropped at the next router and the packet should not be forwarded.

If a distance-vector routing protocol is in use, a neighboring router can either advertise its previous hop for the source as part of its routing update messages. This will 'poison-reverse' the route (or

have the local router prune the branch from the multicast source to the neighboring router because the neighboring router has a better route from the source to the next router or subnetwork).

Since multicast packets are forwarded through the shortest route between source and destination, RPB is fast. A given router also does not need information about the entire spanning tree, nor does it need a mechanism to stop the forwarding of packets.

RPB does not use multicast group membership information in its forwarding decisions.

Reverse Path Multicasting (RPM)

Reverse Path Multicasting (RPM) introduces an enhancement to RPB – an explicit method to prune branches of the spanning tree that have on active multicast group members for the source. RPM constructs a tree that spans only subnetworks with multicast group member and routers along the shortest path between the source and the destinations.

When a multicast router receives a multicast packet, it is forwarded using the RPB constructed spanning tree. Subsequent routers in the tree that have no active path to another router are referred to as leaf routers. If the multicast packet if forwarded to a leaf router that has no active multicast group members for the source, the leaf router will send a prune message to the previous router. This will remove the leaf router's branch from the spanning tree, and no more multicast packets (from that source) will be forwarded to it. Prune messages have a TTL equal to one, so they can be sent only one hop (one router) back toward the source. If the previous router receives prune messages from all of its branch and leaf routers, the previous router will then send it's own prune message back one router toward the multicast source, and the process will repeat. In this way, multicast group membership information can be used to prune the spanning tree

between a given multicast source and the corresponding multicast group.

Since the membership of any given multicast group can change and the network topology can also change, RPM periodically removes all of the prune information it has gathered from it's memory, and the entire process repeats. This gives all subsequent routers on the network a chance to receive multicast packets from all multicast sources on the network. It also gives all user's a chance to join a given multicast group.

Multicast Routing Protocols

This section contains an overview of two multicast routing protocols – Distance Vector Multicast Routing Protocol (DVMRP), and Protocol Independent Multicast-Dense Mode (PIM-DM). The most commonly used routing protocol (not a multicast routing protocol), the Routing Information Protocol, is discussed in a later section.

Distance Vector Multicast Routing Protocol (DVMRP)

The Distance Vector Multicast Routing Protocol (DVMRP) was derived from the Routing Information Protocol (RIP) with the introduction of multicast delivery trees constructed from information about the 'distance' from the local router back toward the multicast source. DVMRP uses an RPM algorithm to construct its multicast delivery trees.

The first multicast packet received by a multicast router using DVMRP is flooded to all interfaces except the one on which the packet was received. Subsequent prune messages are used to

prune branches of the delivery tree that are either not on the shortest path back to the multicast source, or that have no active multicast group members. A 'graft' message is added that allows a previously pruned branch of the multicast delivery tree to be reactivated. This allows for lower latency when a leaf router adds a new member to a multicast membership group. Graft messages are forwarded one hop (one router) back at a time toward a multicast source until they reach a router that is on an active branch of the multicast delivery tree.

If there is more than one multicast router on a network, the one that has the shortest path back to the multicast source is elected to forward multicast packets from that source. All other routers will discard multicast packets from that source. If two multicast routers on a network have the same distance back to a multicast source, the router with the lowest IP address is elected.

DVMRP also supports tunnel interfaces, where two multicast routers are connected through a router that cannot process multicast packets. This allows multicast packets to cross networks with routers that are not multicast-aware.

Protocol-Independent Multicast (PIM)

There are two protocols in Protocol Independent Multicast (PIM), Protocol Independent Multicast-Dense Mode (PIM-DM) which is used when the multicast destinations are closely spaced, and Protocol Independent Multicast-Sparse Mode (PIM-SM) which is used when the multicast destinations are spaced further apart. PIM-DM is most commonly implemented in an intranetwork (LAN) where the distance between users is minimal.

Protocol-Independent Multicast – Dense Mode (PIM-DM)

PIM-DM uses the RPM algorithm to construct multicast delivery trees, but requires the presence of a unicast routing protocol to find routes back to the multicast source. PIM-DM is however, independent of the mechanisms used by the unicast routing protocol.

PIM-DM floods the first multicast packet it receives on all interfaces except for the interface on which it was received, until it receives explicit prune messages from subsequent routers. So, PIM-DM duplicates multicast packets but removes dependency on a particular routing protocol.

Routing

Routing Information Protocol

The Routing Information Protocol is a distance-vector routing protocol. There are two types of network devices running RIP – active and passive. Active devices advertise their routes to others through RIP messages, while passive devices listen to these messages. Both active and passive routers update their routing tables based upon RIP messages that active routers exchange. Only routers can run RIP in the active mode.

Every 30 seconds, a router running RIP broadcasts a routing update containing a set of pairs of network addresses and a distance (represented by the number of hops or routers between the advertising router and the remote network). So, the vector is the network address and the distance is measured by the number of routers between the local router and the remote network.

RIP measures distance by an integer count of the number of hops from one network to another. A router is one hop from a directly connected network, two hops from a network that can be reached through a router, etc. The more routers between a source and a destination, the greater the RIP distance (or hop count).

There are a few rules to the routing table update process that help to improve performance and stability. A router will not replace a route with a newly learned one if the new route has the same hop count (sometimes referred to as 'cost'). So learned routes are retained until a new route with a lower hop count is learned.

When learned routes are entered into the routing table, a timer is started. This timer is restarted every time this route is advertised. If the route is not advertised for a period of time (usually 180 seconds), the route is removed from the routing table.

RIP does not have an explicit method to detect routing loops. Many RIP implementations include an authorization mechanism (a password) to prevent a router from learning erroneous routes from unauthorized routers.

To maximize stability, the hop count RIP uses to measure distance must have a low maximum value. Infinity (that is, the network is unreachable) is defined as 16 hops. In other words, if a network is more than 16 routers from the source, the local router will consider the network unreachable.

RIP can also be slow to converge (to remove inconsistent, unreachable or looped routes from the routing table) because RIP messages propagate relatively slowly through a network.

Slow convergence can be solved by using split horizon update, where a router does not propagate information about a route back to the interface on which it was received. This reduces the probability of forming transient routing loops.

Hold down can be used to force a router to ignore new route updates for a period of time (usually 60 seconds) after a new route

update has been received. This allows all routers on the network to receive the message.

A router can 'poison reverse' a route by adding an infinite (16) hop count to a route's advertisement. This is usually used in conjunction with triggered updates, which force a router to send an immediate broadcast when an update of an unreachable network is received.

RIP Version 1 Message Format

There are two types of RIP messages: routing information messages and information requests. The same format is used by both types.

Figure 5-19. RIP v.1 Message Format

The COMMAND field operations are defined in the following table:

Command	Meaning
1	Request for partial or full routing information
2	Response containing network-distance pairs from sender's routing table
3	Turn on trace mode (obsolete)
4	Turn off trace mode (obsolete)
5	Reserved for Sun Microsystem's internal use

9	Update Request
10	Update Response
11	Update Acknowledgement

Table 5-12. RIP Command Codes

The field VERSION contains the protocol version number (1 in this case), and is used by the receiver to verify which version of RIP the packet was sent from.

RIP 1 Message

RIP is not limited to TCP/IP. Its address format can support up to 14 octets (when using IP, the remaining 10 octets must be zeros). Other network protocol suites can be specified in the Family of Source Network field (IP has a value of 2). This will determine how the address field is interpreted.

RIP specifies that the IP address 0.0.0.0 denotes a default route.

The distances, measured in router hops are entered in the Distance to Source Network, and Distance to Destination Network fields.

RIP 1 Route Interpretation

RIP was designed to be used with classed address schemes, and does not include an explicit subnet mask. An extension to version 1 does allow routers to exchange subnetted addresses, but only if the subnet mask used by the network is the same as the subnet mask used by the address. This means the RIP version 1 cannot be used to propagate classless addresses.

Routers running RIP version 1 must send different update messages for each IP interface to which it is connected. Interfaces

that use the same subnet mask as the router's network can contain subnetted routes, other interfaces cannot. The router will then advertise only a single route to the network.

RIP Version 2 Extensions

RIP version 2 includes an explicit subnet mask entry, so RIP version 2 can be used to propagate variable length subnet addresses or CIDR classless addresses. RIP version 2 also adds an explicit next hop entry, which speeds convergence and helps prevent the formation of routing loops.

RIP2 Message Format

The message format used with RIP2 is an extension of the RIP1 format:

Figure 5-21. Rip Message Format

RIP version 2 also adds a 16-bit route tag that is retained and sent with router updates. It can be used to identify the origin of the route.

Because the version number in RIP2 occupies the same octet as in RIP1, both versions of the protocols can be used on a given router simultaneously without interference.

6

CONFIGURING THE SWITCH USING THE CONSOLE INTERFACE

Your 24-port NWay Ethernet Layer 3 Switch supports a console management interface that allows you to set up and control your Switch, either with an ordinary terminal (or terminal emulator), or over the network using the TCP/IP **TELNET** protocol. You can use this facility to perform many basic network management functions. In addition, the console program will allow you to configure the Switch for management using an SNMP-based network management system. This chapter describes how to use the console interface to access the Switch, change its settings, and monitor its operation.

Notes are added where clarification is necessary.

Where there is a difference in the setup of the switch between its two operational modes (**Layer 2 Only** and **IP Routing**), the sections are divided to correspond with the switch operating mode that is applicable.

> ***Note:*** **IP Routing** *mode switch configuration settings that are saved to non-volatile RAM using* **Save Changes** *from the* **Main Menu** *are retained in the switch's memory when the operational mode is changed.* **IP Routing** *mode*

settings are simply inactive when the switch is in **Layer 2 Only** *mode.*

Before You Start

The DES-3326 Layer 3 Switch supports a wide array of functions and gives great flexibility and increased network performance by eliminating the routing bottleneck between the WAN or Internet and the Intranet. Its function in a network can be thought of as a new generation of router that performs routing functions in hardware, rather than software. It is a router that also has up to 24+2 independent Ethernet collision domains – each of which can be assigned an IP subnet.

This flexibility and rich feature set requires a bit of thought to arrive at a deployment strategy that will maximize the potential of the DES-3326 Layer 3 switch.

General Deployment Strategy

1. Determine how the network would be best segmented. This is probably done using VLANs in an existing layer 2 switched network.

2. Develop an IP addressing scheme. This involves allocating a block of IP addresses to each network segment. Each network subnet is then assigned a network address and a subnet mask. *See Chapter 5,* **Switch Management Concepts** *section titled* **IP Addressing and Subnetting** *for more information.*

3. Determine which network resources must be shared by the subnets. Shared resources may be connected directly to the

Layer 3 switch, if need be. Static routes to each of the shared resources should be determined.

4. Determine how each subnet will communicate with the WAN or Internet. Again, static routes should be determined and default gateways identified.

5. Develop a security scheme. Some subnets on the network need more security or should be isolated from the other subnets. IP or MAC filtering can be used. Also, one or more VLANs on the Layer 3 switch can be configured without an IP subnet – in which case, these VLANs will function as a layer 2 VLAN and would require an external router to connect to the rest of the network.

6. Develop a policy scheme. Some subnets will have a greater need for multicasting bandwidth, for example. A policy is a mechanism to alter the normal packet forwarding in a network device, and can be used to intelligently allocate bandwidth to time-critical applications such as the integration of voice, video, and data on the network.

7. Develop a redundancy scheme. Planning redundant links and routes to network critical resources can save valuable time in case of a link or device failure. The DES-3326 Spanning Tree function can be used to block the redundant link until it is needed.

VLAN Layout

VLANs on the DES-3326 have rather more functions than on a traditional layer 2 switch, and must therefore be laid-out and configured with a bit more care. Layer 3 VLANs could be thought of as network links – not just as a collection of associated end users. Further, Layer 3 VLANs are assigned an IP network address and subnet mask to enable IP routing between them.

Layer 3 VLANs must be configured on the switch before they can be assigned IP subnets. Further, the static VLAN configuration is specified on a per port basis. On the DES-3326, a VLAN can consist of end-nodes – just like a traditional layer 2 switch, but a VLAN can also consist of one or more layer 2 switches – each of which is connected to multiple end-nodes or network resources.

So, a Layer 3 VLAN, consisting of 4 ports, could be connected to 4 layer 2 switches. If these layer 2 switches each have 24 ports, then the Layer 3 VLAN would contain 4 x 24 = 96 end nodes. Assigning an IP subnet to the Layer 3 VLAN would allow wire-speed IP routing from the WAN to each end node and between end nodes.

So, the IP subnets for a network must be determined first, and the VLANs configured on the switch to accommodate the IP subnets. Finally, the IP subnets can be assigned to the VLANs.

Assigning IP Network Addresses and Subnet Masks to VLANs

The DES-3326 allows the assignment of IP subnets to individual VLANs. Any VLAN configured on the switch that is not assigned an IP subnet, will behave as a layer 2 VLAN and will not be capable of IP routing – even if the switch is in IP Routing mode.

Developing an IP addressing scheme is a complex subject, but it is sufficient here to mention that the total number of anticipated end nodes – for each Layer 3 VLAN – must be accommodated with an unique IP address. It should be noted that the switch regards a VLAN with an IP network address and corresponding subnet mask assigned as an IP interface in IP Routing mode.

> ***Note:*** *See the section titled* **IP Addressing and Subnetting** *in Chapter 5 for more information.*

Defining Static Routes

Routes between the IP interfaces and a default gateway or other router with a WAN connection should be determined beforehand and entered into the static/default routing table on the DES-3326.

Connecting to the Switch

You can use the console interface by connecting the Switch to a VT100-compatible terminal or a computer running an ordinary terminal emulator program (e.g., the **terminal** program included with the Windows operating system) using an RS-232C serial cable. Your terminal parameters will need to be set to:

- VT-100/ANSI compatible
- 9,600 baud
- 8 data bits
- No parity
- One stop bit
- No flow control

You can also access the same functions over a **TELNET** interface. Once you have set an IP address for your Switch, you can use a **TELNET** program (in VT-100 compatible terminal mode) to access and control the Switch. All of the screens are identical, whether accessed from the console port or from a **TELNET** interface.

Console Usage Conventions

The console interface makes use of the following conventions:

1. Items in **<***angle brackets***>** can be toggled between several choices using the space bar.

2. Items in **[***square brackets***]** can be changed by typing in a new value. You can use the backspace and delete keys to erase characters behind and in front of the cursor.

3. The up and down arrow keys, the left and right arrow keys, the tab key and the backspace key, can be used to move between selected items.

4. Items in **UPPERCASE** are commands. Moving the selection to a command and pressing Enter will execute that command, e.g. **APPLY**, etc.

Please note that the command **APPLY** only applies for the current session. Use **Save Changes** from the main menu for permanent changes. **Save Changes** enters the current switch configuration into non-volatile ram, and then reboots the switch.

First Time Connecting To The Switch

The Switch supports user-based security that can allow you to prevent unauthorized users from accessing the Switch or changing its settings. This section tells how to log onto the Switch.

> ***Note:*** *The passwords used to access the Switch are case-sensitive; therefore, "S" is not the same as "s."*

When you first connect to the Switch, you will be presented with the first login screen (shown below).

> ***Note:*** *Press Ctrl+R to refresh the screen. This command can be used at any time to force the console program in the switch to refresh the console screen.*

Figure 6-1. Initial screen, first time connecting to the Switch

Note*: There is no initial username or password. Leave the* **username** *and* **password** *fields blank.*

Note*: The switch's operational mode (***Layer 3** *or* **Layer 2***) is displayed in the upper right-hand corner of every menu in the console. The switch operational mode is changed under* **Switch Settings** *from the* **Main Menu** *and is described later in this manual.*

Press **Enter** in both the Username and Password fields. You will be given access to the main menu shown below:

Figure 6-2. Main Menu

***Note**: The first user automatically gets Root privileges (See Table 6-1). It is recommended to create at least one Root-level user for the Switch.*

Creating User Accounts

To create a new user account, highlight **Setup User Accounts** from the **Main Menu** and press **Enter:**

Figure 6-3. Main Menu

Figure 6-4. Setup User Accounts Menu

User Accounts Management

From the **Main Menu**, highlight S**etup User Accounts** and press Enter, then the **Setup User Accounts** menu appears.

1. Toggle the **Action:< >** field to **<Add>** using the space bar. This will allow the addition of a new user. The other options are **<Delete>** - this allows the deletion of a user entry, and **<Update>** - this allows for changes to be made to an existing user entry.

2. Enter the new user name, assign an initial password, and then confirm the new password. Determine whether the new user should have **<Root>, <User+>**, or **<User>** privileges. The space bar toggles between the three options.

3. Highlight **APPLY** and press enter to make the user addition effective.

4. Press **Esc**. to return to the previous screen or Ctrl+T to go to the root screen.

5. A listing of all user accounts and access levels is shown below the user setup menu. This list is updated when Apply is executed.

6. Please remember that Apply makes changes to the switch configuration for the ***current session only.*** ***A***ll changes (including User additions or updates) must be entered into non-volatile ram using the **Save Changes** command on the **Main Menu** - if you want these changes to be permanent.

Root, User+ and Normal User Privileges

There are three levels of user privileges: *Root* and *User+*, and *User*. Some menu selections available to users with *Root* privileges may not be available to those with *User+* and *User* privileges.

The following table summarizes the *Root, User+* and *User* privileges:

Switch Configuration Management	***Privilege***		
	Root	***User+***	***User***
Configuration	Yes	Read Only	Read Only
Network Monitoring	Yes	Read Only	Read Only
Community Strings and Trap Stations	Yes	Read Only	Read Only
Update Firmware and Configuration Files	Yes	No	No
System Utilities	Yes	Ping Only	Ping Only
Factory Reset	Yes	No	No
Reboot Switch	Yes	Yes	No
User Accounts Management			
Add/Update/Delete User Accounts	Yes	No	No
View User Accounts	Yes	Yes	Yes

Table 6-5. Root, User+, and User Privileges

After establishing a User Account with **Root**-level privileges, press **Esc**. Then highlight **Save Changes** and press **Enter** (see below). The switch will save any changes to its non-volatile ram and reboot. You can logon again and are now ready to continue configuring the Switch.

Saving Changes

The DES-3326 has two levels of memory; normal RAM and non-volatile or NV-RAM. Configuration changes are made effective by highlighting `Apply` and pressing **Enter.** When this is done, the settings will be immediately applied to the switching software in RAM, and will immediately take effect.

Some settings, though, require you to restart the switch before they will take effect. Restarting the switch erases all settings in RAM and reloads the stored settings from the NV-RAM. Thus, it is necessary to save all setting changes to NV-RAM before rebooting the switch.

To retain any configuration changes permanently, highlight Save Changes from the main menu. The following screen will appear to verify that your new settings have been saved to NV-RAM:

Figure 6-6. Main Menu

Figure 6-7. Save Changes Screen

Once the switch configuration settings have been saved to NV-RAM, they become the default settings for the switch. These settings will be used every time the switch is rebooted.

Factory Reset

The only way to change the configuration stored in NV-RAM is to save a new configuration using **Save Changes**, or to execute a **Load Factory Default Configuration** from the main menu. This will clear all settings and restore them to their initial values listed in the Appendix. These are the configuration settings entered at the factory and are the same settings present when the switch was purchased.

Figure 6-8. Main Menu

Highlight **Reboot** from the **Main Menu** and press **Enter.**

Figure 6-9. System Reboot Menu

Highlight the appropriate choice and press **Enter** to reset the switch's NV-RAM to the factory default settings (or just reboot the switch). Loading the Factory Default Configuration will erase any User Accounts (and all other configuration settings) you may have entered and return the switch to the state it was in when it was purchased. The Load Factory Default Configuration Except IP Address option is used when the switch will be managed by the Web-based or Telnet manager, both of which require knowledge of the switch's IP address to function.

Logging Onto The Switch Console

***To log in once you have created a registered user, from the* Login screen:**

1. Type in your **username** and press Enter.
2. Type in your **password** and press Enter.
3. The main menu screen will be displayed based on your access level or privilege.

Updating or Deleting User Accounts

To update or delete a user password:

Choose **`Setup User Accounts`** from the **Main Menu**. The following **`Setup User Accounts`** menu appears:

Figure 6-10. User Accounts Management menu

1. Toggle the **Action:<Add>** field using the space bar to choose **Add, Update**, or **Delete**.

2. Type in the **Username** for the user account you wish to change and enter the **Old Password** for that user account.

3. You can now modify the password or the privilege level for this user account.

4. If the password is to be changed, type in the **New Password** you have chosen, and press **enter**. Type in the same new password in the following field to verify that you have not mistyped it.

5. If the privilege level is to be changed, toggle the Access **Level:<Root>** field until the appropriate level is displayed – **Root, User+** or **User**.

6. Highlight **APPLY** and press **enter** to make the change effective.

7. You must enter the configuration changes into the non-volatile ram (NV-RAM) using **Save Changes** from the **Main Menu** if you want the configuration to be used after a switch reboot.

Only a user with **Root** privileges can make changes to user accounts.

Viewing Current User Accounts

Access to the console, whether using the console port or via **TELNET**, is controlled using a user name and password. Up to eight user accounts can be created. The console interface will not let you delete the current logged-in user, to prevent accidentally deleting all of the users with *Root* privilege.

Only users with the ***Root*** privilege can delete users.

To view the current user accounts:

Highlight **Setup User Accounts** from the **Main Menu**. The current user accounts can be read from following screen:

```
Setup User Accounts
-------------------------------------------------------------------------------
Action:<Add>  Username:[                ]
              New Password:[                ]
              Confirm New Password:[                ]
              Access Level:<User*>                                      APPLY
-------------------------------------------------------------------------------
Current Accounts:        User Name            Access Level
                         ---------------      ------------
                         Bill                     User*
                         Chien                    Root
                         Chris                    User
                         Dan                      User
                         Erin                     User
                         Frank                    User
                         Ian                      User
                         Michael                  Root
-------------------------------------------------------------------------------
Function:
Message:
CTRL+I = Root screen          Esc=Prev. screen              CTRL+R = Refres
```

Figure 6-11. Viewing User Accounts

Deleting a User Account

To delete a user account:

```
Setup User Accounts
-------------------------------------------------------------------------------
Action:<Delete>  Username:[                ]  Old Password:[                ]

                                                                        APPLY
-------------------------------------------------------------------------------
Current Accounts:        User Name            Access Level
                         ---------------      ------------
                         Bill                     User*
                         Chien                    Root
                         Chris                    User
                         Dan                      User
                         Erin                     User
                         Frank                    User
                         Ian                      User
                         Michael                  Root
-------------------------------------------------------------------------------
Function:
Message:
CTRL+I = Root screen          Esc=Prev. screen              CTRL+R = Refres
```

Figure 6-12. Deleting User Accounts

1. Toggle the **Action:<Add>** field to **Delete**.
2. Enter the **Username** and **Old Password** for the account you want to delete. You must enter the password for the account to be able to delete it.
3. Highlight **APPLY** and press **Enter** to make the deletion of the selected user take effect.
4. You must enter the configuration changes into the non-volatile ram (NV-RAM) using **Save Changes** from the **Main Menu** if you want the configuration to be used after a switch reboot.

Only users with **Root** privileges can delete user accounts.

Setting Up The Switch

Basic Setup

This section will help prepare the Switch user by describing the **Switch Information, Remote Management Setup, Configure Ports, Serial Port Settings** and **Switch Settings** menus.

Figure 6-13. Main Menu – Basic Setup

Switch Information

Highlight **Switch Information** from the **Main Menu** and press **Enter:**:

Figure 6-14. Switch Information Menu

The **Switch Information** shows the type of switch (Layer 3), which (if any) external modules are installed, and the switch's **MAC Address** (assigned by the factory and unchangeable). In addition, the **Boot PROM** and **Firmware Version** numbers are shown. This information is helpful to keep track of PROM and Firmware updates and to obtain the switch's MAC address for entry into another network device's address table – if necessary.

You can also enter the name of the **System**, its location, and the name and telephone number of the System Administrator. It is recommended that the person responsible for the maintenance of the network system that this Layer 3 switch is installed on be listed here.

Remote Management Setup

Some settings must be entered to allow the switch to be managed from an SNMP-based Network Management System such as SNMP v1 or to be able to access the Switch using the TELNET

protocol or the WEB-based Manager. Please see the next chapter for Web-based network management information.

