

XSTACK[®]

USER MANUAL

PRODUCT MODEL: **xStack**[®] **DES-6500**

MODULAR LAYER 3 CHASSIS ETHERNET SWITCH

RELEASE 3.6

Information in this document is subject to change without notice.

© 2008 D-Link Corporation. All rights reserved.

Reproduction in any manner whatsoever without the written permission of D-Link Computer Corporation is strictly forbidden.

Trademarks used in this text: D-Link and the D-LINK logo are trademarks of D-Link Computer Corporation; Microsoft and Windows are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. D-Link Computer Corporation disclaims any proprietary interest in trademarks and trade names other than its own.

November 2008 P/N 6DES6500..10

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 manual, 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 their 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.

Warnung!

Dies ist ein Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstörungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!

Este es un producto de Clase A. En un entorno doméstico, puede causar interferencias de radio, en cuyo caso, puede requerirse al usuario para que adopte las medidas adecuadas.

Attention!

Ceci est un produit de classe A. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l'utilisateur devrait prendre les mesures adéquates.

Attenzione!

Il presente prodotto appartiene alla classe A. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l'utente debba assumere provvedimenti adeguati.

VCCI Warning

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA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。

Table of Contents

Preface	xii
Intended Readers.....	xiii
Typographical Conventions.....	xiii
Notes, Notices, and Cautions.....	xiii
Safety Instructions.....	xiv
Safety Cautions.....	xiv
General Precautions for Rack-Mountable Products.....	xv
Protecting Against Electrostatic Discharge.....	xvi
Introduction	1
Switch Description.....	1
Features.....	1
DES-6504 12-port 100BASE-FX (SFF) Fast Ethernet Switch module.....	3
DES-6505 8-port 1000BASE-SX (SC) Gigabit Ethernet Switch module.....	3
DES-6506 Patch Panel.....	3
DES-6507 12-port 10BASE-T/100BASE-TX/1000BASE-T Switch module.....	3
DES-6508 16-port 10BASE-T/100BASE-TX Fast Ethernet Switch module.....	4
DES-6509 12-port Mini GBIC (SFP) switch module.....	4
DES-6510 RJ21 connectors provide 24-port 10BASE-T/100BASE-TX Fast Ethernet Switch module.....	4
DES-6511 Power Supply Modules.....	4
DES-6512 2-port 10 GE XFP Switch Module.....	4
Ethernet Technology.....	5
Fast Ethernet.....	5
Gigabit Ethernet Technology.....	5
Switching Technology.....	5
Front-Panel Components and LED Indicators.....	6
Installation	7
Package Contents.....	7
Before You Connect to the Network.....	7
Installing the Switch without the Rack.....	8
Installing the Switch in a Rack.....	8
Mounting the Switch in a Standard 19" Rack.....	9
Power On.....	9
Power Failure.....	9
External Redundant Power System.....	9
Connecting the Switch	10
Switch to End Node.....	10
Switch to Hub or Switch.....	11
Using the xStack [®] DES-6500 Layer 3 modular chassis Ethernet switch as a Network Backbone.....	12
Introduction to Switch Management	13
Management Options.....	13
Web-based Management Interface.....	13

SNMP-Based Management.....	13
Command Line Console Interface through the Serial Port.....	13
Connecting the Console Port (RS-232 DCE).....	13
First Time Connecting to the Switch.....	14
Password Protection.....	16
SNMP Settings.....	17
Traps.....	17
MIBs.....	17
IP Address Assignment.....	18
Connecting Devices to the Switch.....	19
Introduction to Web-based Switch Configuration	20
Introduction.....	20
Logging on to the Web Manager.....	20
Web-based User Interface.....	21
Areas of the User Interface.....	21
Web Pages.....	23
Configuring the Switch.....	24
Switch Information.....	25
Switch IP Settings.....	26
Setting the Switch's IP Address using the Console Interface.....	27
Advanced Settings.....	28
Port Configuration.....	30
Port Mirroring Configuration.....	32
Link Aggregation.....	33
Understanding Port Trunk Groups.....	33
LACP Port Settings.....	36
IGMP Snooping.....	37
Static Router Port Settings.....	39
Spanning Tree.....	40
802.1s MSTP.....	40
802.1w Rapid Spanning Tree.....	40
Port Transition States.....	41
Edge Port.....	41
P2P Port.....	41
802.1d / 802.1w / 802.1s Compatibility.....	41
STP Loopback Detection.....	42
STP Bridge Global Settings.....	43
MST Configuration Identification.....	45
MSTP Port Information.....	48
STP Instance Settings.....	49
STP Port Settings.....	51
Forwarding & Filtering.....	53
Unicast Forwarding.....	53
Static Multicast Forwarding.....	53