The **Remote Management Setup** menu lets you specify how the switch will be assigned an IP address to allow the switch to be identified on the network.

To setup the switch for remote management:

Highlight **Remote Management Setup** from the main menu. The following screen appears:

Figure 6-15. Remote Management Setup

Configuring the Switch's IP Address

The Switch needs to have an IP address assigned to it so that an In-Band network management system (eg. **WEB-based Manager** or **TELNET**) client can find it on the network. The **Remote Management Setup** screen allows you to change the settings for the two different management interfaces used on the Switch: the

Ethernet interface used for in-band communication, and the SLIP interface used over the console port for out-of-band communication.

The fields listed under the **Current Settings** heading are those that are currently being used by the switch. Those fields listed under the Restart Settings heading are those which will be used after the switch has been Rebooted.

Toggle the **Get IP From: < >** field using the space bar to choose from **Manual**, **BOOTP**, or **DCHP**. This selects how the switch will be assigned an IP address on the next reboot (or startu**p**).

The **Get IP From: < >** options are:

- **BOOTP -** The switch will send out a BOOTP broadcast request when it is powered up. The BOOTP protocol allows IP addresses, network masks, and default gateways to be assigned by a central BOOTP server. If this option is set, the Switch will first look for a BOOTP server to provide it with this information before using the default or previously entered settings.

- **DCHP –** The switch will send out a DCHP broadcast request when it is powered up. The DCHP protocol allows IP addresses, network masks, and default gateways to be assigned by a DCHP server. If this option is set, the switch will first look for a DCHP server to provide it with this information before using the default or previously entered settings.

- **Manual** – Allows the entry of an IP address, Subnet Mask, and a Default Gateway for the switch. These fields should be of the form *xxx.xxx.xxx.xxx*, where each *xxx* is a number (represented in decimal form) between 0 and 255. This address should be a unique address on the network assigned for use by the Network Administrator. The fields which require entries under this option are as follows:

- **Subnet Mask –** A Bitmask that determines the extent of the subnet that the Switch is on. Should be of the form *xxx.xxx.xxx.xxx*, where each *xxx* is a number (represented in decimal) between 0 and 255. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed.

- **Default Gateway** - IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an intranet, or you do not want the Switch to be accessible outside your local network, you can leave this field unchanged.

- **Management VID:[ ]** – Allows the entry of the VLAN ID (VID) of a VLAN that will have access to the Web-based manager and to the Telnet manager. This will be the VID of the VLAN that a management station is located on.

Setting Up Trap Receivers

This allows the switch to send traps (messages about errors, etc.) to management stations on the network. Highlight **Setup Trap Recipients** and press **enter.** The trap recipients can be setup from the following screen:

Figure 6-16. Setup Trap Recipients Menu

The **IP Address** field is the IP address of a management station (usually a computer) that is configured to receive the SNMP traps from the switch.

The **SNMP Community String** is similar to a password in that stations that do not know the correct string cannot receive or request SNMP information from the switch.

The **Status** field can be toggled between `Enabled` and `Disabled` to enable or disable the receipt of SNMP traps by the listed management stations.

***Note**: Up to four SNMP trap recipients can be entered.*

Configure Ports

Highlight **Configure Ports** from the main menu and press **enter**:

Figure 6-17. Configure Ports Screen

Toggle the **View Ports:<1 to 12 >** field, using the space bar, to view the configuration of either ports 1 through 12 or ports 13 through 24. To configure an specific port, toggle the **Configure Port:[ ]** field until the appropriate port number appears.

Toggle the **State:< >** field to either **Enable** or **Disable** a given port.

Toggle the **Speed/Duplex:< >** field to either select the speed and duplex/half-duplex state of the port. Auto – auto-negotiation between 10 and 100 Mbps devices, full- or half-duplex. The Auto setting allows the port to automatically determine the fastest settings the device the port is connected to can handle, and then to use those settings. The other options are **100M/Full, 100M/Half, 10M/Full, 10M/Half.** There is no automatic adjustment of port settings with any option other than **Auto**.

Serial Port Settings

The S**erial Port Settings** screen allows the configuration of the switch's serial port and out-of-band TCP/IP communications using SLIP.

Highlight **Serial Port Settings** and press **enter.**

Figure 6-18. Serial Port Settings Screen

Toggle the **Select Protocol:<** **>** field to select either the **Console** or **SLIP protocol**.

The following fields can then be set:

- **Auto-Logout -** This sets the time the interface can be idle before the switch automatically logs-out the user. The options are **2 mins, 5 mins, 10 mins, 15 mins,** or **Never.**
- **Baud Rate** - Sets the serial bit rate that will be used to communicate the next time the Switch is restarted.

Applies only when the serial port is being used for out-of-band (SLIP) management; it does not apply when the port is used for the console port. Available speeds are **2400, 9600, 19,200** and **38,400** bits per second. The default setting is **9600**.

- **Interface Name –** This allows for the naming of the SLIP interface for easy reference.
- **Remote IP Address –** This is the IP address of the management station that will use the SLIP protocol to communicate with the switch.
- **State –** Toggled between Enabled and Disabled as the SLIP connection is enabled or disabled.

Switch Operation Mode

Note: *The switch will retain the configuration entered for* **IP Routing** *when in* **Layer 2 Only** *mode (if the configuration is saved to NV-RAM), but the* **IP Routing** *configuration will not be active. The* **IP Routing** *configuration will become active when the switch is again put in* **IP Routing** *mode.*

Note: *Putting the switch in* **IP Routing** *mode does not – by itself – enable IP routing. The switch must be configured to use IP interfaces before it is capable of IP routing. (See the section titled* **Setting up IP Interfaces** *below.)*

The switch can operate in one of two modes:

1. **Layer 2 Only with IEEE 802.1Q VLAN support**: the switching process is based upon the source and destination MAC addresses only. 802.1Q VLANs are

supported and the switch is considered as a VLAN-tag aware device.

2. **IP Routing with IEEE 802.1Q VLAN support**: the switching process is based upon the IP source and destination addresses, if present. If the IP addresses are not present, the switching process is based upon the MAC addresses (as in Layer 2 above). 802.1Q VLANs are supported and the switch is considered as a VLAN-tag aware device.

The switch must be rebooted when changing the operation mode before the new operation mode can take effect.

Changing the Switch Operation Mode

To change the switch's operating mode:

Highlight **Switch Settings** on the main menu and press **enter.**

Figure 6-19. Switch Settings Screen

Highlight **Switch Operation Mode** on the **Switch Settings** menu and press **enter.**

Figure 6-20. Switch Mode Selection Screen

The field **Select switch operation mode:<** **>** can be toggled using the space bar to one of the two switch operation modes: **Layer 2 Only, Support IEEE 802.1Q VLANs** and **IP Routing, Support IEEE 802.1Q VLANs**.

To make a change in the operation mode of the switch effective, highlight **APPLY** and press **enter.**

Figure 6-21. Change Mode Confirmation Screen

Type **y** and press **Enter.** The switch will then save the changes made during the current session and reboot. The switch must be rebooted to change the operation mode.

Switch Settings – IP Routing Mode

Once the switch is configured for IP Routing (Layer 3 Switching), and rebooted, the **Switch Settings** menu adds some functions compared to the Layer 2 Only mode (figure 6-21 and 6-22, below).

Figure 6-22. Main Menu – Layer 3 IP Routing Mode

Figure 6-23. Main Menu – Layer 2 Switching Mode

Layer 2 Switch Settings

> **Note:** *Layer 2 Switch functions and settings are also available when the switch is configured to operate in the IP Routing (Layer 3) mode.*

To access the Layer 2 Switch Settings menu, highlight **Layer 2 Switch Settings** on the **Switch Settings** menu and press Enter:

Figure 6-24. Layer 2 Switch Settings Menu

The following fields can then be set:

MAC Address Aging Time(sec):[300] This field specifies the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). The Aging Time can be set to any value between **10** and **1,000,000** seconds.

> ***Note***: *A very long Aging Time can result with the out-of-date Dynamic Entries that may cause incorrect packet filtering/forwarding decisions. A very short aging time*

may cause entries to be aged out to soon, resulting in a high percentage of received packets whose source addresses cannot be found in the address table, in which case the switch will broadcast the packet to all ports, negating many of the benefits of having a switch.

Switch GVRP: <Disabled> Group VLAN Registration Protocol is a protocol that allows members to dynamically join VLANs.

Switch GMRP:<Disabled> Group Multicast Registration Protocol is a protocol that allows members to dynamically join Multicast groups.

Broadcast/Multicast Storm Control: The following are a series of entry fields for the parameters that control how the switch will react to Broadcast and Multicast storms:

Upper Threshold for Base Ports: [128]Kpps This is the number of thousands Broadcast/Multicast packets per second received by the switch – on one of the base ports – that will trigger the switch's reaction to a Broadcast/Multicast storm.

Upper Threshold for Module Ports: [128]Kpps This is the number of thousands Broadcast/Multicast packets per second received by the switch – on one of the module ports – that will trigger the switch's reaction to a Broadcast/Multicast storm.

Broadcast Storm Mode:<Disabled> This field can be toggled between **Enabled** and **Disabled** using the space bar. This enables or disables, globally, the switch's reaction to Broadcast storms, triggered at the threshold set above.

Multicast Storm Mode:<Disabled> This field can be toggled between **Enabled** and **Disabled** using the space bar. This enables or disables, globally, the switch's reaction to Multicast storms, triggered at the threshold set above.

Layer 3 IP Routing Protocol Settings

> ***Note:*** *These IP Routing Protocol Settings are only for enabling or disabling, globally, routing protocols available on the switch. The Routing Information Protocol (RIP) is setup under* **IP Networking** *from the* **Main Menu.**

To access the **Layer 3 Switch Settings** menu, highlight **Layer 3 IP Routing Protocol Settings** on the **Switch Settings** menu and press **enter**.

Figure 6-25. Layer 3 IP Routing Protocol Settings

IP Multicast Settings:

> **DVMRP state :<Disabled>** This field can be toggled between **Enabled** and **Disabled** using the space bar. This enables or disables, globally, the Distance-Vector Multicast Routing Protocol (DVMRP).

DVMRP Include Report from Unknown Neighbor :<Disabled> This field can be toggled between **Enabled** and **Disabled** using the space bar. This enables or disables the inclusion of DVMRP membership reports from unknown neighbor routers.

PIM-DM state :<Enabled> This field can be toggled between **Enabled** and **Disabled** using the space bar. This enables or disables, globally, the Protocol Independent Multicasting – Dense Mode (PIM-DM) multicasting protocol.

The DVMRP and PIM-DM are set using the **IP Multicasting Settings** – from the **Main Menu** under **Multicasting**.

Highlight **APPLY** and press enter to make the changes current.

Layer 3 Switch Mode - Setup RIP

The Routing Information Protocol (RIP) is a distance-vector protocol that uses the hop count as its criteria for making routing decisions. RIP is an Interior Gateway Protocol (IGP), which means that it performs routing within a single autonomous system.

Highlight **Setup RIP Configuration** from the **Layer 3 IP Networking** menu and press **enter**.

Figure 6-26. RIP Configuration Menu

RIP Status:<Disabled> can be toggled between **Enabled** and **Disabled** using the space bar. This function allows the RIP protocol to be turned on or off without changing the RIP setup.

Highlight **Setup RIP** on the **RIP Configuration** menu (from the **Setup Layer 3 – IP Networking** menu) and press **enter**.

Figure 6-27. Layer 3 – Setup RIP Menu

Interface Name:[ ] is the name of the IP interface on which RIP is to be setup. This interface must be previously configured on the switch.

Authentication:<Enabled> is toggled between **Enabled** and **Disabled**. When authentication is enabled, a password is used to authenticate communication between routers on the network. Authentication is only supported when RIP is in V1 Compatible or V2 mode.

Password:[ ] is a password to be used to authenticate communication between routers on the network.

TX Mode:<V2 Only> is toggled between **Disabled, V1 Only, V1 Compatible,** and **V2 Only**. This entry specifies which version of the RIP protocol will be used to transmit RIP packets. Disabled prevents the transmission of RIP packets.

RX Mode:<V2 Only> is toggled between **Disabled, V1 Only, V2 Only,** and **V1 and V2**. This entry specifies which version of the

RIP protocol will be used to interpret received RIP packets. Disabled prevents the reception of RIP packets.

Advanced Setup

The switch operation mode setting changes the menus and configuration options for the Advanced Setup of the switch. This section of the manual is therefore divided into two sections for each Advanced Setup menu item to reflect the two switch operation modes – **Layer 2 with IEEE 802.1Q VLAN support** and **IP Routing with IEEE 802.1Q VLAN support.** Where there is no difference in the setup between the two switch operation modes, only one section will be presented.

Configuring VLANs

> ***Note:*** *The switch allows the assignment of an IP interface to each VLAN, in* ***IP Routing*** *mode. The VLANs must be configured before setting up the IP interfaces. VLANs in Layer 2 Only Mode*

The switch reserves one VLAN, VID = 1, called the DEFAULT_VLAN for internal use. The factory default setting assigns all ports on the switch to the DEFAULT_VLAN. As new VLANs are configured, there respective member ports are removed from the DEFAULT_VLAN. If the DEFAULT_VLAN is reconfigured, all ports are again assigned to it. Ports that are not desired to be part of the DEFAULT_VLAN are removed during the configuration.

Packets cannot cross layer 2 VLANs. If a member of one layer 2 VLAN wants to connect to another layer 2 VLAN, it must be through a router.

VLANs by Switch Operating Mode – Layer 2 Only and IP Routing

> ***Note:*** *The switch's default - in both* ***Layer 2 Only*** *mode and* ***IP Routing*** *mode - is to assign all ports to a single 802.1Q VLAN named* DEFAULT_VLAN*. As new VLANs are created, the member ports assigned to the new VLAN will be removed from the default VLAN port member list.*
>
> ***Note****: The* DEFAULT_VLAN *has a VID = 1. An IP interface called System in the IP interface entry menu also has a VID = 1, and therefore corresponds to the* DEFAULT_VLAN.

To create a new 802.1Q VLAN*:*

The VLAN menu adds an entry to edit the VLAN definitions and to configure the port settings for IEEE 802.1Q VLAN support. Highlight **VLANs** from the **Main Menu** and press **enter**.

Figure 6-27. VLAN Menu

To create an 802.1Q VLAN, highlight **Edit 802.1Q VLANs** and press **Enter:**

Figure 6-28. Edit 802.1Q VLANs Menu

To create an 802.1Q VLAN, toggle the **Action: <Add/Modify>** field to **Add/Modify** using the space bar. Enter a VLAN ID number in the **VID#[ ]** field and a name for the new VLAN in the **VLAN Name:[ ]** field.

Choose which ports will be members of the new VLAN and enter their membership status in the **Membership (E/F/-): [ ][ ][ ]** field. The status indicators of the individual ports can be entered directly from the keyboard or toggled using the space bar. Moving between the status indicators of the individual ports is accomplished using the arrow keys.

To set the 802.1Q VLAN membership status of a port:

To enter the 802.1Q VLAN status for a port, highlight the first field of **Membership (E/F/-): [ ][ ][ ].** Each port's 802.1Q VLAN membership can be set individually by highlighting the port's entry using the arrow keys, and then toggling between E, F, or – using the space bar.

> **E** - (Egress Member) specifies the port as being a static member of the VLAN. Egress Member Ports are ports that will be transmitting traffic for the VLAN. These ports can be either tagged or untagged.
>
> **F** - (Forbidden Non-Member) specifies the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically.
>
> **-** (Non-Member) specifies the port as not being a member of the VLAN, but the port can become a member of the VLAN dynamically.

Next, determine which of the ports that are members of the new VLAN will be Tagged or Untagged ports.

***To set a port as either a Tagged or an Untagged port*:**

Highlight the first field of **Tagging (U/T):[ ][ ][ ]** field. Each port's state can be set by highlighting the port's entry using the arrow keys and then toggling between U or T using the space bar.

> **U** - specifies the port as an Untagged member of the VLAN. When an untagged packet is transmitted by the port, the packet header remains unchanged. When a tagged packet exits the port, the tag is stripped and the packet is changed to an untagged packet.
>
> **T** - specifies the port as a Tagged member of the VLAN. When an untagged packet is transmitted by the port, the packet header is changed to include the 32-bit tag associated with the PVID (Port VLAN Identifier – see below). When a tagged packet exits the port, the packet header is unchanged.

If the port is attached to a device that is not IEEE 802.1Q VLAN compliant (VLAN-tag unaware), then the port should be set to U – Untagged.

If the port is attached to a device that is IEEE 802.1Q VLAN compliant, (VLAN-tag aware), then the port should be set to T – Tagged.

Press **APPLY** to make the additions/deletions effective for the current session. To make enter the IP Interfaces into Non-volatile RAM, highlight **Save Changes** from the Main Menu and press enter.

In the following example screen, the VLAN "evilJulius" - VID# 2 – has been added. Ports 1, 2,12, 14, 17, S1P1, and S1P2 are Egress ports (static members of "evilJulius". Ports 5, 6, and 7 are Forbidden ports (non-members and are not allowed to join the VLAN "evilJulius" dynamically.

Example 802.1Q VLAN add screen:

Figure 6-29. Edit 802.1Q VLANs Menu

To configure the member ports of an 802.1Q VLAN:

Figure 6-30. VLAN Menu

To configure the port settings of an 802.1Q VLAN, highlight **Configure 802.1Q Port Settings** and press **enter:**

Figure 6-31. Configure 802.1Q Port Settings

Each port can be configured to use an Ingress Filter. The ports to be configured in a given session can be identified by either entering a range of port numbers or by entering the PVID#.

Ingress filtering is toggled between **On** and **Off** using the space bar.

To configure a port's 802.1Q VLAN settings:

Highlight the **Configure Port from [ ] to [ ]** field and enter the range of port numbers you want to configure. As an alternative you can use the arrow keys to highlight the **PVID#[ ]** field and enter the PVID for the VLAN's member ports you want to configure.

PVID – Port VLAN Identifier – is a classification mechanism that associates a port with a specific VLAN and is used to make forwarding decisions for untagged packets received by the port. For example, if port #2 is assigned a PVID of 3, then all untagged packets received on port #2 will be assigned to VLAN 3. This number is generally the same as the VID# number assigned to the port in the Edit 802.1Q VLANs menu above.

Use the arrow keys to highlight the remaining fields and the space bar to toggle between On and Off.

Ingress Filter – this enables the port to compare the VID tag of an incoming packet with the PVID number assigned to the port. If the two are different, the port filters (drops) the packet.

GVRP – Group VLAN Registration Protocol – this enables the port to dynamically become a member of a VLAN.

GMRP – Group Multicast Registration Protocol – this enables the port to dynamically become a member of a multicast group.

To edit an existing 802.1Q VLAN:

Highlight **VLANs** on the main menu and press **Enter:**

Figure 6-32. VLAN Menu

To edit an existing 802.1Q VLAN, highlight **Edit 802.1Q VLANs** and press **Enter:**

Figure 6-33. Edit 802.1Q VLANs Menu

To edit an existing 802.1Q VLAN, highlight the **Action:<Add/Modify>** field and toggle between **Add/Modify** and **Delete**. In the **Add/Modify** mode, both individual entrees to a selected VLAN and entire VLANs can be added. In the **Delete** mode, entire VLANs can be deleted. VLANs to be edited can be selected by either the **VID#[ ]** field or the **VLAN Name:[ ]** fields. Enter either the VID or the VLAN Name for the 802.1Q VLAN you want to edit and press **enter**.

> Note: *To delete an entire VLAN, toggle the* **Action:<Add/Modify>** *field to* Delete, *enter either the VID or the VLAN Name in the appropriate field and press* ***Enter.*** *Highlight* Apply *and press* ***Enter.*** *The selected VLAN will be deleted. To enter the change into Non-volatile RAM, select* **Save Changes** *from the Main Menu.*

The 802.1Q VLANs are edited by specifying which ports will be Egress Members, Forbidden non-members or non-members.

The ports are further set to be either a Tagged or an Untagged port.

***To edit the 802.1Q VLAN membership of a port*:**

Highlight the first field of **Membership (E/F/-): [ ][ ][ ]**. Each port's 802.1Q VLAN membership can be set individually by highlighting the port's entry using the arrow keys, and then toggling between E, F, or – using the space bar.

> **E** - (Egress Member) specifies the port as being a static member of the VLAN. Egress Member Ports are ports that will be transmitting traffic for the VLAN. These ports can be either tagged or untagged.
>
> **F** - (Forbidden Non-Member) specifies the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically.

- (Non-Member) specifies the port as not being a member of the VLAN, but the port can become a member of the VLAN dynamically.

To edit a port's Tagged or Untagged status:

Highlight the first field of **Tagging (U/T):[ ][ ][ ]** field. Each port's state can be set by highlighting the port's entry using the arrow keys and then toggling between **U** or **T** using the space bar.

U - specifies the port as an Untagged member of the VLAN. When an untagged packet is transmitted by the port, the packet header remains unchanged. When a tagged packet exits the port, the tag is stripped and the packet is changed to an untagged packet.

T - specifies the port as a Tagged member of the VLAN. When an untagged packet is transmitted by the port, the packet header is changed to include the 32-bit tag associated with the PVID (Port VLAN Identifier – see below). When a tagged packet exits the port, the packet header is unchanged.

If the port is attached to a device that is not IEEE 802.1Q VLAN compliant (VLAN-tag unaware), then the port should be set to U – Untagged.

If the port is attached to a device that is IEEE 802.1Q VLAN compliant, (VLAN-tag aware), then the port should be set to T – Tagged.

Each port can be configured to have a PVID or to use an Ingress Filter.

To configure a port's 802.1Q VLAN settings:

Highlight the **Configure Port#[ ]** field and enter the port number of the port you want to configure. Use the arrow keys to highlight the **PVID#[ ]** field and enter the PVID for the port.

PVID – Port VLAN Identifier – is a classification mechanism that associates a port with a specific VLAN and is used to make forwarding decisions for untagged packets received by the port. For example, if port #2 is assigned a PVID of 3, then all untagged packets received on port #2 will be assigned to VLAN 3. This number is generally the same as the VID# number assigned to the port in the **Edit Existing 802.1Q VLANs** menu above.

Use the arrow keys to highlight the remaining fields and the space bar to toggle between On and Off.

Ingress Filter – this enables the port to compare the VID tag of an incoming packet with the PVID number assigned to the port. If the two are different, the port filters (drops) the packet.

GVRP – Group VLAN Registration Protocol – this enables the port to dynamically become a member of a VLAN.

GMRP – Group Multicast Registration Protocol – this enables the port to dynamically become a member of a multicast group.

Setting Up IP Interfaces

***Note**: Each IP interface on the switch corresponds to a VLAN. The VLAN must be configured before the IP interface can be setup.*

***Note**: A VLAN that does not have a corresponding IP interface defined for it, will function as a* **Layer 2 Only** *VLAN – regardless of the* **Switch Operation** *mode.*

The Layer 3 switch allows ranges of IP addresses (OSI layer 3) to be assigned to VLANs (OSI layer 2). Each VLAN must be

configured prior to setting up the corresponding IP interface. An IP addressing scheme must then be established, and implemented when the IP interfaces are set up on the switch.

An example is presented below:

VLAN Name	VID	Switch Ports
System (default)	1	5, 6, 7, 8, 21, 22, 23, 24
Engineering	2	9, 10, 11, 12
Marketing	3	13, 14, 15, 16
Finance	4	17, 18, 19, 20
Sales	5	1, 2, 3, 4
Backbone	6	25, 26

Table 6-1. VLAN Example – Assigned Ports

In this case, 6 IP interfaces (or 6 subnets) are required, so a CIDR notation of 10.32.0.0/11 (or a 11-bit) addressing scheme will work. This addressing scheme will give a subnet mask of 11111111.11100000.00000000.00000000 (binary) or 255.224.0.0 (decimal).

Using a 10.xxx.xxx.xxx IP address notation would give 6 network addresses:

VLAN Name	VID	Network Address
System (default)	1	10.32.0.0
Engineering	2	10.64.0.0
Marketing	3	10.96.0.0

Finance	4	10.128.0.0
Sales	5	10.160.0.0
Backbone	6	10.192.0.0

Table 6-2. VLAN Example – Assigned Network Addresses

The 6 IP interfaces, each with an IP address (or network) address (listed in the table above), and a subnet mask of 255.224.0.0 can be entered into the **Setup IP Interface** menu.

> ***Note:*** *IP interfaces consist of two parts – a subnet mask and an IP address.*
>
> ***Note****: Each IP interface listed above will give a maximum of 2,097,150 unique IP addresses per interface (assuming the 10.xxx.xxx.xxx notation).*

To setup IP Interfaces on the switch:

Highlight **Layer 3 IP Networking** from the **Main Menu** and press **Enter.**

Figure 6-34. Layer 3 - Main Menu

Highlight **Layer 3 IP Networking** from the **Main Menu** and press enter.

Figure 6-35. Layer 3 – IP Networking Menu

Highlight **Setup IP Interface** and press **enter**.

Figure 6-36. Layer 3 – IP Networking Menu

Toggle the **Action:<Add/Modify>** field to **Add/Modify.** Choose a name for the interface to be added and enter it in the **Interface Name:[ ]** field. The corresponding VLAN ID must also be entered in the **VID[ ]** field. Enter the interface's IP address and subnet mask in the corresponding fields. Toggle the **Active:<yes>** field to **yes,** highlight **APPLY** and press enter to make the IP interface effective. Use **Save Changes** from the **Main Menu** to enter the changes into NV-RAM.

> **Action:<Add/Modify>** This field can be toggled between Add/Modify and Delete using the space bar. This enables the addition/modification of a new or existing IP interface entry or the deletion of an existing entry.

Interface Name:[ ] allows the entry of a name for the IP interface. The default IP interface is named "System".

IP Address:[ ] is the IP address to be assigned to this subnet.

Subnet Mask:[ ] is the subnet mask to be applied to this subnet. It has the same form as an IP address.

Active:<Yes> is toggled between Yes and No. This entry makes determines whether the subnet will be active or not.

VID:[ ] allows the entry of the VLAN ID number for the VLAN the IP interface belongs to. The VLAN must have been previously created.

Press **APPLY** to make the additions/deletions effective for the current session. To make enter the IP Interfaces into NV-RAM, use **Save Changes** from the **Main Menu.**

Multicasting

Layer 2 Multicast Setup

IGMP Snooping Settings – by VLAN

To access the **Multicasting Menu**, highlight **Multicasting** from the **Main Menu** and press **ente**r.

Figure 6-37. Multicast Menu

To Enable or Disable IGMP Snooping for a VLAN, highlight **IGMP Snooping Settings**, and press **enter**.

Figure 6-38. IGMP Snooping Settings

To edit a VLAN's IGMP Snooping Settings:

Enter the VID of the VLAN for which the IGMP settings are to be edited.

The **State:< >** field can be toggled between **Enabled** and **Disabled** using the space bar. This enables or disables IGMP snooping for the selected VLAN.

The **Age-out Timer:[ ]** field allows the entry of an IGMP age-out timer value between 10 and 9,999 seconds. This timer determines how long a snooped multicast member's IP and MAC address remain in the IGMP address table. The default value is 260 seconds.

To globally enable or disable IGMP for the switch:

Highlight **Switch Settings** from the **Main Menu** and press **enter**.

Figure 6-39. Switch Settings Menu

Highlight **Layer 2 Switch Settings** and press **enter**.

Figure 6-39. Layer 2 Switch Settings

Highlight the **IGMP Snooping:<** **>** field and toggle between **Enabled** and **Disabled** using the space bar. This enables or disables IGMP Snooping globally for the switch.

Highlight **APPLY** and press **enter** to make the current changes active. Use **Save Changes** from the **Main Menu** to enter the current configuration settings into NV-RAM.

IEEE 802.1Q Multicast Forwarding

To edit the IEEE802.1 Multicast Forwarding settings, highlight **IEEE802.1Q Multicast Forwarding Settings** from the **Multicasting Menu** and press **enter**.

Figure 6-40. Setup IEEE 802.1Q Multicast Forwarding

The **Action:< >** field can be toggled between **Add/Modify** and **Delete** using the space bar. To add a new entry to the multicast forwarding table, select **Add/Modify** and enter the VID of the VLAN that will be receiving the multicast packets. Enter the MAC address of the multicast source, and then enter the member ports.

Each port can be an Egress, Forbidden, or a Non-member of the multicast group, on a per-VLAN basis.

To set a port's multicast group membership status, highlight the first field of **(E/F/-): [ ][ ][ ].** Each port's multicast group membership can be set individually by highlighting the port's entry using the arrow keys, and then toggling between E, F, or – using the space bar.

> **E** - (Egress Member) specifies the port as being a static member of the multicast group. Egress Member Ports are ports that will be transmitting traffic for the multicast group.

F - (Forbidden Non-Member) specifies the port as not being a member of the multicast group and that the port is forbidden from becoming a member of the multicast group dynamically.

- (Non-Member) specifies the port as not being a member of the multicast group, but the port can become a member of the multicast group dynamically.

Static Router Port

Note: *A router port allows UDP multicast and IGMP packets to be forwarded to a designated port on the switch regardless of VLAN configuration.*

A static router port is a port that has a multicast router attached to it. Generally, this router would have a connection to a WAN or to the Internet. Establishing a router port will allow multicast packets coming from the router to be propagated through the network, as well as allowing multicast messages coming from the network to be propagated to the router.

The purpose of a router port is to enable UDP multicast packets, and IGMP multicast group membership messages to reach a multicast router attached to the switch. Routers do not implement IGMP snooping or transmit/forward IGMP report packets. Thus, forwarding all IP UDP multicast packets to a static router port on the DES-3326 guarantees that all multicast routers – attached to the DES-3326 – can reach all multicast group members.

To setup a static router port, highlight **Static Router Port Settings** from the **Multicasting Menu** and press **enter**.

Figure 6-41. Static Router Port Settings

Note: *All IGMP Report packets will be forwarded to the router port.*

Note: *IGMP queries (from the router port) will be flooded to all ports.*

Note: *A router port will be dynamically configured when IGMP query packets, RIPv2 multicast, DVMRP multicast, PIM-DM multicast packets are detected flowing into a port.*

The **Action:< >** field can be toggled between **Add/Modify** and **Delete** using the space bar. To add a port to the static router port table, select **Add/Modify** and enter the VID of the VLAN the router port will belong to.

Highlight the first field of **Router Port (M/-):[ ][ ][ ]**. Each port can be set individually as a router port by highlighting the port's entry using the arrow keys, and then toggling between **M** and **–** using the space bar.

Highlight **APPLY** and press enter to make the changes current. Use **Save Changes** from the **Main Menu** to enter the changes into NV-RAM.

To delete an entry, select **Delete** and enter the VID of the VLAN for which the router port table entry is to be deleted. Highlight **APPLY** and press **enter**. The entry for the VLAN will be deleted. Use **Save Changes** from the **Main Menu** to enter the changes into NV-RAM.

Layer 3 Multicasting

With the switch in IP Routing mode, highlight **Multicasting** from the **Main Menu** and press **enter**.

Figure 6-42. Multicasting Menu

To setup the IEEE802.1q Multicast Forwarding table, highlight **IEEE802.1q Multicast Forwarding** and press **enter**.

Figure 6-43. IEEE 802.1Q Multicast Forwarding Settings

The **Action:<Add/Modify>** field can be toggled between **Add/Modify** and **Delete** using the space bar. To add a new entry to the multicast forwarding table, select **Add/Modify** and enter the VID of the VLAN that will be receiving the multicast packets. Enter the MAC address of the multicast source, and then enter the member ports.

Each port can be an Egress, Forbidden, or a Non-member of the multicast group, on a per-VLAN basis.

To set a port's multicast group membership status, highlight the first field of **(E/F/-): [ ][ ][ ].** Each port's multicast group membership can be set individually by highlighting the port's entry using the arrow keys, and then toggling between E, F, or – using the space bar.

> **E** - (Egress Member) specifies the port as being a static member of the multicast group. Egress Member Ports are

ports that will be transmitting traffic for the multicast group.

F - (Forbidden Non-Member) specifies the port as not being a member of the multicast group and that the port is forbidden from becoming a member of the multicast group dynamically.

- (Non-Member) specifies the port as not being a member of the multicast group, but the port can become a member of the multicast group dynamically.

To setup IP multicasting on the switch:

Highlight **IP Multicast Settings** from the **Multicasting Menu** and press **enter.**

Figure 6-44. Setup IP Multicast Menu

To configure the multicast interface:

Highlight **Multicast Interface Configuration** and press **enter**.

Figure 6-45. Multicast Interface Configuration

Enter the name of the IP interface that is to be configured for multicasting in the **Interface Name:[ ]** field. This must be a previously configured IP interface. *See* **Setting up IP Interfaces**, **Chapter 6** *of this manual for more information.*

The **IGMP: < >** field can be toggled between **Enabled** and **Disabled** using the space bar. This will enable or disable IGMP for the IP interface entered above.

The **Protocol: < >** field can be toggled between **Protocol Independent Multicasting – Dense Mode (PIMDM), Distance Vector Multicasting Routing Protocol (DVMRP),** and **INACT** (inactive). INACT is not a multicast routing protocol. It is used to make a given interface inactive for IP routing.

To configure the IGMP interface:

Highlight **IGMP Interface Configuration** from the **Setup IP Multicast** menu and press **enter**.

Figure 6-46. IGMP Interface Configuration

Enter the name of the interface in the **Interface-Name:[ ]** field. This interface must be previously defined.

The **Ver:< >** field can be toggled between **1** and **2**. This is the version of IGMP that the interface will use (IGMP version 1 or version 2).

The **Query:[ ]** field allows an entry between 1 and 65,535 seconds and defines the time between transmitting IGMP queries.

The **Max-Response:[ ]** field allows an entry between 1 and 25 and defines the maximum time allowed before sending a response report to a query measured in units of seconds.

The **Robustness Var.[ ]** field allows an entry between 2 and 255 and allows for the tuning of IGMP for the expected packet loss rate of a subnet. If a subnet is expected to lose a lot of packets, the Robustness Variable can be increased.

DVMRP

To configure DVMRP for an IP interface:

Highlight **DVMPR Interface Configuration** from the **Setup IP Multicast** menu and press **enter**.

Figure 6-47. DVMRP Interface Configuration

Enter the name of the IP interface for which DVMRP is to be configured in the **Interface Name:[ ]** field. This must be a previously defined IP interface. *See* **Setting up IP Interfaces**, **Chapter 6** *of this manual for more information.*

The Distance Vector Multicast Routing Protocol (DVMRP) is a hop-based method of building multicast delivery trees from multicast sources to all nodes of a network. Because the delivery trees are 'pruned' and 'shortest path', DVMRP is relatively efficient. Because multicast group membership information is forwarded by a distance-vector algorithm, propagation is slow. DVMRP is optimized for high delay (high latency) relatively low bandwidth

networks, and can be considered as a 'best-effort' multicasting protocol. See **Chapter 5, Distance-Vector Multicasting Routing Protocol** for more information.

DVMRP resembles the Routing Information Protocol (RIP), but is extended for multicast delivery. It relies upon RIP hop counts to calculate 'shortest paths' back to the source of a multicast message, but defines a 'route cost' to calculate which branches of a multicast delivery tree should be 'pruned' – once the delivery tree is established.

When a sender initiates a multicast, DVMRP initially assumes that all users on the network will want to receive the multicast message. When an adjacent router receives the message, it checks its unicast routing table to determine the interface that gives the shortest path (lowest cost) back to the source. If the multicast was received over the shortest path, then the adjacent router enters the information into its tables and forwards the message. If the message is not received on the shortest path back to the source, the message is dropped.

The **NMR Report Timer:[35]** This field allows an entry between **1** and **65,535** seconds and defines the time period for DVMRP will hold Neighbor Router reports before issuing poison route messages. *The default is* **35** *seconds.*

The **Route Cost:[1]** field allows an entry between 1 and 255 and defines the route cost for the IP interface. The DVMRP route cost is a relative number that represents the real cost of using this route in the construction of a multicast delivery tree. It is similar to, but not defined as, the hop count in RIP. *The default cost is* **1.**

Route cost is a relative number that is used by DVMRP to calculate which branches of a multicast delivery tree should be 'pruned'. The 'cost' is relative to other costs assigned to other DVMRP routes throughout the network.

> ***Note:*** *The higher the route cost, the lower the probability that the current route will be chosen to be an active branch*

of the multicast delivery tree (not 'pruned') – if there is an alternative route.

The **Probe Interval:[10]** field allows an entry between **1** and **65,535** seconds and defines the interval between 'probes'. DVMRP defines an extension to IGMP that allows routers to query other routers to determine if a multicast group is present on an given router subnetwork or not. This is referred to as a 'probe'. *The default is* **10.**

The **State:<Disabled>** field can be toggled between **Enabled** and **Disabled** and enables or disables DVMRP for the IP interface. *The default is* **Disabled.**

PIM-DM

To configure PIMDM for an IP interface:

Highlight **PIMDM Interface Configuration** from the **Setup IP Multicast** menu and press **enter**.

Figure 6-48. PIM-DM Interface Configuration

Enter the name of the IP interface for which PIM-DM is to be configured in the **Interface Name:[ ]** field. This must be a previously defined IP interface. *See* **Setting up IP Interfaces**, **Chapter 6** *of this manual for more information.*

The Protocol Independent Multicast – Dense Mode (PIM-DM) protocol should be used in networks with a low delay (low latency) and high bandwidth as PIM-DM is optimized to guarantee delivery of multicast packets, not to reduce overhead.

The **Hello Interval:[30]** field allows an entry of between **1** and **65,535** seconds and determines the interval between sending Hello packets to other routers on the network. The Hello messages are used by the router to determine if it is the root router on the delivery tree or not. If the router does not receive a Hello message within the Hello Interval, it will begin transmitting Hello messages to advertise its availability to become the root router. *The default is* **30** *seconds.*

The **Join/Prune Interval:[60]** field allows an entry of between **1** and **65,535** seconds and determines the interval between transmitting (flooding to all interfaces) multicast messages to downstream routers, and automatically 'pruning' a branch from the multicast delivery tree. This interval also determines the time interval the router uses to automatically remove prune information from a branch of a multicast delivery tree and begin to flood multicast messages to all branches of that delivery tree. These two actions are equivalent. *The default is* **60** *seconds.*

The PIM-DM multicast routing protocol is assumes that all downstream routers want to receive multicast messages and relies upon explicit prune messages from downstream routers to remove branches from the multicast delivery tree that do not contain multicast group members.

PIM-DM has no explicit 'join' messages. It relies upon periodic flooding of multicast messages to all interfaces and then either waiting for a timer to expire (the **Join/Prune Interval**) or for the downstream routers to transmit explicit 'prune' messages indicating that there are no multicast members on their respective branches. PIM-DM then removes these branches ('prunes' them) from the multicast delivery tree.

Because a member of a pruned branch of a multicast delivery tree may want to join a multicast delivery group (at some point in the future), the protocol periodically removes the 'prune' information from its database and floods multicast messages to all interfaces on that branch. The interval for removing 'prune' information is the **Join/Prune Interval.**

The **State:<Enabled>** field can be toggled between **Enabled** and **Disabled** using the space bar, and is used to enable or disable PIM-DM for the IP interface. *The default is* **Disabled**.

Static Router Port

> ***Note:*** *A router port allows UDP multicast and IGMP packets to be forwarded to a designated port regardless of VLAN configuration.*

A static router port is a port that has a multicast router attached to it. Generally, this router would have a connection to a WAN or to the Internet. Establishing a router port will allow multicast packets coming from the multicast router to be propagated through the network, as well as allowing multicast messages coming from the network to be propagated to the multicast router.

The purpose of a router port is to enable UDP multicast packets, and IGMP multicast group membership messages to reach a multicast router. Routers do not implement IGMP snooping or transmit/forward IGMP report packets. Thus, forwarding all IP UDP multicast packets to a static router port on the DES-3326

guarantees that a multicast router – attached to the DES-3326 – can reach all multicast group members.

To setup a static router port:

Highlight Setup Static Router Port from the Multicasting Menu and press enter.

Figure 6-49. Static Router Port Setup

All IGMP Report packets will be forwarded to the router port.

IGMP queries (from the router port) will be flooded to all ports.

All UDP multicast packets will be forwarded to the router port. Because routers do not send IGMP reports or implement IGMP snooping, a multi-port router connected to the router port of the Layer 3 switch would not be able to receive UDP data streams at all of its ports unless the UDP multicast packets were all forwarded to the router port.

A router port will be dynamically configured when IGMP query packets, RIPv2 multicast, DVMRP multicast, PIM-DM multicast packets are detected flowing into a port.

The **Action:< >** field can be toggled between **Add/Modify** and **Delete** using the space bar. To add a port to the static router port table, select **Add/Modify** and enter the VID of the VLAN the router port will belong to.

Highlight the first field of **Router Port (M/-):[ ][ ][ ]**. Each port can be set individually as a router port by highlighting the port's entry using the arrow keys, and then toggling between **M** and **–** using the space bar.

Highlight **APPLY** and press **enter** to make the changes current. Use **Save Changes** from the **Main Menu** to enter the changes into NV-RAM.

To delete an entry, select **Delete** and enter the VID of the VLAN for which the router port table entry is to be deleted. Highlight **APPLY** and press **enter**. The entry for the VLAN will be deleted. Use **Save Changes** from the **Main Menu** to enter the changes into NV-RAM.

Port Mirroring

To configure a port for port mirroring:

Highlight **Mirroring** from the **Main Menu** and press **enter**.

Figure 6-50. Mirroring Menu

To select the target port, highlight Target Port Selection and press enter.

Figure 6-51. Target Port Selection

The target port is the port where information will be duplicated and sent for capture and network analysis. This is the port where a network analyzer would be attached to capture packets duplicated from the source port.

To select the source port(s) for mirroring:

Highlight **Setup Port Mirroring** and press enter.

Figure 6-52. Setup Port Mirroring

The **Action:<** **>** field can be toggled between **Add/Modify** and Delete using the space bar. Entries can be added, modified or deleted based upon the port number entered in the Source Port [ ] field.

The **Direction:<** **>** field can be toggled between **Either**, **Ingress** and **Egress**. **Either** mirrors both received and transmitted packets at the given port. **Ingress** mirrors only received packets, while **Egress** mirrors only transmitted packets.

Up to 25 entries can be made to the port mirroring table, but it should be noted that a faster port (a 1000 Mbps Gigabit Ethernet

port, for example) should not be mirrored to a slower port (one of the 24 100 Mbps Fast Ethernet port), because many packets will be dropped.

Priority

To configure a forwarding priority for a given MAC address:

Highlight **Priority** from the main menu and press **Enter**.

Figure 6-53. Setup Priority – MAC Address

The **Action:< >** field can be toggled between **Add/Modify** and **Delete** using the space bar.

Enter the VID (VLAN ID) in the **VID:[ ]** field and the MAC address for which the priority queue is required in the **MAC Address:[ ]** field.

The **Priority Level:<** **>** field can be toggled between **Low, Med-L** (Medium Low)**, Med-H** (Medium High), and **High**, corresponding to the priority of packets sent to or transmitted from the MAC address entered above.

The **Source/Destination:<** **>** field can be toggled between **Src.** (Source), **Dst.** (Destination), and **Either**, corresponding to whether the MAC address entered above will be transmitting packets (a source), receiving packets (a destination) or both (either).

Filtering

Layer 2 Filtering

Layer 2 Only switch operation mode.

To enter a MAC address into the filtering table:

Highlight Filtering from the Main Menu and press enter.

Figure 6-54. Forwarding Menu – MAC Address

Highlight **MAC Address Forwarding** and press **enter**.

Figure 6-55. Static Unicast MAC Forwarding Setup

The **Action:< >** field can be toggled between **Add/Modify** and **Delete** using the space bar.

Enter the VLAN ID in the **VID: [ ]** field and the MAC address to be filtered in the **MAC Address:[ ]** field. This address must be a unicast MAC address.

The **Module:< >** field can be toggled between **Base Unit** (the 24 ports Fast Ethernet ports) and **Slot-1** (the two optional Gigabit ports). Enter the port number in the **Port: [ ]** field.

Highlight **APPLY** and press enter to make the changes current. Use **Save Changes** from the **Main Menu** to save the changes to NV-RAM.

Layer 3 (IP Routing) Filtering

The switch is in IP Routing switch operation mode.

With the switch configured to Layer 3 Operation mode, both MAC and IP addresses can be entered into the filtering table. To enter an address, highlight Filtering from the Main Menu and press enter.

Figure 6-56. Filtering Menu – Layer 3

To enter a MAC address into the filtering table:

Highlight MAC Address Filter and press enter.

Figure 6-57. Setup MAC Address Filter

The **Action:< >** field can be toggled between **Add/Modify** and **Delete** using the space bar. Enter the VLAN ID in the **VID:[ ]** field and the MAC address to be filtered in the **MAC Address:[ ]** field.

The **Source/Destination: < >** field can be toggled between **Src**. (source), **Dst**. (destination), and **Either**. The MAC address entered into the filtering table can be filtered as a source (packets will not be received from the MAC address), as a destination (packets will not be transmitted to the MAC address), or as either a source or destination (packets will not be received from or transmitted to the MAC address.

Highlight **APPLY** and press enter to make the changes current. Use **Save Changes** from the **Main Menu** to enter the changes into NV-RAM.

To enter an IP address into the filtering table:

Highlight IP Address Filter from the Filtering Menu and press enter.

Figure 6-58. IP Address Filtering Setup

The **Action:< >** field can be toggled between **Add/Modify** and **Delete** using the space bar. Enter the IP address to be filtered in the **IP Address:[ ]** field.

The **Source/Destination: < >** field can be toggled between **Src**. (source), **Dst**. (destination), and **Either**. The IP address entered into the filtering table can be filtered as a source (packets will not be received from the IP address), as a destination (packets will not be transmitted to the IP address), or as either a source or destination (packets will not be received from or transmitted to the IP address.

Highlight **APPLY** and press **enter** to make the changes current. Use **Save Changes** from the **Main Menu** to enter the changes into NV-RAM.

Forwarding

Layer 2 Forwarding

Layer 2 Only switch operation mode

To enter a MAC address into the switch's forwarding table:

Highlight **Forwarding** from the **Main Menu** and press **enter**.

Figure 6-59. Forwarding Menu – Layer 2

Highlight **MAC Address Forwarding** from the **Forwarding Menu** and press **enter**.

Figure 6-60. Static Unicast MAC Forwarding Setup – Layer 2

The **Action:< >** field can be toggled between **Add/Modify** and **Delete** using the space bar. Enter the VLAN ID in the **VID:[ ]** field and the MAC address to be statically entered in the forwarding table in the **MAC Address:[ ]** field.

The **Module:< >** field can be toggled between Base Unit (the 24 ports Fast Ethernet ports) and Slot-1 (the two optional Gigabit ports). Enter the port number in the **Port: [ ]** field.

Highlight **APPLY** and press enter to make the changes current. Use **Save Changes** from the Main Menu to enter the changes into NV-RAM.

IP Routing Forwarding

IP routing Switch Operation Mode

With the switch in Layer 3 Operation mode, entrees into the switch's forwarding table can be made using both MAC addresses and IP addresses. Static IP forwarding is accomplished by the entry of a Static IP Route.

Static Address Resolution Protocol (ARP) entrees can also be made from the Forwarding Menu.

MAC Address Forwarding

To enter a MAC address into the switch's forwarding table:

Highlight **Forwarding** from the **Main Menu** and press **enter**.

Figure 6-61. Forwarding Menu – Layer 3

Highlight MAC Address Forwarding and press enter.

Figure 6-62. Static Unicast MAC Forwarding – Layer 3

The **Action:< >** field can be toggled between Add/Modify and Delete using the space bar. Enter the VLAN ID in the **VID:[ ]** field and the MAC address to be statically entered in the forwarding table in the **MAC Address:[ ]** field.

The **Module:< >** field can be toggled between Base Unit (the 24 ports Fast Ethernet ports) and **Slot-1** (the two optional Gigabit ports). Enter the port number in the **Port: [ ]** field.

Highlight **APPLY** and press enter to make the changes current. Use **Save Changes** from the **Main Menu** to enter the changes into NV-RAM.

IP Static Routes

To enter a static IP route into the switch's forwarding table:

Highlight **Static/Default Routes** from the **Forwarding Menu** and press **enter**.

Figure 6-63. Static IP Route Setup

The **Action:< >** field can be toggled between **Add** and **Delete** using the space bar. Enter the VLAN ID in the **VID:[ ]** field and the MAC address to be statically entered in the forwarding table in the **MAC Address:[ ]** field.