VLANs.....	55
Understanding IEEE 802.1p Priority.....	55
VLAN Description.....	55
Notes about VLANs in the xStack® DES-6500 Modular Layer 3 Chassis Ethernet Switch	55
IEEE 802.1Q VLANs	56
802.1Q VLAN Tags.....	57
Port VLAN ID	58
Tagging and Untagging	58
Ingress Filtering.....	58
Default VLANs.....	59
Port-based VLANs.....	59
VLAN Segmentation	59
VLAN and Trunk Groups.....	60
Protocol VLANs	60
VLAN Entry	61
GVRP Settings.....	64
Traffic Control	65
Port Security.....	68
Port Lock Entries	69
QoS	70
The Advantages of QoS	70
Understanding QoS.....	71
Bandwidth Control.....	72
QoS Scheduling Mechanism	73
QoS Output Scheduling	74
Configuring the Combination Queue.....	75
802.1p Default Priority	76
802.1p User Priority.....	76
Traffic Segmentation.....	77
System Log Server.....	79
System Severity Log	81
SNTP Settings.....	82
Time Settings.....	82
Time Zone and DST	83
Access Profile Table	85
Configuring the Access Profile Table	86
CPU Interface Filtering.....	99
CPU Interface Filtering State Settings	99
CPU Interface Filtering Table.....	99
Safeguard Engine	109
Port Access Entity (802.1X).....	111
802.1x Port-Based and MAC-Based Access Control.....	111
Authentication Server	112
Authenticator	112

Client	112
Authentication Process	113
Understanding 802.1x Port-based and MAC-based Network Access Control	114
Port-Based Network Access Control	114
MAC-Based Network Access Control	115
802.1x Auth Mode Settings	115
802.1X Authenticator Settings	116
Local Users	118
PAE System Control	119
Port Capability	119
Initializing Ports for Port Based 802.1x	120
Initializing Ports for MAC Based 802.1x	121
Reauthenticate Port(s) for Port Based 802.1x	121
Reauthenticate Port(s) for MAC-based 802.1x	122
RADIUS Server	123
Layer 3 IP Networking	124
Layer 3 Global Advanced Settings	124
IP Multinetting	125
IP Interface Setup	125
MD5 Key Configuration	128
Route Redistribution Settings	129
Static/Default Route Settings	130
Static ARP Table	132
RIP	133
RIP Global Configuration	134
RIP Settings	135
OSPF	136
OSPF General Settings	153
OSPF Area ID Settings	153
OSPF Interface Settings	154
OSPF Virtual Interface Settings	157
OSPF Area Aggregation Settings	159
OSPF Host Route Settings	160
IP Multicast Routing Protocol	161
IGMP	161
IGMP Versions 1 and 2	161
IGMP Version 3	162
IGMP Interface Configuration	164
DVMRP Interface Configuration	165
DVMRP Configuration	165
DVMRP Interface Settings	165
PIM Protocol	167
PIM-SM	167
Discovering and Joining the Multicast Group	167
Distribution Trees	167