Highlight **APPLY** and press **enter** to make the changes current. Use **Save Changes** from the **Main Menu** to enter the changes into NV-RAM.

Static ARP

To make a static ARP entry:

Highlight **Static ARP** from the **Forwarding** menu and press **enter**.

Figure 6-64. Static IP Route Setup

The **Action:< >** field can be toggled between **Add** and **Delete** using the space bar. Enter the IP interface name in the **Interface:[ ]** field and the corresponding IP address in the **IP Address:[ ]** field and subnet mask in the **Subnet Mask:[ ]** field. The IP address of the gateway (usually a router with a connection to a WAN or the Internet) is entered in the **Gateway IP:[ ]** field and a corresponding metric (a number representing the distance the gateway is from the IP interface in "hops" – or the number or routers between the IP interface and the gateway).

Highlight **APPLY** and press **enter** to make the changes current. Use **Save Changes** from the **Main Menu** to enter the changes into NV-RAM.

Spanning Tree

Switch Spanning Tree Settings

To globally configure STP on the switch:

Highlight Spanning Tree on the main menu and press Enter.

Figure 6-65. Configure Spanning Tree - Global

The Spanning Tree Protocol (STP) operates on two levels: on the switch level, the settings are globally implemented. On the port level, the settings are implemented on a per user-defined Group basis.

> ***Note:*** *The factory default setting should cover the majority of installations. However, it is advisable to keep the default settings as set at the factory; unless, it is absolutely necessary.*

The user-changeable parameters in the Switch are as follows:

- **Max. Age: [ ]** The Max. Age can be set from 6 to 40 seconds. At the end of the Max. Age, if a BPDU has still not been received from the Root Bridge, your Switch will start sending its own BPDU to all other Switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.

- **Hello Time:[ ]** The Hello Time can be set from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other Switches that it is indeed the Root Bridge. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge.

  Note: *The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.*

- **Forward Delay:[ ]** The Forward Delay can be from 4 to 30 seconds. This is the time any port on the Switch spends in the listening state while moving from the blocking state to the forwarding state.

- **Priority:[ ]** A Priority for the switch can be set from 0 to 65535. 0 is equal to the highest Priority. This number is used in the voting process between switches on the network to determine which switch will be the root switch. A low number indicates a high priority, and a high probability that this switch will be elected as the root switch.

  Note: *Observe the following formulas when setting the above parameters:*

  Max. Age ≤ 2 x (Forward Delay - 1 second)
  Max. Age ≥ 2 x (Hello Time + 1 second)

Port Group Spanning Tree Settings

In addition to setting Spanning Tree parameters for use on the switch level, the DES-3326 allows for the configuration of groups of ports, each port-group of which will have its own spanning tree, and will require some of its own configuration settings. An STP

Group will use the switch-level parameters entered above, with the addition of Port Priority and Port Cost.

An STP Group spanning tree works in the same way as the switch-level spanning tree, but the root bridge concept is replaced with a root port concept. A root port is a port of the group that is elected on the basis of port priority and port cost, to be the connection to the network for the group. Redundant links will be blocked, just as redundant links are blocked on the switch level.

The STP on the switch level blocks redundant links between switches (and similar network devices). The port level STP will block redundant links within an STP Group.

To define which ports will be members of an STP Group:

Highlight **Group Create/Delete** and press **enter.**

Figure 6-66. Port Group STP Configuration

Toggle the **Action:<Add/Modify>** field to **Add/Modify**. Choose a name for the group and enter it in the **Group Name:[ ]** field. The group name does not necessarily have to correspond to any

name that has been previously entered in the switch's configuration.

Figure 6-67. Port Group STP Settings

Toggle the **View Ports:<** **>** field to the range of ports to be configured. The Fast Ethernet ports displayed for configuration in groups of 12 and the two (optional) Gigabit Ethernet ports are displayed together.

The Port Group STP parameters that can be configured are:

- **Port Priority** A Port Priority can be from **0** to **255**. The lower the number, the greater the probability the port will be chosen as the Root Port.

- **Port Cost** A Port Cost can be set from **1** to **65535**. The lower the number, the greater the probability the port will be chosen to forward packets.

Link Aggregation

Link aggregation allows several ports to be grouped together and to act as a single link. This gives a bandwidth that is a multiple of a single link's bandwidth.

Link Aggregation is most commonly used to link a bandwidth intensive network device or devices – such as a server or server farm – to the backbone of a network.

The configuration of the lowest numbered port in the group becomes the configuration for all of the ports in the aggregation group. This port is called the base port of the group, and all configuration options – including the VLAN configuration – that can be applied to the base port are applied to the entire link aggregation group.

Load balancing is automatically applied to the links in the aggregation group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

> ***Note:*** *The Spanning Tree Protocol will treat a link aggregation group as a single link, on the switch level. On the port level, the STP will use the port parameters of the base port in the calculation of port cost and in determining the state of the link aggregation group. If two redundant link aggregation groups are configured on the switch, STP will block one entire group – in the same way STP will block a single port that has a redundant link.*

To configure a link aggregation group:

Highlight **Link Aggregation** on the **Main Menu** and press **enter.**

Figure 6-68. Link Aggregation Setup

Toggle the **Group ID:[1]** field to one of the six possible link aggregation groups configurable on the switch. Toggle the **Master Module:<Base Unit>** field to configure a group either on the Base Unit (the 24 Fast Ethernet ports) or on the Slot-1 (optional) module (the 2 Gigabit Ethernet ports).

> ***Note:*** *The two (optional) Gigabit ports can only be grouped together as a link aggregation group. They cannot be combined with Fast Ethernet ports in a link aggregation group.*

Specify the **Group Width:[2].** This is the number of ports, in sequential order from the base port, that will be included in the link aggregation group.

The **Method:<Disabled>** field can be toggled between Enabled and Disabled – and is used to turn a link aggregation group on or off. This is useful for diagnostics, to quickly isolate a bandwidth

intensive network device or to have an absolute backup aggregation group that is not under automatic control.

Highlight **Apply** and press **enter** to make the link aggregation group configuration active. Use **Save Changes** from the **Main Menu** to enter the configuration into NV-RAM.

Switch Utilities

Layer 2 Switch Utilities

To access the* Switch Utilities *menu:

Highlight **Utilities** from the **Main Menu** and press **enter.**

Figure 6-69. Switch Utilities Menu

Note: *Trivial File Transfer Protocol (TFTP) services allow the switch firmware to be upgraded by transferring a new firmware file from a TFTP server to the switch. A configuration file can also be loaded into the switch from a TFTP server, switch settings can be saved to the TFTP server, and a history log can be uploaded from the switch to the TFTP server.*

Updating Firmware

To update the switch's firmware:

Highlight ***Upgrade*** **Firmware from TFTP Server** and press **enter.**

Figure 6-70. Upgrade Firmare

Enter the IP address of the TFTP server in the **Server IP Address:[ ]** field.

> ***Note:*** *The TFTP server must be on the same IP subnet as the switch.*

Enter the path and the filename to the firmware file on the TFTP server. Note that in the above example, the firmware file is in the root directory of the C drive of the TFTP server.

> ***Note:*** *The TFTP server must be running TFTP server software to perform the file transfer. TFTP server software is a part of many network management software packages,, or can be obtained as a separate program.*

Highlight **APPLY** and press **enter** record the IP address of the TFTP server. Use **Save Changes** from the **Main Menu** to enter the address into NV-RAM

Highlight **START** and press **enter** to initiate the file transfer.

Downloading a Configuration File

To download a switch configuration file from a TFTP server:

Highlight **Use a Configuration File on TFTP Server** and press **enter.**

Figure 6-71. Download Configuration File

Enter the IP address of the TFTP server and specify the location of the switch configuration file on the TFTP server.

Highlight **APPLY** and press **enter** record the IP address of the TFTP server. Use **Save Changes** from the **Main Menu** to enter the address into NV-RAM

Highlight **START** and press **enter** to initiate the file transfer.

Uploading a Settings File

To upload a settings file to the TFTP server:

Highlight **Save Settings to TFTP Server** and press **enter.**

Figure 6-72. Upload Setting File

Enter the IP address of the TFTP server and the path and filename of the settings file on the TFTP server and press **APPLY.** Highlight **START** and press **enter** to initiate the file transfer.

Uploading a History Log File

To save a History Log on a TFTP server:

Highlight **Save History Log to TFTP Server** and press **enter.**

Figure 6-73. Upload Log File

Enter the IP address of the TFTP server and the path and filename for the history log on the TFTP server. Highlight **APPLY** and press **enter** to make the changes current. Highlight **START** and press **enter** to initiate the file transfer.

Testing Connectivity with Ping

To test the connection with another network device using Ping:

Highlight **Ping Test** and press **enter.**

Figure 6-74. Ping Connectivity Test

Enter the IP address of the network device to be pinged and the number of test packets to be sent (3 is usually enough). Highlight **START** and press **enter** to initiate the ping program.

Layer 3 Utilities

Layer 3 (IP Routing) switch operation mode adds BOOTP Relay and DNS Relay to the utilities available on the switch.

BOOTP/DHCP Relay

To setup BOOTP/DHCP Relay services on the switch:

Highlight **Utilities** on the **Main Menu** and press **enter**.

Figure 6-75. Switch Utilities Menu – Layer 3

Highlight **BOOTP/DHCP Relay** on the **Switch Utilities** menu and press **enter**.

Figure 6-76. BOOTP/DHCP Relay Setup – Layer 3

The **BOOTP/DHCP:<Disabled>** field can be toggled between **Disabled** and **Enabled** using the space bar. The **BOOTP HOPS Count Limit [4]** determines the number of router hops the relay will be allowed to cross. A hop count between 1 and 16 can be entered. The **BOOTP/DHCP Relay Time Threshold:[4]** Sets the minimum time (in seconds) that the switch will wait before forwarding a BOOTREQUEST packet. If the value in the seconds field of the packet is less than the relay time threshold, the packet will be dropped.

To enter the IP addresses of BOOTP Relay servers:

Highlight **BOOTP/DHCP Relay Interface Configuration** and press **Enter.**

Figure 6-77. BOOTP/DHCP Relay Setup – Layer 3

Toggle to **Add** and enter the subnet name for which BOOTP Relay will be active. The subnet's network IP address will be displayed in the **IP:** field. Enter the IP address of the BOOTP Relay server

(or servers, as the case may be), highlight **APPLY** and press **enter** to enter the information into the BOOTP Relay table. Use **Save Changes** from the **Main Menu** to enter the information into NV-RAM.

DNS Relay

To enter the IP addresses of DNS Relay servers:

Highlight **DNS Relay** on the **Switch Utilities** menu and press **enter**.

Figure 6-78. DNS Relay Setup – Layer 3

The **DNS Relay Status <Disabled>** can be toggled between **Disabled** and **Enabled** using the space bar. Toggle the field to **Enabled,** enter the IP address of the Primary name server and a secondary server, if so desired.

The **DNS Relay Cache Status:<Disabled>** can be toggled between **Disabled** and **Enabled.** This determines if a DNS cache will be enabled on the switch.

The **DNS Relay Static Table Lookup Status:<Disabled>** can be toggled between **Disabled** and **Enabled.** This determines if the static DNS table (entered under **Static Table Setting,** below) will be used or not.

To make a static DNS table entry:

Highlight Static Table Setting on the DNS Relay menu and press Enter.

Figure 6-79. DNS Relay Setup – Layer 3

The **Action:<Add/Edit>** field can be toggled between **Add/Edit** and **Delete.** Enter the Domain name and its corresponding IP address. Highlight **APPLY** and press **enter** to make the change current. Use **Save Changes** to enter the table into NV-RAM.

Network Monitoring

The DES-3326 provides extensive network monitoring capabilities.

Layer 2 Network Monitoring

To display the network data compiled by the switch:

Highlight **Network Monitoring** on the **Main Menu** and press **enter**.

Figure 6-80. Network Monitoring Menu

Port Utilization

To view the port utilization:

Highlight **Port Utilization** on the **Network Monitoring** menu and press **enter**.

Figure 6-81. Port Utilization Table

The **Port Utilization** screen shows the number of packets transmitted and received per second and calculates the percentage of the total available bandwidth being used on the port (displayed under **%Util.**).

Port Error Statistics

To view the error statistics for a port:

Highlight **Port Error Packets** on the **Network Monitoring** menu and press **enter**.

Figure 6-82. Port Error Statistics Table

The **Module:<Base Unit>** field can be toggled between **Base Unit** and **Slot-1** to select which group of ports will be displayed.

Enter the port number of the port to be viewed. The **Interval:<2 sec>** field can be toggled from 2 seconds to 1 minute, or suspend. This sets the interval at which the error statistics are updated.

Port Packet Analysis Table

To view an analysis of the size of packets received or transmitted by a port:

Highlight **Port Packet Analysis** on the **Network Monitoring** menu and press **enter**.

```
Packet Analysis                                                    Layer 3 Switch
Module:<Base Unit>   Port:[1 ]        [LIVE COUNTS]        Interval:< 2 sec >

                 Frames     Frames/sec                    Total      Total/sec

64               1680       12            RX Bytes  342686     1234
65-127           886        2             RX Frames 3119       15
128-255          509        1
256-511          72         0             TX Bytes  0          0
512-1023         2          0             TX Frames 0          0
1024-1518        23         0

Unicast RX       5          0
Multicast RX     579        0
Broadcast RX     2588       15


Function:Clear Counter.
Message:
CTRL+T = Root screen          Esc=Prev. screen                CTRL+R = Refresh
```

Figure 6-83. Port Packet Size and Mode Analysis Table

In addition to the size of packets received or transmitted by the selected port, statistics on the number of unicast, multicast, and broadcast packets are displayed.

MAC Address Forwarding Table

To view the MAC address forwarding table:

Highlight **Browse MAC Address** on the **Network Monitoring** menu and press **enter**.

Figure 6-84. View the MAC Forwarding Table

The **Browse By:<ALL >** field can be toggled between **ALL, MAC Address, Port,** and **VLAN.** This sets a filter to determine which MAC addresses from the forwarding table are displayed. **ALL** specifies no filter.

To search for a particular MAC address:

Toggle the **Browse By:<ALL >** field to **MAC Address.** A **MAC Address:[000000000000]** field will appear. Enter the MAC address in the field and press **enter.**

GVRP Status Table

To view the GVRP status table:

Highlight **GVRP Status** from the **Network Monitoring** menu and press **enter.**

Figure 6-85. GVRP Status Table

GMRP Status Table

To view the GMRP status table:

Highlight **GMRP Status** from the **Network Monitoring** table and press **enter.**

Figure 6-86. GMRP Status Table

IGMP Snooping Table

To view the IGMP snooping table:

Highlight **IGMP Status** from the **Network Monitoring** menu and press **enter.**

Figure 6-87. IGMP Snooping Status Table

Switch History Log

To view the switch history log:

Highlight **Switch History** from the **Network Monitoring** menu and press **enter.**

Figure 6-88. Switch History Table

Layer 3 Network Monitoring

When the switch is in Layer 3 (IP Routing) mode, several items are added to the **Network Monitoring** menu.

The following items are added to the* Network Monitoring *menu when the switch is in Layer 3 (IP Routing) mode:

- **Browse IP Address**
- **Routing Table**
- **ARP Table**
- **IP Multicast Forwarding Table**
- **IGMP Group Table**
- **DVMRP Routing Table**

Figure 6-89. Network Monitoring Menu – Layer 3

IP Address Forwarding Table

To view the IP address forwarding table:

Highlight **Browse IP Address** from the **Network Monitoring** menu and press **enter.**

Figure 6-90. IP Forwarding Table – Layer 3

To display a particular IP address, enter the IP address in the **Jump to IP Address:[0.0.0.0]** field, highlight **GO,** and press **enter.**

IP Routing Table

To view the contents of the routing table:

Highlight **Router Table** on the **Network Monitoring** menu and press **enter**.

Figure 6-91. View the IP Routing Table

To display a particular Destination IP address, enter the IP address in the **Jump to Destination Address:[0.0.0.0]** field, the gateway address in the **Gateway:[0.0.0.0]** field, and the subnet mask in the **Mask:[0.0.0.0]** field, highlight **GO,** and press **enter.**

ARP Table

To view the ARP table:

Highlight **ARP Table** on the **Network Monitoring** menu and press **enter**.

Figure 6-92. View the ARP Table

To display a particular IP interface or an IP address, enter either the IP interface name in the **Jump to Interface Name:[ ]** field or enter the IP address in the **IP Address:[0.0.0.0]** field, highlight **GO,** and press **enter.**

IP Multicast Forwarding Table

To view the IP multicast forwarding table:

Highlight **IP Multicast Forwarding Table** from the **Network Monitoring** menu and press **enter**.

Figure 6-93. View the IP Multicast Forwarding Table

To display a particular multicast group, enter the IP address in the **Jump to Multicast Group:[0.0.0.0]** field, enter the source IP address in the **Source IP:[0.0.0.0]** field, and the source subnet mask in the **Source Mask:[0.0.0.0]** field, highlight **GO,** and press **enter.**

DVMRP Routing Table

To view the DVMRP routing table:

Highlight **Browse DVMRP Routing Table** from the **Network Monitoring** menu and press enter.

Figure 6-94. View the DVMRP Routing Table

To display a particular source IP address, enter either the IP address in the **Jump to IP Address:[0.0.0.0]** field, or the source subnet mask in the **Source Mask:[0.0.0.0]** field, highlight **GO,** and press **enter.**

This sets a filter to determine which IP addresses from the table are displayed.

Reboot

The DES-3326 has several reboot options.

To reboot the switch from the console:

Highlight **Reboot** from the **Main Menu** and press **enter.**

Figure 6-95. System Reboot Menu

The reboot options are as follows:

Reboot simply restarts the switch. Any configuration settings not saved using **Save Changes** from the **Main Menu** will be lost. The switch's configuration will be restored to the last configuration saved in NV-RAM.

Save Configuration & Reboot saves the configuration to NV-RAM (identical to using **Save Changes**) and then restarts the switch.

Reboot & Load Factory Default Configuration restarts the switch using the default factory configuration. All configuration data will be lost. This is identical to using **Factory Reset** and then **Reboot.**

Reboot & Load Factory Default Configuration Except IP Address restarts the switch using the default factory configuration, except the user configured IP address will be retained. All other configuration data will be lost.

A confirmation screen will appear:

Figure 6-96. System Reboot Confirmation

To reboot the switch, in the mode entered above, highlight **Yes** and press **enter.**

7

WEB-BASED NETWORK MANAGEMENT

Introduction

The DES-3226 offers an embedded Web-based (HTML) interface allowing users to manage the switch from anywhere on the network through a standard browser such as Netscape Navigator/Communicator or Microsoft Internet Explorer. The Web browser acts as a universal access tool and can communicate directly with the Switch using the HTTP protocol.

The Web-based management module and the Console program (and Telnet) are different ways to access the same internal switching software and configure it. Thus, all settings encountered in web-based management are the same as those found in the console program.

> ***Note:*** This Web-based Management Module does not accept Chinese language input (or other languages requiring 2 bytes per character).

Where there is a difference in the setup of the switch between its two operational modes (**Layer 2 Only** and **IP Routing**), the

sections are divided to correspond with the switch operating mode that is applicable.

> ***Note:*** **IP Routing** *mode switch configuration settings that are saved NV-RAM using* **Save Changes** *from the* **Main Menu** *are retained in the switch's memory when the operational mode is changed.* **IP Routing** *mode settings are simply inactive when the switch is in* **Layer 2 Only** *mode.*

Before You Start

The DES-3326 Layer 3 Switch supports a wide array of functions and gives great flexibility and increased network performance by eliminating the routing bottleneck between the WAN or Internet and the Intranet. Its function in a network can be thought of as a new generation of router that performs routing functions in hardware, rather than software. It is a router that also has up to 24+2 independent Ethernet collision domains – each of which can be assigned an IP subnet.

This flexibility and rich feature set requires a bit of thought to arrive at a deployment strategy that will maximize the potential of the DES-3326 Layer 3 switch.

General Deployment Strategy

1. Determine how the network would be best segmented. This is probably done using VLANs in an existing layer 2 switched network.

2. Develop an IP addressing scheme. This involves allocating a block of IP addresses to each network segment. Each network subnet is then assigned a network address and a

subnet mask. *See Chapter 5,* **Switch Management Concepts** *section titled* **IP Addressing and Subnetting** *for more information.*

3. Determine which network resources must be shared by the subnets. Shared resources may be connected directly to the Layer 3 switch, if need be. Static routes to each of the shared resources should be determined.

4. Determine how each subnet will communicate with the WAN or Internet. Again, static routes should be determined and default gateways identified.

5. Develop a security scheme. Some subnets on the network need more security or should be isolated from the other subnets. IP or MAC filtering can be used. Also, one or more VLANs on the Layer 3 switch can be configured without an IP subnet – in which case, these VLANs will function as a layer 2 VLAN and would require an external router to connect to the rest of the network.

6. Develop a policy scheme. Some subnets will have a greater need for multicasting bandwidth, for example. A policy is a mechanism to alter the normal packet forwarding in a network device, and can be used to intelligently allocate bandwidth to time-critical applications such as the integration of voice, video, and data on the network.

7. Develop a redundancy scheme. Planning redundant links and routes to network critical resources can save valuable time in case of a link or device failure. The DES-3326 Spanning Tree function can be used to block the redundant link until it is needed.

VLAN Layout

VLANs on the DES-3326 have rather more functions than on a traditional layer 2 switch, and must therefore be laid-out and configured with a bit more care. Layer 3 VLANs (VLANs with an IP interface assigned to them) could be thought of as network links – not just as a collection of associated end users. Further, Layer 3 VLANs are assigned an IP network address and subnet mask to enable IP routing between them.

Layer 3 VLANs must be configured on the switch before they can be assigned IP subnets. Further, the static VLAN configuration is specified on a per port basis. On the DES-3326, a VLAN can consist of end-nodes – just like a traditional layer 2 switch, but a VLAN can also consist of one or more layer 2 switches – each of which is connected to multiple end-nodes or network resources.

So, a Layer 3 VLAN, consisting of 4 ports, could be connected to 4 layer 2 switches. If these layer 2 switches each have 24 ports, then the Layer 3 VLAN would contain 4 x 24 = 96 end nodes. Assigning an IP subnet to the Layer 3 VLAN would allow wire-speed IP routing from the WAN to each end node and between end nodes.

So, the IP subnets for a network must be determined first, and the VLANs configured on the switch to accommodate the IP subnets. Finally, the IP subnets can be assigned to the VLANs.

Assigning IP Network Addresses and Subnet Masks to VLANs

The DES-3326 allows the assignment of IP subnets to individual VLANs. Any VLAN configured on the switch that is not assigned an IP subnet, will behave as a layer 2 VLAN and will not be capable of IP routing – even if the switch is in IP Routing mode.

Developing an IP addressing scheme is a complex subject, but it is sufficient here to mention that the total number of anticipated end nodes – for each Layer 3 VLAN – must be accommodated with an unique IP address. It should be noted that the switch regards a VLAN with an IP network address and corresponding subnet mask assigned as an IP interface in IP Routing mode.

Defining Static Routes

Routes between the IP interfaces and a default gateway or other router with a WAN connection should be determined beforehand and entered into the static/default routing table on the DES-3326.

Getting Started

The first step in getting started in using web-based management for your Switch is to secure a browser. A Web browser is a program which allows a person to read hypertext, for example, Netscape Navigator or Microsoft Internet Explorer. Follow the installation instructions for the browser.

The second and last step is to configure the IP interface of the Switch. This can be done manually through a console (see the Configure IP Address section in "Using The Console Interface" chapter 6).

Management

To begin managing your Switch simply run the browser you have installed on your computer and point it to the IP address you have defined for the device. The URL in the address bar should read

something like: http://123.123.123.123, where the numbers 123 represent the IP address of the switch.

> ***Note:*** *The Factory default IP address for the switch is 10.90.90.90.*

In the page that opens, click on the **Login to DES-3326 Manager** button:

Figure 7-1. Login Button

This opens the main page in the management module.

The switch management features available in the web-based are explained below.

Configuring the Switch

User Accounts Management

From the **Main Menu**, highlight S**etup User Accounts** and press Enter, then the **User Account Management** menu appears.

Figure 7-2. User Accounts Control Table

Click **New** to add a user.

Figure 7-3. User Accounts Control Table - Edit

1. Enter the new user name, assign an initial password, and then confirm the new password. Determine whether the new user should have **Root, User+**, or **User** privileges.

2. Click on **APPLY** to make the user addition effective.

3. A listing of all user accounts and access levels is shown on the user accounts control table. This list is updated when Apply is executed.

4. Please remember that Apply makes changes to the switch configuration for the ***current session only.*** ***A***ll changes (including User additions or updates) must be entered into non-volatile ram using the **Save Changes** command on the **Main Menu** - if you want these changes to be permanent.

Root, User+ and Normal User Privileges

There are three levels of user privileges: *Root* and *User+*, and *User*. Some menu selections available to users with *Root* privileges may not be available to those with *User+* and *User* privileges.

The following table summarizes the *Root*, *User+* and *User* privileges:

Switch Configuration Management	Privilege		
	Root	User+	User
Configuration	Yes	Read Only	Read Only
Network Monitoring	Yes	Read Only	Read Only
Community Strings and Trap Stations	Yes	Read Only	Read Only
Update Firmware and Configuration Files	Yes	No	No
System Utilities	Yes	Ping Only	Ping Only
Factory Reset	Yes	No	No
Reboot Switch	Yes	Yes	No
User Accounts Management			
Add/Update/Delete User Accounts	Yes	No	No
View User Accounts	Yes	Yes	Yes

Table 7-1. Root, User+, and User Privileges

After establishing a User Account with **Root**-level privileges, highlight **Save Changes** and press **Enter** (see below). The switch will save any changes to its non-volatile ram and reboot. You can logon again and are now ready to continue configuring the Switch.

Saving Changes

The DES-3326 has two levels of memory; normal RAM and non-volatile or NV-RAM. Configuration changes are made effective by highlighting `Apply` and pressing **Enter.** When this is done, the settings will be immediately applied to the switching software in RAM, and will immediately take effect.

Some settings, though, require you to restart the switch before they will take effect. Restarting the switch erases all settings in

RAM and reloads the stored settings from the NV-RAM. Thus, it is necessary to save all setting changes to NV-RAM before rebooting the switch.

To retain any configuration changes permanently, highlight Save Changes from the main menu. The following screen will appear to verify that your new settings have been saved to NV-RAM:

Figure 7-5. Save Changes Screen

Once the switch configuration settings have been saved to NV-RAM, they become the default settings for the switch. These settings will be used every time the switch is rebooted.

Factory Reset

The following menu is used to restart the switch using only the configuration that was supplied by the factory. A factory reset returns all configuration options to their default values and restores the switch's configuration to the factory settings.

All user-entered configuration information will be lost.

Figure 7-6. Factory Reset Screen

Click **Yes** if you want the switch to retain its current IP address. Click **No** to reset the switch's IP address to the factory default, 10.90.90.90.

Click the **Reset to Factory Default** button to restart the switch.

USING WEB-BASED MANAGEMENT

Setting Up Web Management

Before running Web-based management, some basic configuration of the switch may need to be performed. The following at a minimum must be configured or known for the switch to be managed:

- IP Address
- Administrator password

In addition, several other parameters may need to be configured or known to properly communicate with the switch or allow full management capability. These include:

- Default Gateway
- Trap Destination and Community Name

Configuration of these items may be made from the User Interface, which is accessible via either the serial console or Telnet. Refer to the User Guide that came with your system for more information subsection describe the required configuration.

Setting an IP Address

The IP address for the switch must be set before it can be managed with the web-based manager. The switch IP address may be automatically set using BootP protocol, in which case the actual address assigned to the switch must be known.

The IP address may alternatively be set manually as follows:

1. Starting at the Main Menu of the User Interface, select Configuration / IP Address.
2. Select IP Address from the menu and enter the IP address.
3. Select Subnet Mask from the menu and enter the appropriate mask.
4. Click APPLY to make the change effective. Use Save Changes to enter the IP address into NV-RAM.

Setting a Default Gateway

The default gateway parameter defines the IP address of a router or other network device to which IP packets are to be sent if destined for a subnet outside of that in which the switch is operating. This parameter must be set if you are attempting to manage the switch from a remote network or across the Internet.

1. Starting at the Main Menu of the User Interface, select Configuration / IP Address.

2. Select Gateway IP from the menu and enter the router IP address. Press APPLY.

Setting the Administrator Password

Management access to the switch is restricted based on the administrator password. Administrators have read/write access for parameters governing the SNMP agent. You should therefore assign a password to the default administrator as soon as possible, and store it in a safe place.

Setting Trap Destinations

If you wish to record SNMP traps, or events, generated by the switch, you must configure a destination for the IP Trap Managers. A trap destination is the IP address of the computer system on which the web-based manager is being run.

1. Starting at the Main Menu of the User Interface, select Management / IP Trap Managers.

2. Select an entry for an IP Trap Manager from the menu, then enter the IP address and community name.

3. Move to the Status field, and use the Space bar to select ENABLED.

4. Click APPLY to make the changes effective. Use Save Changes to enter the configuration into NV-RAM.

Saving Configuration Changes

Clicking the **APPLY** button makes any configuration change active, but only for the current session. If the switch is restarted (rebooted) without entering the configuration changes into the non-volatile RAM (flash RAM), the configuration changes will be lost.

To enter configuration changes into the switch's non-volatile RAM, select **Save Changes** from the main screen. Click on the **Save Configuration** button to enter the current configuration into NV-RAM. The configuration will then be loaded into the switch's memory when it is restarted.

Figure 7-7. Save Changes Screen

Starting and Stopping the Web-based Manager

Do the following to use the web-based manager:

1. Start a Java-enabled Web browser from any machine with network access to the switch. (Preferred browsers include Internet Explorer

4.0 or above, or Netscape Navigator 4.0 or above.)

2. Enter the IP address for the switch you want to manage in the URL field of the browser.

3. The screen below will appear, prompting you to enter the user name and password for management access.

Figure 7-8. Password Screen

Use the User Name, and Password previously entered in the Setting Up Web Management section. This will allow read/write access to the switch.

The full application will now launch. A four-frame page will display with the product graphic located in the upper right hand frame.

4. To stop the web-based manager, close the Web browser application.

Web-based Manager's User Interface

The user interface provides access to various switch configuration and management screens, allows you to view performance statistics, and permits you to graphically monitor system status.

Areas of the User Interface

Figure 2-1 shows the user interface. The user interface is divided into 3 distinct areas as described in Table 2-1.

Figure 7-9. Main Web-Manager Screen

Area	Function

1	Presents a graphical near real-time image of the front panel of the switch. This area displays the switch's ports and expansion modules, showing port activity, duplex mode, or flow control, depending on the specified mode. Various areas of the graphic can be selected for performing management functions, including the ports, expansion modules, management module, or the case.
2	Allows the selection of commands.
3	Presents switch information based on your selection and the entry of configuration data.

Function	Description
System	Provides basic system description, including contact information.
Switch	Shows hardware/firmware version numbers, power status, and expansion modules in use.
IP	Includes boot state, IP address, and Telnet session count.
SNMP	Configures communities and trap managers; and activates traps.
Security	Sets password for system access.
Upgrade	Downloads new version of firmware to update your system.
Configure	Allows you to save/restore the switch configuration to a file on a server.
Address Table	Provides full listing of unicast address, sorted by address or VLAN.
STP	Enables Spanning Tree Protocol; also sets parameters for switch priority, hello time, maximum message age, and forward delay; as well as port priority and path cost.
Priority	Configures default port priorities and queue assignments.

Management VID	Allows you to restrict management access to the switch to one VLAN.
VLAN	Configures VLAN group members, automatic registration with GVRP, and other port-specific VLAN settings.
IGMP	Configures IGMP multicast filtering.
Port	Enables any port, sets communication mode to auto-negotiation, full-duplex or half-duplex, and enables/disables flow control.
Mirror	Sets the source and target ports for mirroring.
Trunk	Specifies ports to group into aggregate trunks.
Statistics	Displays statistics on network traffic passing through the selected port.

CONFIGURING AND MONITORING THE SWITCH

This section, arranged by topic, describes how to perform common monitoring and configuration tasks on the switch using the web-based manager.

Screen Hierarchy

The contents of this chapter are arranged following the structure shown below. Entries in **Bold** typeface are available only when the switch is in IP routing mode.

Initial Screen	Sub-screens
System	*No Sub-Menus*
Switch	Switch Operation Mode Layer 2 Switch Settings **Layer 3 IP Routing Protocol Settings** **Setup IP Interfaces** **Setup RIP**
IP	*No Sub-menus*
Security	User Accounts Table User Accounts Table – Add
Management	Management Station IP Settings Community Strings Trap Receivers Serial Port Settings

Port	*No Sub-menus*
Spanning Tree	STP Switch Settings Configure STP Groups STP Port Settings
Forwarding	MAC Address Forwarding Static/Default Routes Static ARP
Filtering	MAC Filtering IP Address Filtering
Priority	*No Sub-menus*
Mirroring	Target Port Selection Port Mirroring Settings
Multicasting	IEEE 802.1Q Multicast Forwarding Multicast Interface Configuration IGMP Settings **DVMRP Settings** **PIMDM Settings** **Static Router Port Settings**
VLANs	802.1Q Static VLANs Port VLAN ID (PVID) Port Ingress Filter Port GVRP Settings Port GMRP Settings **Static Router Port Settings**
Trunk	*No Sub-menus*
Statistics	Port Packet Analysis Port Error Port Utilization

Address Table	Browse MAC Address Sequentially **Browse IP Address Sequentially** **Routing Table** **ARP Table**
Applications	Switch History **Browse Router Port** **Browse IP Address Sequentially** **Routing Table** **ARP Table**
Utilities	Update Firmware from Server Use Configuration File on Server Save Settings to Server **Save History Log to Server** **BOOTP/DHCP Relay** **DNS Relay**
Save	*No Sub-menus*
Reset	Restart System Factory Reset

System Information

Use the System Information screen to display descriptive information about the switch, or for quick system identification as shown in the following figure and table.

Figure 7-10. Switch Information Screen

Parameter	Description
System Name[2]	Name assigned to the switch system.
Hardware Version	Hardware version of the main board.
Firmware Version	System firmware version in ROM.
Internal Power Status	Power status for the switch.

Redundant Power Status	Redundant power status for the switch.
IP Address[2]	IP address of the agent you are managing. The agent module supports SNMP over UDP/IP transport protocol. In this environment, all systems on the Internet, such as network interconnection devices and any PC accessing the agent module (or running management software) must have an IP address. Valid IP addresses consist of four numbers, of 0 to 255, separated by periods. Anything outside of this format will not be accepted by the configuration program.
Location[1]	Specifies the area or location where the system resides.
Contact[1]	Contact person for the system.

[1]Maximum string length is 99, but the screen only displays 45 characters. You can use the arrow keys to browse the whole string.

[2]The default value is 10.90.90.90

IP Configuration

Use the IP Configuration screen to set the boot-up option, or to manually configure the IP address for the agent module. The screen shown below is described below in the following table.

Figure 7-11. IP Address Screen

Current Settings

Parameter	Default	Description
Get IP From	Manual	Specifies the method to assign the switch an IP address.

IP Address	10.90.90.90	Displays the IP address currently assigned to the switch.
Subnet Mask	255.0.0.0	Displays the Subnet Mask currently assigned to the switch.
Default Gateway	0.0.0.0	Displays the Default Gateway currently assigned to the switch. Note that the gateway must be defined if the management station is located on a different IP segment than the switch.
Management VID	1	Displays the VID of the VLAN that is currently allowed to access the management module on the switch.

New Settings (at Switch Restart)

Parameter	Description
Get IP From	Specifies the method used to assign the switch an IP address. The options are **Manual, DCHP,** and **BOOTP.**
IP Address	Allows the manual input of an IP address for the switch.
Subnet Mask	Allows the input of a Subnet Mask.
Default Gateway	Allows the input of the IP address of a Default Gateway used to pass trap

	messages from the switch's agent to the management station. Note that the gateway must be defined if the management station is located on a different IP segment than the switch.
Management VID	Allows the input of a VLAN VID to restrict access to the management module on the switch to a single VLAN.

Management

Use the Management Menus to configure the IP addresses of up to 3 Management stations, to configure SNMP Community strings, the IP addresses of Trap receivers, and to configure the Serial Port settings.

Management Station IP Settings

You can specify the IP addresses of up to 3 management stations that will be allowed to access the management agent of the switch. If you enter IP addresses in this menu, then only management stations with those IP addresses will be allowed to access the management agent of the switch. All other IP addresses will be blocked.

Figure 7-12. Management Station IP Settings Screen

Parameter	Description
IP Address	The IP address of the management station that you want to give access to the switch's management agent. Entering an IP address in this menu will block access by an IP address not listed in this table.

SNMP Configuration (Community Strings)

Use the Management Configuration screen to display and modify parameters for the Simple Network Management Protocol (SNMP). The switch includes an on-board SNMP agent which monitors the status of its hardware, as well as the traffic passing through its ports. A computer attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the on-board agent are controlled by community strings. To communicate with the switch, the NMS must first submit a valid community string for authentication. The options for configuring community strings and related trap functions are described in the following figures and table.

SNMP Community Strings

The following figure and table describe how to configure the community strings authorized for management access. Up to 4 community names may be entered.

Figure 7-13. Community Strings Screen

Parameter	Description
Community String	A string of up to 20 characters used for authentication of users wanting access to the switch's SNMP agent.
Access Right	Specifies the level of access for an authorized user. The levels can be Read-Only, or Read-Write.
Status	Specifies whether the current string is Valid or Invalid. This is used to temporarily limit access to the switch's SNMP agent.

Trap Receivers

The following figure and table describe how to specify management stations that will receive authentication failure messages or other trap messages from the switch. Up to 4 trap managers may be entered.

Figure 7-13. Trap Receivers Screen

Parameter	Description
Trap Receiving Station	The IP address of the management station that will receive traps generated by the switch.
Community String	A string of up to 20 characters used for authentication of users wanting to receive traps from the switch's SNMP agent.
Status	Specifies whether the current string is Enabled or Disabled. This is used to temporarily limit the receipt of traps generated by the switch.

Serial Port Settings

The following figure and table describe the configuration of the switch's serial port (sometimes referred to as a 'console port'). Use Select Protocol to switch between the Console and SLIP (Serial Line IP) protocols.

Figure 7-14. Serial Port Settings

Console Settings

Parameter	Description
Baud Rate	Specifies the rate data will be exchanged over the serial link. The default value is 9600 baud.
Data Bits	Specifies the number of bits that will carry data over the serial link. The default value is 8 bits.
Stop Bits	Specifies the number of bits that indicate when a serial word ends. The default value is 1 bit.

Auto-Logout	Specifies length of time a management session can be idle. When this time has expired, the switch's management agent will disconnect the user. The default value is 10 minutes.

Slip Settings

Parameter	Description
Baud Rate	Specifies the rate data will be exchanged over the serial link. The default value is 9600 baud.
Interface Name	The name of the IP interface, previously defined on the switch, that will communicate with the remote management station.
Local IP Address	The IP address that corresponds to the IP interface name above.
Remote IP Address	The IP address of the remote management station that will communicate with the switch using SLIP.
MTU	Maximum Transfer Unit, specifies the maximum number of bytes (octets) that can be transferred in a single packet. The options are 1006 and 1500.

Switch

The switch can operate in one of two modes:

3. **Layer 2 Only with IEEE 802.1Q VLAN support**: the switching process is based upon the source and destination MAC addresses only. 802.1Q VLANs are supported and the switch is considered as a VLAN-tag aware device.

4. **IP Routing with IEEE 802.1Q VLAN support**: the switching process is based upon the IP source and destination addresses, if present. If the IP addresses are not present, the switching process is based upon the MAC addresses (as in Layer 2 above). 802.1Q VLANs are supported and the switch is considered as a VLAN-tag aware device.

The switch must be rebooted when changing the operation mode before the new operation mode can take effect.

Switch Operation Mode

The field **Restart Mode** can be set using the drop down menu to one of the two switch operation modes: **Layer 2 Only, Support IEEE 802.1Q VLANs** and **IP Routing, Support IEEE 802.1Q VLANs**.

To make a change in the operation mode of the switch effective, click the **APPLY** button**.** The switch must be restarted to change the operating mode.

Figure 7-15. Switch Operation Mode Screen

Parameter	Description
Current Mode	Displays the switch's current operating mode.
Restart Mode	Allows the selection of the operating mode of the switch after a switch restart. The options are Layer 2, Support IEEE 802.1Q VLANs, and IP Routing, Support IEEE 802.1Q VLANs.

Layer 2 Switch Settings

Note: *Layer 2 Switch functions and settings are also available when the switch is configured to operate in the IP Routing (Layer 3) mode.*

Note: *A very long MAC Address Aging Time can result with the out-of-date Dynamic Entries that may cause incorrect packet filtering/forwarding decisions. A very short aging time may cause entries to be aged out to soon, resulting in a high percentage of received packets whose source addresses cannot be found in the address table, in which case the switch will broadcast the packet to all ports, negating many of the benefits of having a switch.*

Figure 7-16. Layer 2 Switch Settings Screen

Parameter	Description
MAC Address Aging Time	Specifies the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). The Aging Time can be set to any value between **10** and **1,000,000** seconds.
Broadcast/Multicast Storm Mode	Allows the Broadcast/Multicast Storm control to be **Enabled** or **Disabled**. This enables or disables, globally, the switch's reaction to Multicast storms, triggered at the threshold set below.

Upper Threshold for Base Ports	This is the number of thousands Broadcast/Multicast packets per second received by the switch – on one of the base ports – that will trigger the switch's reaction to a Broadcast/Multicast storm.
Upper Threshold for Module Ports	This is the number of thousands Broadcast/Multicast packets per second received by the switch – on one of the module ports – that will trigger the switch's reaction to a Broadcast/Multicast storm.
GVRP	Group VLAN Registration Protocol is a protocol that allows members to dynamically join VLANs.
GMRP	Group Multicast Registration Protocol is a protocol that allows members to dynamically join Multicast groups.
IGMP Snooping	Allows IGMP Snooping to be **Enabled** or **Disabled.** This enables or disables IGMP snooping for the switch.

Layer 3 IP Routing Protocol Settings

Note: *These IP Routing Protocol Settings are only for enabling or disabling, globally, routing protocols available on the switch. The Routing Information Protocol (RIP) is setup in the Setup RIP section later in this manual.*

Figure 7-17. Layer 3 IP Routing Protocol Settings

Parameter	Description
RIP	Allows RIP to be **Enabled** or **Disabled.** This enables or disables, globally, the Routing Information Protocol (RIP).
DVMRP	This enables or disables, globally, the Distance-Vector Multicast Routing Protocol (DVMRP).
DVMRP Incld. Report.	(This version of DVMRP allows reports from Unknown neighbor routers). This enables or disables, globally, the Distance-Vector Multicast Routing Protocol (DVMRP).
PIMDM	This enables or disables, globally, the Protocol Independent

Multicasting – Dense Mode (PIM-DM) multicasting protocol.

Setup IP Interface

The first menu displays the current IP interfaces on the switch. The Add and Edit menus are used to add a new IP interface, and to edit an existing IP interface, respectively.

Each IP interface on the switch corresponds to a VLAN. The VLAN must be configured before the IP interface can be setup. The IP interface must have the same name (and the same VID number) as its corresponding VLAN.

Note: *A VLAN that does not have a corresponding IP interface defined for it, will function as a* **Layer 2 Only** *VLAN – regardless of the* **Switch Operation** *mode.*

Figure 7-18. Setup IP Interface Screen

Parameter	Description
System	Displays the name of the IP interface corresponding to the IP address and subnet mask below.
IP Address	The IP address of the IP interface (sometimes referred to as a network address).
Subnet Mask	The subnet mask corresponding to the IP address and IP interface name above.

VID	The VLAN ID of the VLAN corresponding to this IP interface.
Active	Displays whether the IP interface is active or inactive.
New	A link to the IP Interface – Add menu.
More	A link to the IP Interface – Edit menu.

Add IP Interface

The following menu is used to add a new IP interface to the switch.

Figure 7-19. Setup IP Interface - Edit Screen

Parameter	Description
Subnet Name	A name given to identify this IP interface.
IP Address	The IP address of this IP interface (sometimes referred to as a network address).

Subnet Mask	The subnet mask for this IP interface.
VID	The VLAN ID of the VLAN corresponding to this IP interface.
Active	Allows this IP interface to be Active or Inactive on the switch.
Port Member	Allows the selection of ports to be members of this IP interface and its corresponding VLAN.

Edit IP Interface

The same menu is used to edit an existing IP interface as is used to add a new IP interface to the switch.

Figure 7-20. Setup IP Interface – Edit Screen

Parameter	Description
Subnet Name	Displays the subnet name corresponding to the IP address entered below.

IP Address	The IP address of the IP interface to be edited.
Subnet Mask	The subnet mask of the IP interface to be edited.
VID	The VLAN ID of the VLAN corresponding to this IP interface.
Active	Allows this IP interface to be Active or Inactive on the switch.
Port Member	Displays the ports that are members of this IP interface and its corresponding VLAN.

Setup RIP

The Routing Information Protocol (RIP) is a distance-vector protocol that uses the hop count as its criteria for making routing decisions. RIP is an Interior Gateway Protocol (IGP), which means that it performs routing within a single autonomous system.

Figure 7-21. Setup RIP Screen

Parameter	Description
Subnet Name	Displays the name of the subnet on which RIP is to be setup. This subnet must be previously configured on the switch.
IP Address	Displays the IP address corresponding to the subnet name above.

Tx Mode	Displays whether transmitted RIP packets will be structured as **V1 only, V1 Compatible, V2 Only,** or **Disabled**. This entry specifies which version of the RIP protocol will be used to transmit RIP packets. Disabled prevents the transmission of RIP packets.
Rx Mode	Displays whether received RIP packets will be interpreted as RIP version **V1 only, V2 Only, V1 and V2,** or **Disabled**. This entry specifies which version of the RIP protocol will be used to receive RIP packets. The Disabled entry prevents the reception of RIP packets.
Auth.	Displays whether RIP is configured to use an authorization string.
More	A link to the Setup RIP - Edit

Edit RIP Setup

The following menu is used to edit the switch's RIP setup.

Figure 7-22. Setup RIP – Edit Screen

Parameter	Description

Subnet Name	Displays the name of the subnet on which RIP is to be edited. This subnet must be previously configured on the switch.
IP Address	Displays the IP address corresponding to the subnet name above.
Tx Mode	Allows transmitted RIP packets to be structured as **V1 only, V1 Compatible, V2 Only,** or **Disabled**. This entry specifies which version of the RIP protocol will be used to transmit RIP packets. Disabled prevents the transmission of RIP packets.
Rx Mode	Determines how received RIP packets will be interpreted – as RIP version **V1 only, V2 Only, V1 and V2,** or **Diabled**. This entry specifies which version of the RIP protocol will be used to receive RIP packets. The Disabled entry prevents the reception of RIP packets.
Auth.	Allows RIP to be configured to use an authorization string.

Port Configuration

The following figure and table describe the configuration of ports on the switch. You can select a port to be configured by clicking on the port in Area 1 (the switch icon at the top of the web-based manager's user interface). This port then becomes the currently selected port and all entries in the following figure will apply to this port.

Figure 7-23. Configure Port Screen

Parameter	Description
Port Type	A read-only field that indicates the type of port currently selected.
Status	A read-only field that indicates the current status of the selected port.
State	Allows the currently selected port to be Enabled or Disabled.
Speed/Duplex	Allows the specification of the speed and full- or half-duplex state of the currently selected port. For 100 Mpbs ports the choices are; Auto, 10/Half, 10/Full, 100/Half, and 100/Full. For Gigabit ports, the choices are; Auto, 1000/Full.
Flow Control	Allows flow control to be Enabled or Disabled for the currently selected port.

Spanning Tree Protocol Configuration

The Spanning Tree Protocol can be used to detect and disable network loops, and to provide backup links between switches, bridges, or routers. This allows the switch to interact with other bridging devices (that is, STP compliant switches, bridges, or routers) in your network to ensure that only one route exists between any two stations on the network. For a more detailed description of how to use this protocol, refer to "Spanning Tree Concepts", in the DES-3326 Management Guide.

The following figures and tables describe the configuration of the Spanning Tree Protocol (STP) on the switch.