Register and Register Suppression Messages	167
Assert Messages.....	168
PIM-DM Interface Configuration	168
PIM Global Settings.....	168
PIM Interface Settings	168
PIM Candidate BSR Settings.....	170
PIM Parameter Settings	171
PIM Candidate RP Global Settings.....	172
PIM Candidate RP Settings.....	172
PIM Register Checksum Settings.....	173
PIM Static RP Settings.....	174
DNS Relay	175
DNS Relay Information.....	175
DNS Relay Static Settings	176
DHCP / BOOTP Relay	177
DHCP Auto Configuration Settings.....	177
DHCP / BOOTP Relay Information	177
DHCP/BOOTP Relay Settings	178
DHCP Relay Option 82 Settings.....	178
VRRP	180
VRRP Global Settings	180
VRRP Virtual Router Settings.....	181
VRRP Authentication Settings	184
Security Management.....	185
Security IP.....	185
User Account Management.....	185
Admin and User Privileges	186
Secure Shell (SSH).....	187
SSH Configuration.....	187
SSH Algorithm.....	188
SSH User Authentication Mode.....	190
Access Authentication Control.....	191
Authentication Policy & Parameters	192
Application's Authentication Settings	193
Authentication Server Group	194
Authentication Server Host.....	195
Login Method Lists.....	196
Enable Method Lists	197
Local Enable Password	199
Enable Admin	199
Secure Socket Layer (SSL)	201
Download Certificate	201
Configuration.....	202
SNMP Manager.....	204

SNMP Settings.....	204
SNMP Trap Settings.....	205
SNMP User Table.....	205
SNMP View Table.....	207
SNMP Group Table.....	208
SNMP Community Table.....	210
SNMP Host Table.....	211
SNMP Engine ID.....	212
Monitoring.....	213
CPU Utilization.....	214
Port Utilization.....	215
Packets.....	216
Received (RX).....	216
UMB Cast (RX).....	218
Transmitted (TX).....	220
Errors.....	222
Received (RX).....	222
Transmitted (TX).....	224
Size.....	226
Stacking Information.....	228
Device Status.....	229
MAC Address.....	230
Switch History Log.....	231
IGMP Snooping Group.....	232
IGMP Snooping Forwarding.....	233
Browse Router Port.....	234
Port Access Control.....	235
Authenticator State.....	235
Authenticator Diagnostics.....	237
Authenticator Session Statistics.....	239
Authenticator Statistics.....	241
RADIUS Account Client.....	243
RADIUS Auth Client.....	245
Layer 3 Feature.....	247
Browse IP Address Table.....	247
Browse Routing Table.....	248
Browse ARP Table.....	248
Browse IP Multicast Forwarding Table.....	249
Browse IP Multicast Interface Table.....	249
Browse IGMP Group Table.....	249
OSPF Monitor.....	250
Browse OSPF LSDB Table.....	250
Browse OSPF Neighbor Table.....	251
OSPF Virtual Neighbor.....	252

DVMRP Monitoring	253
Browse DVMRP Routing Table	253
Browse DVMRP Neighbor Table	254
Browse DVMRP Routing Next Hop Table	254
PIM Monitoring	255
Browse PIM Neighbor Table	255
PIM IP MRoute Table	255
Browse PIM RP Set Table	256
Switch Maintenance	257
TFTP Services	257
Download Firmware	257
Download Configuration	258
Upload Configuration	258
Upload History Log	258
Ping Test	259
Traceroute	259
Save Configuration	260
Reset	260
Reboot Device	260
Logout	261
D-Link Single IP Management	262
Single IP Management (SIM) Overview	262
SIM Using the Web Interface	263
Topology	265
Tool Tips	267
Right Click	267
Group Icon	268
Commander Switch Icon	268
Member Switch Icon	269
Candidate Switch Icon	270
Menu Bar	271
Group	271
Device	271
View	271
Firmware Upgrade	273
Configuration File Backup/Restore	273
Appendix A	274
Appendix B	276
Upgrading Instructions for Release 3 Firmware (R3.00.B33)	276
Line Card Firmware Compatibility	276
Precautions for Adding New Line Cards to the Chassis	276
Upgrading to R3.00-B33	277
Adding Runtime R1.01 DES-6505/DES-6507/DES-6509 Line Cards to the Runtime R1.3/1.4/2.0/2.5/3.0 Chassis	283

Firmware Downgrade Procedure	287
Appendix C	293
Cables and Connectors.....	293
Appendix D.....	294
Cable Lengths.....	294
Glossary	295
Tech Support.....	305

Preface

The *xStack® DES-6500 Modular Layer 3 Chassis Ethernet Switch User Manual* is divided into sections that describe the system installation and operating instructions with examples.