Figure 7-24. STP Switch Settings

Parameter	Default	Description
Spanning Tree Protocol	Enabled	Allows the STP to be globally Enabled or Disabled on the switch.
Max Age	20	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to

		reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STP information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. The minimum value is the higher of 6 or [2 x (Hello Time +1)]. The maximum value is the lower of 40 or [2 x (Forward Delay –1)].
Hello Time	2	The time interval (in seconds) at which the root device transmits a configuration message.
Forward Delay	15	The maximum time (in seconds) the root device will wait before changing states (i.e., from the listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward packets. In addition, each port needs time to listen for conflicting

		information that would make it return to a blocking state; otherwise, temporary data loops might result. Maximum value is 30 Minimum value is the higher of 4 or [(Max. Age / 2) +1]
Bridge Priority	32,768	Device priority used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STP root device. The lower the numeric value, the higher the priority. If all devices have the same priority, the device with the lowest MAC address will become the root device. Range 0 to 65535.

Spanning Tree Groups

Figure 7-25. Spanning Tree Groups Screen

The DES-3326 switch allows you to configure Spanning Tree Groups that consist of a group of ports that will be handled as though they were a single spanning tree device. The following figures and tables describe how to configure a spanning tree group.

***Note**: This function is available only when the switch is in IP Routing mode.*

Parameter	Description
Group Name	A name given to identify a given STP group.
Port Members	A list of the ports that belong to a given group.
More	A link to the Edit STP Group menu.
New	A link to the Add STP Group menu.

Add an STP Group

The following figure and table describe how to select a group of ports to become an STP Group. Click on the Exit icon to return to the Spanning Tree Groups menu.

Figure 7-26. STP Group Settings – Edit Screen

Parameter	Description
Group Name	A 12 character name used to identify the STP group.
Port Number	Check boxes used to select a port to be a member of the STP group. Click on the box corresponding to the port you want to add to the STP group.

Edit STP Group Settings

The following figure and table describe how to edit the settings of an STP Group. The STP Group Settings – Edit menu allows you to change which ports are members of the currently selected STP group. Click on the Exit icon to return to the Spanning Tree Groups menu.

Figure 7-27. STP Group Settings – Edit Screen

Parameter	Description
Group Name	The group name of the selected STP group.
Designated Root Bridge	The current root bridge for the STP group.
Root Priority	The current value of the bridge priority for the group.
Cost to Root	Displays the currently assigned cost for the route from the designated port for the STP group to the root bridge.
Last Topology Change	The time (in seconds) since the last change in the root bridge or designated port for the STP group.
Topology Change Count	The number of topology changes, for the currently selected STP group, since the switch was last restarted.

STP Port Settings

The following figure and table describe the display of the current STP port settings on the switch.

Figure 7-28. STP Port Settings Screen

Parameter	Description
Port Cost	A port cost can be set between 1 and 65535. The lower the cost, the greater the probability the port will be chosen as the designated port (chosen to forward packets).
Port Priority	A port priority can be set between 0 to 255. The lower the priority, the greater the probability the port will be chosen as the root port.
Status	Displays the status (Enabled or Disabled) for the corresponding port.

Group Name	Displays the previously assigned name for the STP group the corresponding port belongs to.

Forwarding

The following figures and tables describe how to setup static packet forwarding on the switch.

Figure 7-29. Setup Static Unicast MAC Forwarding Screen

Add an Entry

Parameter	Description
MAC Address	The MAC address to which packets will be statically forwarded.
VID	The VLAN ID number of the VLAN to which the above MAC address belongs.
PortMap	Allows the designation of the port on which the above MAC address resides.

Entries

Parameter	Description
MAC Address	Displays the MAC address corresponding to the static forwarding table entry.
VID	Displays the VLAN ID number of the VLAN to which the above MAC address belongs.
PortMap	Displays the port on which the above MAC address resides.

Static / Default Routes

The following figures and tables describe the entry of a Static / Default Routes into the IP routing table.

Figure 7-30. Static/Default Routers Screen

Parameter	Description
IP Address	Displays the IP addresses statically entered into the IP forwarding table.
Subnet Mask	Displays the corresponding subnet mask for the IP address above.

Gateway IP	Displays the corresponding IP address of the next hop gateway for the IP address above.
Metric	Displays the Routing Information Protocol (RIP) metric. This is the number of hops between the IP address and the Gateway. This is a number between 1 and 15.
New	A link to Static/Default Routes – Add menu.
Delete	Click on this icon to delete the entry.

Static / Default Routes – Add

The following figure and table describe the entry of a Static / Default Route into the switch's IP routing table. Click on the Exit icon to return to the Static / Default Routes menu.

Figure 7-31. Static/Default Routes – Add Screen

Parameter	Description

IP Address	The IP address to be statically entered into the IP forwarding table.
Subnet Mask	The corresponding subnet mask for the IP address above.
Gateway IP	The corresponding IP address of the next hop gateway for the IP address above.
Metric	The Routing Information Protocol (RIP) metric. This is the number of hops between the IP address and the Gateway. This is a number between 1 and 15.

Static ARP

The following figure and table describe the entry of a static Address Resolution Protocol (ARP) into the switch's static ARP table.

Figure 7-32. Static ARP Screen

Parameter	Description
Interface Name	Displays the IP interface on which the IP address previously entered into the static ARP table resides.
Interface IP	Displays the corresponding network address or IP address of the IP interface name above.

IP Address	Displays the IP address of the end node or station.
MAC Address	Displays the MAC address corresponding to the IP address above.
New	A link to the Static ARP – Add menu.
Delete	Click on the icon to delete the static ARP entry.

Static ARP – Add

The following figure and table describe adding an entry to the switch's static ARP table. Click on the Exit icon to return to the Static ARP menu.

Figure 7-33. Static ARP – Add Screen

Parameter	Description
Interface Name	The IP interface on which the IP address to be added to the static ARP table resides.
IP Address	The IP address of the end node or station.

MAC Address	The MAC address corresponding to the IP address above.

Filtering

The following figures and tables describe how to add a MAC or IP address to the MAC or IP filtering tables on the switch.

Figure 7-34. Setup MAC Address Filter Screen

Add and Entry

Parameter	Description
MAC Address	The MAC address that is to be filtered on the switch.
VID	The VLAN ID number of the VLAN on which the MAC address above resides.
State	Allows the selection of the state of the MAC address under which packets will be dropped by the switch. The options are; Dst. – destination, Src. – source, and Either. When Dst. is chosen, packets with the above MAC address as their destination will be dropped. When Src. is chosen,

	packets which the above MAC address as their source will be dropped. When Either is chosen, all packets to or from the above MAC address will be dropped by the switch.

Entries

Parameter	Description
MAC Address	Displays the MAC address that is to be filtered on the switch.
VID	Displays the VLAN ID number of the VLAN on which the MAC address above resides.
State	Displays the state of the MAC address under which packets will be dropped by the switch. The options are; Dst. – destination, Src. – source, and Either.
Remove	Click the icon to remove the entry from the filtering table.

IP Address Filter

The following figure and table describe the entry of an IP address into the switch's filtering table.

Figure 7-35. Filter Address Setup Screen

Filter Address Table

Parameter	Description
Address	The IP address that is to be filtered on the switch.
State	Allows the selection of the state of the above IP address under which packets will be dropped by the switch. The options are; DstAddr – destination address, ScrAddr – source address, and DstScrAddr – either a destination or a source address. When DstAddr is chosen, packets with the above IP address as their destination will be dropped, When ScrAddr is chosen, packets with the above IP address as their source will be dropped. When DstScrAddr is chosen, all packets with the above IP address will be dropped by the switch.

The Filter Address Table

Parameter	Description
Address	Displays the IP address that is to be filtered on the switch.
State	Displays the state of the above IP address under which packets will be dropped by the switch. The options are; DstAddr – destination address, ScrAddr – source address, and DstScrAddr – either a destination or a source address.
Remove	Click the icon to remove the entry from the filtering table.

Priority

The following figure and table describe how to setup an entry into the switch's priority table.

Figure 7-36. Setup MAC Address Priority

Add an Entry

Parameter	Description

MAC Address	The MAC address for which priority on the switch is to be established.
VID	The VLAN ID of the VLAN on which the MAC address above resides.
Level	The priority of the above MAC address. The options are; Low, Med-L – medium low, Med-h – medium high, and High.
State	The state under which the above priority will be active. The options are; Dst. – destionation, Src. – source, and Either. When Dst. is chosen, packets with the above MAC address as their destination will be given the selected priority. When Src. is chosen, packets with the above MAC address as their source will be given the selected priority. When Either is chosen, all packets with the above MAC address will be given the selected priority.

Entries

Parameter	Description
MAC Address	Displays the MAC address for which priority on the switch is to be established.
VID	Displays the VLAN ID of the VLAN on which the MAC address above resides.
Level	Displays the priority of the above MAC address. The options are; Low, Med-L – medium low, Med-h – medium high, and High.
State	Displays the state under which the above priority will be active. The options are; Dst. – destination, Src. – source, and Either.

Mirroring

Traffic from any source port to a target port can be mirrored for real-time analysis. A logic analyzer or an RMON probe can then be attached to study the traffic crossing the source port in a completely unobtrusive manner. When mirroring port traffic, note that the target port must be configured in the same VLAN and be operating at the same speed as the source port. If the target port is operating at a lower speed, the source port will be forced to drop its operating speed to match that of the target port.

The port mirror configuration screen can be used to designate a single RJ-45 port pair for mirroring as shown below:

Target Port Selection

The following figure and table describe the selection of a target port. A target port in a port mirroring pair is the port that will receive packets that are duplicate at the mirror port.

Figure 7-37. Target Port Selection

Parameter	Description
Target Port	The port that will receive the packets duplicated at the mirror port.

Mirror Port Configuration

The following figure and table describe the selection of a mirror port for port mirroring. A mirror port is the port (of a target – mirror pair) that will have its traffic duplicated and forwarded to the target port.

Figure 7-38. Setup Mirror Port Configuration Screen

Add and Entry

Parameter	Description
Source Port	The port that will be mirrored. All packets entering and leaving the source port can be duplicated in the mirror port.
Direction	Allows the specification of which packets will be mirrored based upon whether the packets are flowing into or out of a port, or all packets (both directions). The options are; Ingress – packets flowing into the mirror port, Egress – packets flowing out of the mirror port, and Either – both in to and out of the mirror port. For example, if Ingress is chosen, all packets flowing into the mirror port will be duplicated and forwarded to the target port.

Entries

Parameter	Description
Source Port	Displays the port that will be mirrored.
Direction	Allows the specification of which packets will be mirrored based upon whether the packets are flowing into or out of a port, or all packets (both directions). The options are; Ingress – packets flowing into the mirror port, Egress – packets flowing out of the mirror port, and Either – both in to and out of the mirror port.

IEEE 802.1Q Multicast Forwarding

The following figure and table describe how to set up Multicast forwarding on the switch.

Figure 7-39. Setup IEEE 802.1Q Multicast Forwarding Screen

Parameter	Description

MAC Address	The MAC address of the static source of multicast packets.
VID	The VLAN ID of the VLAN the above MAC address belongs to.
PortMap / State	Allows the selection of ports that will be members of the static multicast group and ports that are either forbidden from joining dynamically, or that can join the multicast group dynamically, using GMRP. The options are; None – no restrictions on the port dynamically joining the multicast group, Egress – the port is a static member of the multicast group, and Forbidden – the port is restricted from joining the multicast group dynamically. For example, if None is chosen, then an end station attached to the port can join the multicast group using GMRP.

Multicast Interface Configuration

The following figure and table describe how to configure a multicast interface.

Figure 7-40. Multicast Interface Configuration Screen

Parameter	Description
Interface Name	The name of the IP interface (previously defined) on the switch for which a multicast interface is to be configured.
IP Address	The IP address (sometimes referred to as a network address) that corresponds to the interface name above.
IGMP	Allows IGMP to be Enabled or Disabled for the IP interface.
Multicast Routing Protocol	*As of firmware release 1.00-B14*, Allows the selection of the multicast routing protocol to be used with the above IP interface. The options are; DVMRP – Distance Vector Multicast Routing Protocol, PIMDM

	– Protocol Independent Multicasting Dense Mode, and INACT – the interface is inactive. For example, if DVMRP is chosen, then this routing protocol will be used to forward multicast packets for the above IP interface.

IGMP Settings

The following figure and table describe how to configure Internet Group Management Protocol (IGMP) on the switch.

Figure 7-41. IGMP Interface Setup Screen

Parameter	Description
Interface Name	The name of the IP interface (previously defined) on the switch for which a multicast interface is to be configured.

IP	The IP address corresponding to the IP interface name above.
Version	The version number of the IGMP to be used for the above IP interface.
Query	The time (in seconds) between the transmission of IGMP query packets.
Max. Resp.	The maximum number of respondents to an IGMP query. Range is between 1 and 25.
Robustness Var.	The Robustness Variable – a numeric value between 1 and 255 defining the maximum time (in seconds) between the receipt of IGMP queries. If this timer expires without the receipt of another IGMP query, the switch assumes the queerer is no longer present.

DVMRP Settings

The following figure and table descript the configuration of DVMRP on the switch.

Figure 7-42. DVMRP Interface Configuration Screen

Parameter	Description
Interface Name	The name of the IP interface (previously defined) on the switch for which a multicast interface is to be configured.
IP Address	The IP address (sometimes referred to as a network address) corresponding to the interface name above.
Probe Interval	DVMRP defines an extension to IGMP that allows routers to query other routers to determine if a multicast group is present on an given router subnetwork or not. This is referred to as a 'probe'. The default value is 10 seconds.
Nbr Report Timer	The time (in seconds) for which Non-Membership Reports (NMR) are valid. The default value is 35 seconds.

Route Cost	Allows the assignment of a DVMRP route cost to the above IP interface. A DVMRP route cost is a relative number that represents the real cost of using this route in the construction of a multicast delivery tree. It is similar to, but not defined as, the hop count in RIP. The default value is 1.
State	Allows DVMRP to be Disabled or Enabled for the above IP interface. The default is Disabled.

PIM-DM Setup

The following figure and table describe the configuration of a Protocol Independent Multicast - Dense Mode (PIMDM) interface on the switch.

Figure 7-43. PIMDM Interface Configuration Screen

Parameter	Description
Interface Name	The name of the IP interface (previously defined) on the switch for which a multicast interface is to be configured.
IP Address	The IP address (sometimes referred to as a network address) corresponding to the interface name above.
Hello Interval	Determines the interval between sending Hello packets to other routers on the network. The Hello messages are used by the router to determine if it is the root router on the delivery tree or not. If the router does not receive a Hello message within the Hello Interval, it will begin transmitting Hello messages to advertise its availability to become the root router. The range is between 1 and 65535 seconds. *The default is* **30** *seconds.*
Join/Prune Interval	Determines the interval between transmitting (flooding to all interfaces) multicast messages to downstream routers, and automatically 'pruning' a branch from the multicast delivery tree. This interval also determines the time interval the router uses to automatically remove prune information from a branch of a multicast delivery tree and begin to flood multicast messages to all branches of that delivery tree. These two actions are equivalent. The range is between 1 and 65535 seconds. *The default is* **60** *seconds.*

State	Allows PIMDM to be Disabled or Enabled for the above IP interface. The default is Disabled.

Static Router Port Settings

The following figures and table describe how to set up a static router port on the switch.

Figure 7-44. Static Router Port Settings Screen

Parameter	Description
VID	The VLAN ID of the VLAN the static router port resides on.
Port Members	The ports that are set up as static router ports.
New	A link to the Static Router Port Settings – Add menu.
Delete	Click on the icon to delete the entry from the static router port table.

Add a Static Router Port

The following figure and table describe how to add a static router port on the switch. Click on the Exit icon to return to the Static Router Port Settings menu.

Figure 7-45. Static Router Port Settings – Add Screen

Parameter	Description
VID	The VLAN ID of the VLAN on which the static router port resides.
Port Member	Click the box corresponding to the port that will be a static router port.

VLANs

IEEE 802.1Q VLANs

The following figures and tables describe how to set up 802.1Q VLANs on the switch.

Figure 7-46. 802.1Q Static VLANs Screen

Parameter	Description
VID	The VLAN ID of the VLAN on which the static router port resides.
VLAN Name	The name of the VLAN for which ports are to be configured.

Add a Static 802.1Q VLAN

The following figure and table describe how to add an 802.1Q VLAN on the switch.

Figure 7-47. 802.1Q Static VLANs Entry Settings – Edit Screen

Parameter	Description
VID	The VLAN ID of the VLAN that is being created.

VLAN Name	The name of the VLAN that is being created.
Port	Corresponds to the ports that will be members of the VLAN.
Tag	Specifies the port as either 802.1Q tagging or 802.1Q untagging. Checking the box will designate the port as Tagging.
None	Specifies the port as not being a static member of the VLAN, but with no restrictions for joining the VLAN dynamically through GVRP.
Egress	Specifies the port as being a static member of the VLAN. Egress Member Ports are ports that will be transmitting traffic for the VLAN.
Forbidden	Specifies the port as not being a static member of the VLAN, and as being forbidden from joining the VLAN dynamically.

Edit 802.1Q VLANs

The following figure and table describe how to edit an existing 802.1Q VLAN entry on the switch.

Figure 7-48. 802.1Q Static VLANs Entry Settings – Edit Screen

Parameter	Description
VLAN ID (VID)	The VLAN ID of the VLAN to be edited. For editing, VLANs are identified by name.
VLAN Name	The name of the VLAN to be edited.
Port	A list of the ports that are static members of the currently selected VLAN.
Tag	Specifies the port as either 802.1Q tagging or 802.1Q untagging. Checking the box will designate the port as Tagging.
None	Specifies the port as not being a static member of the VLAN, but with no restrictions for joining the VLAN dynamically through GVRP.
Egress	Specifies the port as being a static member of the VLAN. Egress Member Ports are

	ports that will be transmitting traffic for the VLAN.
Forbidden	Specifies the port as not being a static member of the VLAN, and as being forbidden from joining the VLAN dynamically.

Port VLAN ID (PVID)

The following figure and table describe how to configure the PVID for the switch.

Figure 7-49. Port VLAN ID (PVID) Screen

Parameter	Description

Port VLAN ID	The PVID is used by the port to tag outgoing, untagged packets, and to make filtering decisions about incoming packets. If the port is specified as tagging, and an untagged packet if forwarded to the port for transmission, the port will add an 802.1Q tag using the PVID to write the VID in the tag. When the packet arrives at its destination, the receiving device will use the PVID to make VLAN forwarding decisions. If a packet is received by the port, and Ingress filtering is enabled, the port will compare the VID of the incoming packet to its PVID. If the two are unequal, the port will drop the packet. If the two are equal, the port will receive the packet.
Port	Shows the current PVID assignment for each port. The switch's default is to assign all ports to the Default_VLAN with a VID of 1.

Port Ingress Filter

The following figure and table describe how to configure a Port Ingress Filter on the switch.

Figure 7-50. Port Ingress Filter Screen

Parameter	Description
Port	The number of the port for which ingress filtering is to be Enabled or Disabled.
Ingress Filter	Specifies the port to check the VID of incoming packets against its VID or PVID. If the two are equal, the port will receive the packet. It the two are unequal, the port will drop the packet. This is used to limit traffic to a single VLAN.

Port GVRP Settings

The following figure and table describe how to configure the Port Group VLAN Registration Protocol (GVRP) on the switch.

Figure 7-51. Port GVRP Settings Screen

Parameter	Description
Port	The number of the port for which GVRP is to be Enabled or Disabled.
GVRP	For each corresponding port, GVRP can be Enabled or Disabled.

Port GMRP Settings

The following figure and table describe how to configure the Port Group Multicast Registration Protocol (GMRP) on the switch.

Figure 7-52. Port GMRP Settings Screen

Parameter	Description
Port	The number of the port for which GMRP is to be Enabled or Disabled.
GMRP	For each corresponding port, GMRP can be Enabled or Disabled.

Port Trunking

Port trunks can be used to increase the bandwidth of a network connection or to ensure fault recovery. You can configure up to 6 trunk connections (combining 2 to 8 ports into a fat pipe) between any two DES-3326 or other Layer 2 switches. However, before making any physical connections between devices, use the Trunk Configuration menu to specify the trunk on the devices at both ends. When using a port trunk, note that:

- The ports used in a trunk must all be of the same media type (RJ-45, 100 Mbps fiber, or 1000 Mbps fiber). The ports that can be assigned to the same trunk have certain other restrictions (see below).
- Ports can only be assigned to one trunk.
- The ports at both ends of a connection must be configured as trunk ports.
- None of the ports in a trunk can be configured as a mirror source port or a mirror target port.
- All of the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- The Spanning Tree Protocol will treat all the ports in a trunk as a whole.
- Enable the trunk prior to connecting any cable between the switches to avoid creating a data loop.
- Disconnect all trunk port cables or disable the trunk ports before removing a port trunk to avoid creating a data loop.

Use the Port Trunking Configuration screen to set up port trunks as shown below.

Figure 7-53. Link Aggregation Screen

Parameter	Description
Group	The switch allows up to 6 port trunks groups to be configured. The group number identifies each of these groups.
Master Port	The port of the trunk group whose configuration (speed, full- or half-duplex, etc.) will be used by all of the ports in the trunk group.
Number of Members	The number of contiguous ports in the selected trunk group.
State	Allows the trunk group to be Enabled or Disabled.
Anchor	The same as the master port.

The RJ-45 ports used for each trunk must all be on the same internal switch chip. The port groups permitted include:

Group 1	Group 2	Group 3	Group 4
1,2,3,4,	5,6,7,8,	9,10,11,12,	25,26
13,14,15,16	17,18,19,20	21,22,23,24	

Only two ports on an optional front-panel module (ports 25 and 26) can be configured as a trunk group.

BOOTP/DHCP Relay

BOOTP/DHCP relay enables end stations to use a BOOTP or DHCP server to obtain TCP/IP configuration information or boot files to be loaded into memory, even if the servers are not on the local IP interface.

If the BOOTP or DCHP server and end station are on the same IP interface, no relay is necessary. If the servers and the end stations are on different IP interfaces, a relay agent is necessary for the switch to forward the messages.

The relay agent forwards these packets between IP interfaces, and therefore must know the IP addresses of the BOOTP and DHCP servers and their respective subnet names (or IP interface names).

When the switch receives packets destined for a BOOTP or DHCP server, it forwards them to specific servers as defined in the following configuration. The switch also forwards packets from the BOOTP or DHCP servers to the appropriate subnets.

The first task is to set some parameters for the relay agent to decide whether or not to forward a given BOOTP/DCHP packet.

Figure 7-54. BOOTP/DHCP Relay Screen

Parameter	Description
BOOTP/DHCP Relay Status	Allows the BootP/DHCP relay function to be Enabled or Disabled.
BOOTP HOPS Count Limit	Allows the maximum number of hops (routers) that the BootP messages can be relayed through to be set. If a packet's hop count is more than the hop count limit, the packet is dropped. The range is between 1 and 16 hops. The default value is 4.
BOOTP/DHCP Relay Time Thresh.	Sets the minimum time (in seconds) that the switch will wait before forwarding a BOOTREQUEST packet. If the value in the seconds field of the packet is less than the relay time threshold, the packet will

be dropped. The range is between 1 and 65,535 seconds. The default value is 4 seconds.

Static Bootp Relay Setup

The second task is to tell the BOOTP/DCHP relay agent where the servers are located in terms of IP addresses and subnet names (IP interface names).

The following figure and table describe how to set up the static Bootp Relay function on the switch.

Figure 7-55. BOOTP Relay Setup Screen

Parameter	Description
Subnet Name	The subnet name (IP interface name) of the network that the BOOTP server is located on.

Relay Server	The IP address of the BOOTP relay server. Multiple servers may be entered for a given subnet name (IP interface name).
Relay Server	Displays the entered IP address of the BOOTP relay server for the corresponding subnet.
Remove	Click on the icon to remove the entry from the table.

DNS Relay

DNS relay enables end stations to use a DNS server to resolve domain names into IP addresses, even if the server and the end station are not on the local IP interface.

If the DNS server and end station are on the same IP interface, no relay is necessary. If the servers and the end stations are on different IP interfaces, a relay agent is necessary for the switch to forward the messages.

The relay agent forwards these packets between IP interfaces, and therefore must know the IP addresses of the DNS servers and their respective subnet names (or IP interface names).

When the switch receives packets destined for a DNS server, it forwards them to specific servers as defined in the following configuration. The switch also forwards packets from the DNS servers to the appropriate subnets.

The first task is to set some parameters for the relay agent to decide whether or not to forward a given DNS packet.

Figure 7-56. DNS Relay Setup Screen

Parameter	Description
DNS Relay State	Allows the DNS relay function to be Enabled or Disabled on the switch.
Primary Name Server	The IP address of the primary DNS server.
Secondary Name Server	The IP address of a secondary DNS server.
DNS Relay Cache Status	Allows the DNS cache on the switch to be Enabled or Disabled.
DNS Static Table Lookup	Allows the DNS Static Table Lookup function on the switch to be Enabled or Disabled.

Static DNS Table

The second task is to tell the DNS relay agent where the servers are located in terms of IP addresses and subnet names (IP interface names).

The following figure and table describe how to set up the static DNS Relay function on the switch.

Figure 7-57. DNS Static Table Configuration Screen

Parameter	Description
Domain Name	The subnet name (IP interface name) of the network that the BOOTP server is located on.
IP Address	The IP address of the BOOTP relay server. Multiple servers may be entered for a given subnet name (IP interface name).
State	Displays the entered IP address of the BOOTP relay server for the corresponding subnet.

Statistics

WebView allows various statistics about the switch's performance to be viewed.

Port Packet Analysis

Update Interval: Suspend Clear

Frame Size/Type	Frames	Frames/sec
64	1490866	116
65-127	130479	10
128-255	1024821	7
256-511	3184	1
512-1023	270	0
1024-1518	77128	0
	Frames	Frames/sec
Unicast RX	124140	2
Multicast RX	1111705	8
Broadcast RX	1487236	123

Packet Type		Total	Total/sec
Rx	Bytes	398110565	10078
	Frames	2723081	133
Tx	Bytes	1070199	64
	Frames	3667	1

Figure 7-58. Port Packet Analysis Screen

Parameter	Description
Update Interval	The interval (in seconds) that the table will be updated. The default is *Suspend*.
Frame Size/Type	The size in octets (bytes) of frames transferred through the switch.

Frames	The total number of frames transferred through the switch of the corresponding size indicated.
Frames/sec	The number of frames per second transferred through the switch of the corresponding size indicated.
Packet Type	Rx – received Tx - transmitted

Port Error Statistics

The following figure and table describe the port error statistics compiled by the switch's management agent.

Parameter	Description
Update Interval	The interval (in seconds) that the table is updated. The default is *Suspend*.
Rx	Received packets.
CRC Error	For 10 Mbps ports, the counter records CRC errors (FCS or alignment errors). For 100 Mbps ports, the counter records the sum of CRC errors and code errors (frames received with rxerror signal).
Undersize	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.

	Oversize	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
	Fragments	The total number of frames received that were less that 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or an alignment error.
	Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or an alignment error.
	Drop Pkts	The total number of events in which packets were dropped due to a lack of resources.
Tx		Transmitted packets.
	ExDefer	The number of frames for which the first transmission attempt on a particular interface was delayed because the medium was busy.
	CRC Error	For 10 Mbps ports, the counter records CRC errors (FCS or alignment errors). For 100 Mbps ports, the counter records the sum of CRC errors and code errors (frames received with rxerror signal).
	Late Coll.	Late Collisions. The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
	Ex. Coll.	Excessive Collisions. The number of frames for which transmission failed due to excessive collisions.

Single Coll.*	Single Collision Frames. The number of successfully transmitted frames for which transmission is inhibited by more than one collision.
Coll.	An estimate of the total number of collisions on this network segment.

Port Utilization Statistics

The following figure and table describe the port utilization statistics compiled by the switch's management agent.

Figure 7-59. Port Utilization Screen

Parameter	Description
Update Interval	The interval (in seconds) that the chart is updated. The default is *Suspend*.

Address Table

The following figures and tables describe how to browse the switch's address tables.

Browse MAC Address Table

WebView allows the switch's MAC address table (sometimes referred to as a forwarding table) to be viewed.

VID	MAC Address	Port	Learned
1	00-00-00-00-24-37	1	dynamic
1	00-00-81-9a-a0-9f	1	dynamic
1	00-00-14-95-b5-4a	1	dynamic
1	00-00-f8-7c-1c-29	1	dynamic
1	00-01-02-03-04-05	1	dynamic
1	00-01-30-5c-df-00	1	dynamic
1	00-04-5a-08-52-62	1	dynamic
1	00-04-ac-09-68-02	1	dynamic
1	00-10-6f-03-0f-b1	1	dynamic
1	00-18-96-55-0a-01	1	dynamic
1	00-20-48-2d-7e-ed	1	dynamic
1	00-20-48-2e-21-53	1	dynamic
1	00-20-48-36-00-01	1	dynamic
1	00-20-48-5a-70-a2	1	dynamic
1	00-20-48-5b-16-64	1	dynamic
1	00-20-48-68-02-31	1	dynamic
1	00-21-32-11-79-99	1	dynamic
1	00-30-65-d0-08-0a	1	dynamic
1	00-30-65-d0-10-0a	1	dynamic
1	00-33-26-00-26-00	CPU	self

Figure 7-60. Browse MAC Address Table

Parameter	Description
VID	The VLAN ID of the VLAN the port is a member of.
MAC Address	The MAC address entered into the address table.
Port	The port that the MAC address above corresponds to.
Learned	How the switch discovered the MAC address. The possible entries are Dynamic, Self, and Static.

Browse IP Address Table

WebView allows the IP address table (sometimes referred to as a forwarding table) to be viewed.

Figure 7-61. IP Address Table

Parameter	Description
IP Name	The name of the IP Interface corresponding to the IP address below.
IP Address	The IP address corresponding to the IP interface name above.
Port#	The port the IP interface is attached to.
Learned	How the switch discovered the IP interface. The possible entries are Dynamic, and Static.

Browse the Routing Table

WebView allows the switch's routing table to be viewed.

Figure 7-62. Browse Routing Table

Parameter	Description
Destination Address	IP address of a learned or statically entered destionation.
Mask	Displays the subnet mask corresponding to the above destination IP address.
Gateway	Displays the default or next hop gateway to reach the destination.
Jump	Click the Jump button to go to a particular combination of destination IP address, subnet mask, and gateway address.
Interface Name	Displays the IP interface name the destination resides on.
Hops	Displays the number of hops (routers) between the switch and the destination.

Protocol	Displays the routing protocol in use by the link to the destination.

Browse the ARP Table

WebView allows the Address Resolution Protocol (ARP) table compiled by the switch to be viewed.

The ARP table allows the switch to relate often used IP addresses to MAC addresses quickly, and without having to make ARP requests.

Figure 7-63. ARP Table

Parameter	Description

Start Interface Name	Allows the specification of an IP interface name to start the display of the ARP table. If the specified IP interface name is present in the ARP table, then it will be the first entry of the displayed table.
Start IP Address	Allows the specification of an IP address to start the display of the ARP table. If the specified IP address is present in the ARP table, then it will be the first entry of the displayed table.
Interface Name	The IP interface name corresponding to the IP address below.
Interface IP Address	The interface IP address (sometimes referred to as a network address) corresponding to the IP address below.
IP Address	The IP address that corresponds to the MAC address below.
MAC Address	The MAC address that corresponds to the IP address above.
Type	How the IP address, MAC address pair were entered into the ARP table. The possible entries are Static and Dynamic.

Applications

The following figures and tables describe the applications available when using the web-based manager.

Switch History

The web-based manager allows the switch's history log, as compiled by the switch's management agent, to be viewed.

Sequence	Time	Log Text
146	000d01h40m	Console session time out .....
145	000d01h30m	Console session time out .....
144	000d01h20m	Console session time out .....
143	000d01h10m	Console session time out .....
142	000d01h00m	Console session time out .....
141	000d00h50m	Console session time out .....
140	000d00h40m	Console session time out .....
139	000d00h30m	Console session time out .....
138	000d00h20m	Console session time out .....
137	000d00h11m	Successful login through web.
136	000d00h10m	Console session time out .....
135	000d00h01m	Successful login through web.
134	000d00h00m	Topology Change
133	000d00h00m	Module 1, Port 1 Link Up
132	000d00h00m	Cold Start
131	000d00h57m	Configuration saved to flash.
130	000d00h57m	Change switch to Layer 3 with IEEE802.1Q vlan
129	000d00h50m	Console session time out .....
128	000d00h40m	Console session time out .....
127	000d00h30m	Console session time out .....

Figure 7-64. Switch History

Parameter	Description
Sequence	A counter incremented whenever an entry to the switch's history log is made. The table displays the last entry (highest sequence number) first.
Time	Displays the time in days, hours, and minutes since the switch was last restarted the history log entry was made.
Log Text	Displays text describing the event that triggered the history log entry.

Browse the Router Port Table

A static router port is simply a port that has a router attached to it. Generally, this router would have a connection to a WAN or to the Internet. Establishing a router port allows multicast packets coming from the router to be propagated throughout the network, as well as allowing multicast messages coming from the network to be propagated to the attached router.

The purpose of a router port is to enable UDP multicast packets, and IGMP multicast group membership messages to reach a multicast router. Routers do not implement IGMP snooping or transmit/forward IGMP report packets. Thus, forwarding all IP UDP multicast packets to a static router port guarantees that all multicast routers – attached to the switch – can reach all multicast group members.

The switch monitors each port for UDP multicast packets and IGMP multicast group membership reports. When these packets are detected on a port, that port is dynamically assigned as router port.

Figure 7-65. Browse Router Port

Parameter	Description
Start VID	Allows a VID to be specified to search the router port table with.
Jump	Click the Jump button to search the router port table using the VID entered above.
Port Members	Ports that are router ports, both statically and dynamically assigned.
D: dynamic router port	Ports that are dynamically assigned as router ports.

Browse IGMP Snooping Table

The switch's IGMP snooping table can be browsed using WebView. The table is displayed by VLAN IP (VID).

Figure 7-66. IGMP Snooping Table

Parameter	Description
VID	VLAN ID of the VLAN for which the IGMP Snooping table is to be displayed.
View	Click on the View button to display the IGMP Snooping Table for the current VID.
Multicast Group	The IP address of a multicast group learned by IGMP snooping.
Mac Address	The corresponding MAC address learned by IGMP snooping.
Port Map	Displays the ports that have forwarded multicast packets from the above source.
Reports	The number of IGMP reports for the listed source.

Browse IP Multicast Forwarding Table

The switch allows WebView to browse its IP multicast forwarding table for static and dynamic (learned) entries. The table can also be searched using a combination of a multicast group IP address, and a multicast source IP address – subnet mask.

Figure 7-67. IP Multicast Forwarding Table

Parameter	Description
Multicast Group	The IP address of a multicast group used in combination with the source IP address and the corresponding subnet mask to search the IP multicast forwarding table for a specific entry.
SourceIP	The IP address of a multicast source used in combination with the multicast group IP address and the corresponding subnet mask to search the IP multicast forwarding table for a specific entry.
Mask	The subnet mask of a multicast source used in combination with the source IP address

	and the corresponding multicast group IP address to search the IP multicast forwarding table for a specific entry.
Jump	Click on the Jump button to search the IP multicast forwarding table for the above specified entry.
UpStream Neighbor	Displays the IP address of the next hop router between the multicast group and the source.
Ttl	Displays the Time-To-Live value of packets from the multicast source in hops.
If-mprot	Displays the multicast routing protocol used by the current source.

Browse IGMP Table

The following figure and table describe how to browse the switch's IGMP table.

Figure 7-68. IGMP Group Table

Parameter	Description
Interface Name	Allows the IGMP table to be searched using a combination of an IP interface name and a Multicast group IP address.
Start Multicast Grp	Allows the IGMP table to be searched using a combination of an IP interface name and a Multicast group IP address.
Jump	Click on the Jump button to search the IGMP table for the IP interface name – Multicast group IP address combination entered above.

Browse DVMRP Routing Table

The following figure and table describe how to browse the switch's DVMRP routing table.

Figure 7-69. DVMRP Routing Table

Parameter	Description
Source Address	Allows the DVMRP routing table to be searched for the entered IP address – subnet mask combination.
Source Mask	Allows the DVMRP routing table to be searched for the entered IP address – subnet mask combination.
Jump	Click on the Jump button to search the DVMRP routing table for the IP address – subnet mask combination entered above.
Next Hop Router	Displays the IP address of the next hop router for the source address.
Hops	Displays the number of hops (routers) between the multicast group member and the switch.
Learned	Displays how the switch discovered the source address. The possibilities are Static, and Dynamic.
Interface Name	The IP interface name of the source address.

Utilities

Trivial File Transfer Protocol (TFTP) services allow the switch firmware to be upgraded by downloading a new firmware file from a TFTP server to the switch. A configuration file can also be loaded into the switch, and switch settings can be saved to a TFTP

server. In addition, the switch's history log can be uploaded from the switch to a TFTP server.

The following figures and tables describe how to use the utilities available in WebView.

Update Firmware

Note: *The TFTP server must be on the same IP subnet as the switch.*

The following figure and table describe how to update the switch's firmware from a server.

Figure 7-70. Update Firmware from Server Screen

Parameter	Description
Server IP Address	The IP address of the TFTP server.
File Name	The full file name (including path) of the new firmware file on the TFTP server.

Configuration Files

A configuration file can be downloaded from a TFTP server to the switch. This file is then used by the switch to configure itself.

Figure 7-71. Use Configuration File on Server Screen

Parameter	Description
Server IP Address	The IP address of the TFTP server.
File Name	The full file name (including path) of the configuration file on the TFTP server.

Save Switch Settings to a TFTP Server

The switch's current settings san be uploaded to a TFTP Server by the switch's management agent.

Figure 7-72. Save Settings to TFTP Server Screen

Parameter	Description
Server IP Address	The IP address of the TFTP server.
File Name	The full file name (including path) of the settings file on the TFTP server.

Save Switch History to TFTP Server

The switch's management agent can upload its history log file to a TFTP server.

Figure 7-73. Save Switch History to TFTP Server

Parameter	Description
Server IP Address	The IP address of the TFTP server.
File Name	The full file name (including path) of the history file on the TFTP server.

Reset

The following menu is used to restart (reboot) the switch. Click on **Yes** to save the current switch configuration to non-volatile RAM (flash RAM), or **No** if you want to restart the switch using the last-saved (previous) configuration.

Click the **Restart** button to restart the switch.

Figure 7-74. Restart System Screen

Factory Reset

The following menu is used to restart the switch using only the configuration that was supplied by the factory. A factory reset returns all configuration options to their default values and restores the switch's configuration to the factory settings.

All user-entered configuration information will be lost.

Figure 7-75. Factory Reset Screen

Click **Yes** if you want the switch to retain its current IP address. Click **No** to reset the switch's IP address to the factory default, 10.90.90.90.

Click the **Reset to Factory Default** button to restart the switch.

A

TECHNICAL SPECIFICATIONS

	General	
Standards:	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3z 1000BASE-SX Gigabit Ethernet IEEE 802.1 P/Q VLAN IEEE 802.3x Full-duplex Flow Control ANSI/IEEE 802.3 Nway auto-negotiation	
Protocols:	CSMA/CD	
Data Transfer Rates:	Half-duplex	Full-duplex
Ethernet	10 Mbps	20Mbps
Fast Ethernet	100Mbps	200Mbps
Gigabit Ethernet	n/a	2000Mbps
Topology:	Star	

	General
Network Cables: 10BASE-T: 100BASE-TX: Fiber Optic:	 2-pair UTP Cat. 3,4,5 (100 m) EIA/TIA- 568 100-ohm STP (100 m) 2-pair UTP Cat. 5 (100 m) EIA/TIA-568 100-ohm STP (100 m) IEC 793-2:1992 Type A1a - 50/125um multimode Type A1b - 62.5/125um multimode Both types use MTRJ or SC optical connector
Number of Ports:	24 x 10/100 Mbps NWay ports 2 Gigabit Ethernet (optional)

	Physical and Environmental
AC inputs:	100 - 240 VAC, 50/60 Hz (internal universal power supply)
Power Consumption:	40 watts maximum
DC fans:	2 built-in 40 x 40 x10 mm fan
Operating Temperature:	0 to 50 degrees Celsius
Storage Temperature:	-25 to 55 degrees Celsius
Humidity:	Operating: 5% to 95% RH non-condensing; Storage: 0% to 95% RH non-condensing
Dimensions:	441 mm x 207 mm x 44 mm (1U), 19 inch rack-mount width

	Physical and Environmental
Weight:	2 kg
EMI:	FCC Class A, CE Class A, VCCI Class A, BSMI Class A, C-Tick Class A FCC Part 15/IECES-003 (Canada), VCCI Class A ITE, EN55022/EN50082-1 or EN%%o24, C-Tick (AS/NZS3548, BSMI (CNS 13438)
Safety:	UL, CSA, CE Mark, TUV/GS UL 1950 & CSA22.2 No 950, IEC 950 (CB), TUV (EN60950)

	Performance
Transmission Method:	Store-and-forward
RAM Buffer:	16 MB per device
Filtering Address Table:	8K MAC address per device
Packet Filtering/ Forwarding Rate:	Full-wire speed for all connections. 148,800 pps per port (for 100Mbps) 1,488,000 pps per port (for 1000Mbps)
MAC Address Learning:	Automatic update.
Forwarding Table Age Time:	Max age:10–9999 seconds. Default = 300.

B

RJ-45 PIN SPECIFICATION

When connecting the DES3226S Switch to another switch, a bridge or a hub, a modified crossover cable is necessary. Please review these products for matching cable pin assignment.

The following diagram and table show the standard RJ-45 receptacle/connector and their pin assignments for the switch-to-network adapter card connection, and the straight/ crossover cable for the Switch-to-switch/hub/bridge connection.

Figure B-1. The standard RJ-45 receptacle/connector

RJ-45 Connector pin assignment	
Contact	Media Direct Interface Signal
1	Tx + (transmit)
2	Tx - (transmit)
3	Rx + (receive)
4	Not used
5	Not used
6	Rx - (receive)
7	Not used
8	Not used

Table B-1. The standard Category 3 cable, RJ-45 pin assignment

The following shows straight cable and crossover cable connection:

Figure B-2. Straight cable for Switch (uplink MDI-II port) to switch/Hub or other devices connection

Figure B-3. Crossover cable for Switch (MDI-X port) to switch/hub or other network devices (MDI-X port) connection

C

SAMPLE CONFIGURATION FILE

This Appendix provides a sample configuration file that can be used with the Update Firmware and Configuration Files screen in the console program.

The configuration file is a simple text file that you create. It has two functions: to point to the location of a file on a TFTP server, and to set the IP address, subnet mask and default gateway for the switch. The file being uploaded can be either new Runtime switching software, or a switch settings file which was previously saved on the TFTP server using the *Save settings to TFTP Server* option in the *System Utilities* menu. The IP address settings defined in the configuration file will override all other IP settings, even those defined in the settings file being uploaded. This enables the settings from one switch to be uploaded to another switch without their IP settings being the same (and thus coming into conflict).

Commands:

- `Code_type` – this command tells the switch the type of file you wish to upload to the switch. Possible Code_types are `PROM`, `RUNTIME`, or `CONFIG`. This should always be the first setting.

- PROM – PROM update file.
- RUNTIME – Switching software update file.
- CONFIG – Image file of switch settings created by the settings backup procedure.

♦ `Image_file` – this command tells the switch the complete path and filename for the file to be loaded into the switch. For example, "`e:\3326\3326prom.tfp`". Make sure double-quotes are used as in the example file below.

♦ `Ip_addr` – this is the IP address that will be assigned to the switch. This command is included for downloading a configuration settings file to another switch. The IP address defined in this file will override the IP address in the configuration settings file, thus the switch you are downloading to can have a different IP address than the one that created the configuration settings file. An example IP address is `10.12.19.102`.

♦ `Subnet_mask` – this is the subnet mask that will be assigned to the switch. An example subnet mask is `255.128.0.0`.

♦ `Default_gateway` – this is the default gateway IP that will be assigned to the switch. An example default Gateway IP is `10.254.254.253`.

♦ # – Remark. When placed as the first character on a line, the entire line will be ignored by the switch. This allows items to be labeled, or unused commands to remain in the file so that the syntax will not be forgotten.

Notes about the Configuration File:

This configuration file can only contain 4 settings: `Code_type`, `Ip_addr`, `Subnet_mask` and `Default_gateway`.

Each command can only appear once in the configuration file.

If both the Firmware Update and Use Configuration file options are enabled, the Firmware Update command will take precedence and only the firmware file will be uploaded to the switch.

The Config image file, which contains all configuration settings and was created by the switch is prefixed with the version number of the runtime software to help with file management.

```
# Sample Config File

Code_type=PROM
Image_file="e:\3326\3326prom.tfp"

# specify IP address
Ip_addr = 10.12.19.102

# specify subnet mask
Subnet_mask = 255.0.0.0

# specify default gateway
Default_gateway = 10.1.1.254
```

D

RUNTIME SWITCHING SOFTWARE DEFAULT SETTINGS

Load Mode	Ethernet
Switch Operation Mode	Layer 2
Configuration update	Disable
Firmware update	Disable
Configuration file name	None
Firmware file name	None
Out-of-band baud rate	9600
RS232 mode	Console
IP address	10.90.90.90
Subnet mask	255.0.0.0
Default Gateway	0.0.0.0
BootP service	Disable
TFTP server IP address	0.0.0.0
IGMP Snooping	Disable
Console time out	10 min
User name	None
Password	None
Device STP	Enable
Port STP	Enable
Port enable	Enable
Bridge max age	20 secs
Bridge hello time	2 sec
Bridge forward delay	15 sec

Bridge priority	32768
Port STP cost	19 (Gigabit=4)
Port STP priority	128
Forwarding table aging time	300 secs
Nway	Enable
Flow control	Disable
Broadcast storm rising threshold	128Kpps
Community string	"public", "private"
VLAN mode	IEEE 802.1Q
SNMP VLAN(802.1Q)	1
Default port VID	1
Ingress rule checking	Disable
Mirror	disable

E

UNDERSTANDING AND TROUBLESHOOTING THE SPANNING TREE PROTOCOL

When the spanning-tree algorithm determines a port should be transitioned to the forwarding state, the following occurs:

- The port is put into the listening state where it receives BPDUs and passes them to the switch's CPU. BPDU packets from the CPU are processed. If no BPDUs that suggest the port should go to the blocking state are received:
- The port waits for the expiration of the forward delay timer. It then moves to the learning state.
- In the learning state, the port learns station location information from the source address of packets and adds this information to its forwarding database.
- The expiration of forwarding delay timer moves the port to the forwarding state, where both learning and forwarding are enabled. At this point, packets are forwarded by the port.

Blocking State

A port in the blocking state does not forward packets. When the switch is booted, a BPDU is sent to each port in the switch putting these ports into the blocking state. A switch initially assumes it is the root, and then begins the exchange of BPDUs with other switches. This will determine which switch in the network is the best choice for the root switch. If there is only one switch on the network, no BPDU exchange occurs, the forward delay timer expires, and the ports move to the listening state. All STP enabled ports enter the blocking state following switch boot.

A port in the blocking state does the following:

- Discards packets received from the network segment to which it is attached.
- Discards packets sent from another port on the switch for forwarding.
- Does not add addresses to its forwarding database
- Receives BPDUs and directs them to the CPU.
- Does not transmit BPDUs received from the CPU.
- Receives and responds to network management messages.

Network Segment
Port 1
Forwarding
Addresses
BPDUs
Network
Management
Packets
Data
Packets
Forwarding
Database
CPU
Switching
Fabric
Discard
BPDUs
Data
Packets
Port 2
Blocking
Network Segment

Listening State

The listening state is the first transition for a port from the blocking state. Listening is an opportunity for the switch to receive BPDUs that may tell the switch that the port should not continue to transition to the forwarding state, but should return to the blocking state (that is, a different port is a better choice).

There is no address learning or packet forwarding from a port in the listening state.

A port in the listening state does the following:

- Discards frames received from the network segment to which it is attached.
- Discards packets sent from another port on the switch for forwarding.
- Does not add addresses to its forwarding database
- Receives BPDUs and directs them to the CPU.
- Processes BPDUs received from the CPU.
- Receives and responds to network management messages.

Network Segment
Port 1
Forwarding
Addresses
BPDUs
Network
Management
Packets
Data
Packets
Forwarding
Database
CPU
Switch
Fabric
Discard
BPDUs
Data
Packets
Port 2
Listening
BPDUs
Network Segment

Learning State

A port in the learning state prepares to participate in frame forwarding. The port enters the learning state from the listening state.

A port in the learning state does the following:

- Discards frames received from the network segment to which it is attached.
- Discards packets sent from another port on the switch for forwarding.
- Adds addresses to its forwarding database.
- Receives BPDUs and directs them to the CPU.
- Processes and transmits BPDUs received from the CPU.
- Receives and responds to network management messages.

Network Segment
Port 1
Forwarding
Addresses
BPDUs
Network
Management
Packets
Data
Packets
Forwarding
Database
CPU
Switch
Fabric
Discard
Addresses
BPDUs
Data
Packets
Port 2
Learning
BPDUs
Network Segment

Forwarding State

A port in the forwarding state forwards packets. The port enters the forwarding state from the learning state when the forward delay timer expires.

A port in the forwarding state does the following:

- Forwards packets received from the network segment to which it is attached.
- Forwards packets sent from another port on the switch for forwarding.
- Incorporates station location information into its address database.
- Receives BPDUs and directs them to the system CPU.
- Receives and responds to network management messages.

Network Segment
Port 1
Forwarding
Addresses
BPDUs
Network
Management
Packets
Data
Packets
Forwarding
Database
CPU
Switch
Fabric
Addresses
BPDUs
Port 2
Learning
Network Segment

Disabled State

A port in the disabled state does not participate in frame forwarding or STP. A port in the disabled state is virtually non-operational.

A disabled port does the following:

- Discards packets received from the network segment to which it is attached.
- Discards packets sent from another port on the switch for forwarding.
- Does not add addresses to its forwarding database.
- Receives BPDUs, but does not direct them to the system CPU.
- Does not receive BPDUs for transmission from the system CPU.
- Receives and responds to network management messages.

Network Segment
Port 1
Forwarding
Addresses
BPDUs
Network
Management
Packets
Data
Packets
Forwarding
Database
CPU
Switch
Fabric
Discard
BPDUs
Data
Packets
Port 2
Learning
Network Segment

Troubleshooting STP

Spanning Tree Protocol Failure

A failure in the STA generally leads to a bridging loop. A bridging loop in an STP environment comes from a port that should be in the blocking state, but is forwarding packets.

In this example, B has been elected as the designated bridge and port 2 on C is in the blocking state. The election of B as the designated bridge is determined by the exchange of BPDUs between B and C. B had a better BPDU than C. B continues sending BPDUs advertising its superiority over the other bridges on this LAN. Should C fail to receive these BPDUs for longer than

the MAX AGE (default of 20 seconds), it could start to transition its port 2 from the blocking state to the forwarding state.

It should be noted: A port must continue to receive BPDUs advertising superior paths to remain in the blocking state.

There are a number of circumstances in which the STA can fail – mostly related to the loss of a large number of BPDUs. These situations will cause a port in the blocking state to transition to the forwarding state.

Full/Half Duplex Mismatch

A mismatch in the duplex state of two ports is a very common configuration error for a point-to-point link. If one port is configured as a full duplex, and the other port is left in auto-negotiation mode, the second port will end up in half-duplex because ports configured as half- or full-duplex do not negotiate.

In the above example, port 1 on B is configured as a full-duplex port and port 1 on A is either configured as a half-duplex port, or left in auto-negotiation mode. Because port 1 on B is configured as a full-duplex port, it does not do the carrier sense when accessing the link. B will then start sending packets even if A is using the link. A will then detect collisions and begin to run the flow control algorithm. If there is enough traffic between B and A, all packets (including BPDUs) will be dropped. If the BPDUs sent from A to B are dropped for longer than the MAX AGE, B will lose its connection to the root (A) and will unblock its connection to C. This will lead to a data loop.

Unidirectional Link

Unidirectional links can be caused by an undetected failure in one side of a fiber cable, or a problem with a ports transceiver. Any

failure that allows a link to remain up while providing one-way communication is very dangerous for STP.

In this example, port 2 on B can receive but not transmit packets. Port 2 on C should be in the blocking state, but since it can no longer receive BPDUs from port 2 on B, it will transition to the forwarding state. If the failure exists at boot, STP will not converge and rebooting the bridges will have no effect. (Note: Rebooting would help temporarily in the previous example).

This type of failure is difficult to detect because the Link-state LEDs for Ethernet links rely on the transmit side of the cable to detect a link. If a unidirectional failure on a link is suspected, it is usually required to go to the console or other management software and look at the packets received and transmitted for the port. A unidirectional port will have many packets transmitted but none received, or vice versa, for example.

Packet Corruption

Packet corruption can lead to the same type of failure. If a link is experiencing a high rate of physical errors, a large number of consecutive BPDUs can be dropped and a port in the blocking state would transition to the forwarding state. The blocking port would have to have the BPDUs dropped for 50 seconds (at the default settings) and a single BPDU would reset the timer. If the MAX AGE is set too low, this time is reduced.

Resource Errors

The DES-3326 Layer 3 switch performs its switching and routing functions primarily in hardware, using specialized ASICs. STP is implemented in software and is thus reliant upon the speed of the CPU and other factors to converge. If the CPU is over-utilized, it is possible that BPDUs may not be sent in a timely fashion. STP is generally not very CPU intensive and is given priority over other processes, so this type of error is rare.

It can be seen that very low values for the MAX AGE and the FORWARD DELAY can result in an unstable spanning tree. The loss of BPDUs can lead to data loops. The diameter of the network can also cause problems. The default values for STP give a maximum network diameter of about seven. This means that two switches in the network cannot be more than seven hops apart. Part of this diameter restriction is the BPDU age field. As BPDUs are propagated from the root bridge to the leaves of the spanning tree, each bridge increments the age field. When this field is beyond the maximum age, the packet is discarded. For large diameter networks, STP convergence can be very slow.

Identifying a Data Loop

Broadcast storms have a very similar effect on the network to data loops, but broadcast storm controls in modern switches have (along with subnetting and other network practices) have been very effective in controlling broadcast storms. The best way to determine if a data loop exists is to capture traffic on a saturated link and check if similar packets are seen multiple times.

Generally, if all the users of a given domain are having trouble connecting to the network at the same time, a data loop can be suspected. The port utilization data in the switch's console will give unusually high values in this case.

The priority for most cases is to restore connectivity as soon as possible. The simplest remedy is to manually disable all of the ports that provide redundant links. Disabling ports one at a time, and then checking for a restoration of the user's connectivity will identify the link that is causing the problem, if time allows. Connectivity will be restored immediately after disabling a data loop.

Avoiding Trouble

Know where the root is located.

Although the STP can elect a root bridge, a well-designed network will have an identifiable root for each VLAN. Careful setup of the STP parameters will lead to the selection of this best switch as the root for each VLAN. Redundant links can then be built into the network. STP is well suited to maintaining connectivity in the event of a device failure or removal, but is poorly suited to designing networks.

Know which links are redundant.

Organize the redundant links and tune the port cost parameter of STP to force those ports to be in the blocking state.

For each VLAN, know which ports should be blocking in a stable network. A network diagram that shows each physical loop in the network and which ports break which loops is extremely helpful.

Minimize the number of ports in the blocking state.

A single blocking port transitioning to the forwarding state at an inappropriate time can cause a large part of a network to fail. Limiting the number of blocked ports help to limit the risk of an inappropriate transition.

This is a common network design. The switches C and D have redundant links to the backbone switches A and B using trunks. Trunks, by default, carry all the VLAN traffic from VLAN 1 and VLAN 2. So switch C is not only receiving traffic for VLAN 1, but it is also receiving unnecessary broadcast and multicast traffic for VLAN 2. It is also blocking one port for VLAN 2. Thus, there are three redundant paths between switches A and B and two blocked ports per VLAN. This increases the chance of a data loop.

In this example, the VLAN definitions are extended to switches A and B. This gives only a single blocked port per VLAN and allows the removal of all redundant links by removing switch A or B from the network.

Impact of Layer 3 Switching.

The IP routing operational mode of the DES-3326 Layer 3 switch can accomplish the following:

- Building a forwarding table, and exchanging information with its peers using routing protocols.
- Receiving packets and forwarding them to the correct interface based upon their destination address

With layer 3 switching, there is no performance penalty to introducing a routing hop and creating an additional segment of the network.

Using layer 3 switches and IP routing eliminates the need for STP port blocking because the packets are routed by destination addresses. The link redundancy remains, and relying on the routing protocols gives a faster convergence than with STP.

The drawback is that the introduction of layer 3 switching usually requires a new addressing scheme.

E

BRIEF REVIEW OF BITWISE LOGICAL OPERATIONS

AND

The logical AND operation compares 2 bits and if they are both "1", then the result is "1", otherwise, the result is "0".

	0	*1*
0	0	0
1	0	1

OR

The logical OR operation compares 2 bits and if either or both bits are "1", then the result is "1", otherwise, the result is "0".

	0	*1*
0	0	1
1	1	1

XOR

The logical XOR (exclusive OR) operation compares 2 bits and if exactly one of them is a "1", then the result is "1", otherwise the result is "0".

	0	***1***
0	0	1
1	1	0

NOT

The logical NOT operation simply changes the value of a single bit. If it is a "1", the result is "0", if it is a "0", the result is "1". This operation is carried out on a single bit.

0	***1***
1	0

INDEX

1

1000BASE-SX Gigabit Module.... 22
100BASE-FX Fiber (MTRJ Type) Module..... 21
100BASE-FX Fiber Module..... 20
100BASE-TX Device..... 27
100BASE-TX Module 20
10BASE-T Device 26

8

802.1Q Static VLANs 256

A

AC inputs..... 352
AC power cord 12
Accessory pack..... 12
Add a Static 802.1Q VLAN 311
Add a Static Router Port..... 310
Add an STP Group 285
Add IP Interface 276
Address Table..... 253, 332
Administrator..... 121
Aging Time, definition of..... 36
Aging Time, range of..... 36
Applications..... 337
APPLY 119
ARP Table..... 257
Auto polarity detection..... 7
Automatic learning..... 37
auto-negotiate..... 6

B

Baud Rate..... 140
BOOTP protocol..... 136
Bootp Relay..... 257
BOOTP server 136
BOOTP/DHCP Relay..... 321
Bridge Forward Delay 46
Bridge Hello Time..... 45, 205
Bridge Max. Age 45, 204
Bridge Priority..... 45, 205, 284
broadcast domains..... 53
Broadcast storms..... 65
Broadcast/Multicast Storm Mode272
Browse IGMP Snooping Table .. 340
Browse IGMP Table 343
Browse IP Address Sequentially 257
Browse IP Address Table 333
Browse IP Multicast Forwarding Table..... 342
Browse MAC Address Sequentially 257
Browse MAC Address Table 332
Browse Router Port 257
Browse the ARP Table 336
Browse the Router Port Table .. 339
Browse the Routing Table..... 334

C

Changing your Password..... 128
Coll..... 330
Community Name 31
Community Strings..... 255
Configuration 133
Configuration Files 346
Configure IP Address 135
Configure STP Groups 256
Connecting to the Switch
VT100-compatible terminal... 118
Connections
Switch to End Node 24
Switch to Hub or Switch..... 25
console 114, 119
Console..... 23
console port..... 6, 17

Console port (RS-232 DCE)..... 29
Console port settings..... 29
Console Settings..... 268
Console Timeout 140
Cost to Root 287
CRC Error..... 328, 329
Create/Modify User Accounts ... 128
crossover cable..... 26
Crossover cable..... 355

D

Data filtering..... 7
Data filtering rate 7
Data forwarding 7
Data forwarding rate..... 7
Default Gateway..... 137, 249
Designated Root Bridge 287
Diagnostic port 6
Dimensions 352
DNS Relay 257
Drop Pkts..... 329
DVMRP..... 274
DVMRP Incld. Report 274
DVMRP Settings 256
Dynamic filtering 37

E

Edit 802.1Q VLANs..... 313
Edit IP Interface..... 277
Edit RIP Setup 279
Edit STP Group Settings..... 286
Egress 313
Egress port 53
Eliminating Broadcast Storms.... 66
End Node 24
Enterasys WebView User Interface
..... 252
Ethernet protocol..... 11
Ex. Coll. 330
ExDefer..... 329

F

factory reset..... 126
Factory Reset..... 257
Filter Address Table..... 296
Filtering..... 36, 294
Flash memory..... 9
Forward Delay..... 283
Forwarding 35, 289
Fragments 329
Front Panel..... 17
Full-duplex 6

G

gateway router 31
General User 123, 244
Gigabit Ethernet 11
GMRP 273
Group Name 287, 289
GVRP 273

H

half-duplex..... 6
Hello Interval 308
Hello Time 283
Humidity 352

I

IEEE 802.1Q Multicast Forwarding
..... 256, 302
IEEE 802.1Q tagging 53
IEEE 802.1Q VLANs..... 53, 311
IGMP 254
IGMP Settings..... 256, 305
IGMP Snooping 273
Illustration of STA 46
Ingress port..... 53, 59
IP Address 30
IP Address Filter 295
IP Address Filtering..... 256
IP Addresses and SNMP
Community Names..... 30
IP Configuration..... 135, 261

J

Jabbers 329
Join/Prune Interval..... 309

L

Last Topology Change..... 287
Late Coll. 329
Layer 2 Switch Settings.... 255, 271

Layer 3 IP Routing Protocol Settings..... 255, 274
LED Indicators 22
load-balancing 51
log in 128
Logging on 119

M

MAC Address Aging Time..... 272
MAC address filtering 37
MAC Address Forwarding..... 256
MAC Address Learning..... 353
MAC Filtering 256
MAC-based VLANs 53
Main Menu .121, 122, 125, 126, 127
Management..... 9
Management Information Base (MIB) 33
Management Station IP Settings 255, 264
master port 49
Max Age 282
Max. Age 45, 204, 205
Metric..... 292
MIB 33
MIB objects..... 33
MIB-II 33
MIB-II (RFC 1213) 9
MIBs 33
Mirror 254
Mirror Port Configuration 300
Mirroring 299
module 6, 18
Modules 19
Multicast Interface Configuration 256

N

Network Classes
Class A, B, C for Subnet Mask137
NV-RAM 125, 246
NWay 6

O

Operating Temperature 352
Out-of-Band/Console Setting menu 140
Oversize 329

P

password 120, 247
PIMDM 274
PIMDM Settings..... 256
Port Configuration 280
Port Cost..... 288
Port Error 256
Port Error Statistics..... 328
Port GMRP Settings..... 318
Port GVRP Settings 256
Port Ingress Filter..... 256, 316
Port Mirroring Settings 256
Port Packet Analysis..... 256, 327
Port Priority 46, 207, 288
Port Trunking..... 49, 319
Port Utilization 257
Port Utilization Statistics 330
Port VLAN ID (PVID) 256, 314, 315
port-based VLANs 53
ports..... 6
Power 23
Power Consumption 352
Priority 253, 297

R

RAM..... 124, 245
RAM Buffer 353
Rear Panel 18, 19
refresh 119
Restart System 257
RIP 274
RJ-45 Pin Specification 354
Root Priority 287
Routing Table 257
RS-232 6

S

Save Changes..... 119
Save History Log to Server 257
Save Settings to Server..... 257
Save Switch History to TFTP Server 348

Save Switch Settings to a TFTP Server 347
Saving Changes 124, 245
Screen Hierarchy..... 255
security 31, 53
Segmenting Broadcast Domains . 66
Serial Port Settings 255, 267
Setting an IP Address 248
Setting the Administrator Password 249
Setting Trap Destinations..... 249
Setting Up The Switch 132
Setting Up Web Management... 247
Setup..... 13
Setup IP Interface 275
Setup IP Interfaces..... 255
Setup RI 255
Setup RIP 278
Single Coll 330
SLIP management..... 141
Slip Settings 269
SNMP 253
SNMP Community Strings 265
SNMP Configuration (Community Strings)..... 265
Spanning Tree Algorithm 9
Spanning Tree Algorithm (STA) . 38
Spanning Tree Groups 284
Spanning Tree Protocol37, 253, 282
Spanning Tree Protocol Configuration 282
Static / Default Routes 290
Static / Default Routes – Add.... 291
Static ARP 292
Static ARP – Add..... 293
Static Bootp Relay Setup .. 257, 323
Static Router Port Settings256, 309
Static/Default Routes 256
Statistics 254, 327
Status..... 288
Storage Temperature 352
Store and forward switching..... 6
STP 253
STP Port Settings..... 256, 287
STP Switch Settings..... 256
straight cable..... 355
Subnet Mask..... 137
Super User..... 123, 244
Switch History..... 257, 338
Switch Operation Mode..... 255, 270
System Information..... 258

T

Tag 312
tagging 54
Tagging 53
Target Port Selection 256, 300
TCP/IP Settings..... 135
TELNET 114
terminal emulator 118
terminal parameters 118
Third-party vendors' SNMP software..... 34
Topology Change Count 287
Transmission Methods..... 353
Trap managers 32
Trap Receivers..... 255, 266
Trap Type
Authentication Failure 33
Cold Start..... 32
Link Change Event..... 33
New Root..... 33
Topology Change..... 33
Warm Start 32
Traps..... 32
trunk group 49

U

unauthorized users..... 119
Undersize..... 328
Unpacking 12
untagging..... 53
Untagging..... 53
Update Firmware from Server . 257
Uplink 18, 26
Upper Threshold for Base Ports273
Upper Threshold for Module Ports 273
Use Configuration File on Server257
User Accounts Management 129
User Accounts Table 255
username 120
Utilities..... 345

V

View/Delete User Accounts..... 130
VLAN 37, 51, 254
VLANs 311
VT100-compatible terminal 118

W

web-based management..... 238
Web-based management module238
Weight 353

D-Link® Offices

AUSTRALIA **D-LINK AUSTRALASIA**
Unit 16, 390 Eastern Valley Way, Roseville, NSW 2069, Australia
TEL: 61-2-9417-7100 FAX: 61-2-9417-1077
TOLL FREE: 1800-177-100 (Australia), 0800-900900 (New Zealand)
WEB: www.dlink.com.au E-MAIL: info@dlink.com.au

CANADA **D-LINK CANADA**
2180 Winston Park Drive, Oakville, Ontario L6H 5W1 Canada
TEL: 1-905-829-5033 FAX: 1-905-829-5223
WEB: www.dlink.ca FTP: ftp.dlinknet.com E-MAIL: techsup@dlink.ca

CHILE **D-LINK SOUTH AMERICA**
Isidora Goyenechea #2934 of.702, Las Condes, Santiago, Chile
TEL: 56-2-2323185 FAX: 56-2-2320923 WEB: www.dlink.cl

CHINA **D-LINK CHINA**
15th Floor, Science & Technology Tower,
No. 11, Baishiqiao Road, Haidian District, Beijing 100081 China
TEL: 86-10-68467106-9 FAX: 86-10-68467110 WEB: www.dlink.co.cn

DENMARK **D-LINK DENMARK**
Naverland 2, DK-2600 Glostrup, Copenhagen, Denmark
TEL:45-43-969-040 FAX:45-43-424-347 WEB: www.dlink.dk

EGYPT **D-LINK MIDDLE EAST**
7 Assem Ebn Sabet Street, Heliopolis Cairo, Egypt
TEL: 202-2456176 FAX: 202-2456192 WEB: www.dlink-me.com

FRANCE **D-LINK FRANCE**
Le FLORILEGE #2, Allee de la Fresnerie
78330 Fontenay Le Fleury France
TEL: 33-1-3023-8688 FAX: 33-1-3023-8689
WEB: www.dlink-france.fr E-MAIL: info@dlink-france.fr

GERMANY **D-LINK GERMANY**
Bachstr. 22, D/65830 Kriftel Germany
TEL: 49-(0)6192-97110 FAX: 49-(0)6192-971111
WEB: www.dlink.de BBS: 49-(0)6192-971199 (Analog) 49-(0)6192-9711 98 (ISDN)
INFO: 00800-7250-0000 (toll free) HELP: 00800-7250-4000 (toll free)

INDIA **D-LINK INDIA**
Plot No.5, Kurla-Bandra Complex Road,
Off Cst Road, Santacruz (E), Bombay - 400 098 India
TEL: 91-22-6526578 FAX: 91-22-6528476 WEB: www.dlink.india.com

ITALY **D-LINK ITALY**
Via Nino Bonnet No. 6, 20154 Milano, Italy
TEL: 39-2-2900-0676 FAX: 39-2-2900-1723 E-Mail: dlink@tin.it

JAPAN **D-LINK JAPAN**
10F, 8-8-15 Nishi-Gotanda, Shinagawa-ku, Tokyo 141 Japan
TEL: 81-3-5434-9678 FAX: 81-3-5434-9868 WEB: www.d-link.co.jp

SINGAPORE **D-LINK INTERNATIONAL**
1 International Business Park, #03-12 The Synergy, Singapore 609917
TEL: 65-774-6233 FAX: 65-774-6322
WEB: www.dlink.intl.com E-MAIL: info@dlink.com.sg

SWEDEN **D-LINK SWEDEN**
World Trade Centre P. O. Box 70396, 107 24 Stockholm Sweden

TEL: 46-8-700-6211 FAX: 46-8-219-640 E-MAIL: info@dlink.se

TAIWAN **D-LINK TAIWAN**
2F, No. 119 Pao-Chung Road, Hsin-Tien, Taipei, Taiwan
TEL: 886-2-2910-2626 FAX: 886-2-2910-1515 WEB: www.dlinktw.com.tw

U.K. **D-LINK EUROPE**
D-Link House, 6 Garland Road, Stanmore, London HA7 1DP U.K.
TEL: 44-181-235-5555 FAX: 44-181-235-5500
WEB: www.dlink.co.uk E-MAIL: info@dlink.co.uk

U.S.A. **D-LINK U.S.A.**
53 Discovery Drive, Irvine, CA 92618 USA
TEL: 1-949-788-0805 FAX: 1-949-753-7033
WEB: www.dlink.com E-MAIL: tech@dlink.com

Registration Card

Print, type or use block letters.

Your name: Mr./Ms_____
Organization: _____Dept. _____
Your title at organization: _____
Telephone:_____ Fax:_____
Organization's full address: _____
_____
Country: _____
Date of purchase (Month/Day/Year): _____

Product Model	Product Serial No.	* Product installed in type of computer (e.g., Compaq 486)	* Product installed in computer serial No.

(* Applies to adapters only)

Product was purchased from:
Reseller's name: _____
Telephone:_____ Fax:_____
Reseller's full address: _____
_____
_____

Answers to the following questions help us to support your product:

1. Where and how will the product primarily be used?
☐Home ☐Office ☐Travel ☐Company Business ☐Home Business ☐Personal Use

2. How many employees work at installation site?
☐1 employee ☐2-9 ☐10-49 ☐50-99 ☐100-499 ☐500-999 ☐1000 or more

3. What network protocol(s) does your organization use ?
☐XNS/IPX ☐TCP/IP ☐DECnet ☐Others_____

4. What network operating system(s) does your organization use ?
☐D-Link LANsmart ☐Novell NetWare ☐NetWare Lite ☐SCO Unix/Xenix ☐PC NFS ☐3Com 3+Open
☐Banyan Vines ☐DECnet Pathwork ☐Windows NT ☐Windows NTAS ☐Windows '95
☐Others_____

5. What network management program does your organization use ?
☐D-View ☐HP OpenView/Windows ☐HP OpenView/Unix ☐SunNet Manager ☐Novell NMS
☐NetView 6000 ☐Others_____

6. What network medium/media does your organization use ?
☐Fiber-optics ☐Thick coax Ethernet ☐Thin coax Ethernet ☐10BASE-T UTP/STP
☐100BASE-TX ☐100BASE-T4 ☐100VGAnyLAN ☐Others_____

7. What applications are used on your network?

☐Desktop publishing ☐Spreadsheet ☐Word processing ☐CAD/CAM
☐Database management ☐Accounting ☐Others_____

8. What category best describes your company?

☐Aerospace ☐Engineering ☐Education ☐Finance ☐Hospital ☐Legal ☐Insurance/Real Estate ☐Manufacturing
☐Retail/Chainstore/Wholesale ☐Government ☐Transportation/Utilities/Communication ☐VAR
☐System house/company ☐Other_____

9. Would you recommend your D-Link product to a friend?

☐Yes ☐No ☐Don't know yet

10.Your comments on this product?

_____

_____

PLEASE
PLACE STAMP
HERE

TO:

D-Link®