Section 1, Introduction - Describes the Switch and its features.

Section 2, Installation- Helps you get started with the basic installation of the Switch and also describes the front panel, rear panel, side panels, and LED indicators of the Switch.

Section 3, Connecting the Switch - Tells how you can connect the Switch to your Ethernet network.

Section 4, Introduction to Switch Management - Introduces basic Switch management features, including password protection, SNMP settings, IP address assignment and connecting devices to the Switch.

Section 5, Introduction to Web-based Switch Management - Talks about connecting to and using the Web-based switch management feature on the Switch.

Section 6, Configuring the Switch - A detailed discussion about configuring some of the basic functions of the Switch, including accessing the Switch information, using the Switch's utilities and setting up network configurations, such as Quality of Service, the Access Profile Table, port mirroring and configuring the Spanning Tree.

Section 7, Management - A discussion of the security features of the Switch, including Security IP, User Accounts, and Access Authentication Control.

Section 8, SNMP Manager – A detailed discussion regarding the Simple Network Monitoring Protocol including description of features and a brief introduction to SNMP.

Section 9, Monitoring - Features graphs and screens used in monitoring features and packets on the Switch.

Section 10, Maintenance - Features information on Switch utility functions, including TFTP Services, Switch History, Ping Test Save Changes and Rebooting Services.

Section 11, Single IP Management - Discussion on the Single IP Management function of the Switch, including functions and features of the Java based user interface and the utilities of the SIM function.

Appendix A, Technical Specifications - The technical specifications of the DES-6500.

Appendix B Upgrading Instructions for Release 3 Firmware (R3.00-B33) A detailed explanation about the latest firmware release and downloading instruction for the DES-6500.

Appendix C, Cables and Connectors - Describes the RJ-45 receptacle/connector, straight-through and crossover cables and standard pin assignments.

Appendix D, Cable Lengths - Information on cable types and maximum distances.

Glossary - Lists definitions for terms and acronyms used in this document.

Intended Readers

The *xStack® DES-6500 Modular Layer 3 Chassis Ethernet Switch User Manual* contains information for setup and management of the Switch. This manual is intended for network managers familiar with network management concepts and terminology.

Typographical Conventions

Convention	Description
[]	In a command line, square brackets indicate an optional entry. For example: [copy filename] means that optionally you can type copy followed by the name of the file. Do not type the brackets.
Bold font	Indicates a button, a toolbar icon, menu, or menu item. For example: Open the File menu and choose Cancel . Used for emphasis. May also indicate system messages or prompts appearing on your screen. For example: You have mail. Bold font is also used to represent filenames, program names and commands. For example: use the copy command.
Boldface Typewriter Font	Indicates commands and responses to prompts that must be typed exactly as printed in the manual.
Initial capital letter	Indicates a window name. Names of keys on the keyboard have initial capitals. For example: Click Enter.
<i>Italics</i>	Indicates a window name or a field. Also can indicate a variables or parameter that is replaced with an appropriate word or string. For example: type <i>filename</i> means that you should type the actual filename instead of the word shown in italic.
Menu Name > Menu Option	Menu Name > Menu Option Indicates the menu structure. Device > Port > Port Properties means the Port Properties menu option under the Port menu option that is located under the Device menu.

Notes, Notices, and Cautions



A **NOTE** indicates important information that helps you make better use of your device.




A **NOTICE** indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.



A **CAUTION** indicates a potential for property damage, personal injury, or death.

Safety Instructions

Use the following safety guidelines to ensure your own personal safety and to help protect your system from potential damage.

Throughout this safety section, the caution icon () is used to indicate cautions and precautions that you need to review and follow.



Safety Cautions

To reduce the risk of bodily injury, electrical shock, fire, and damage to the equipment, observe the following precautions.

- Observe and follow service markings.
 - Do not service any product except as explained in your system documentation.
 - Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose you to electrical shock.
 - Only a trained service technician should service components inside these compartments.
- If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your trained service provider:
 - The power cable, extension cable, or plug is damaged.
 - An object has fallen into the product.
 - The product has been exposed to water.
 - The product has been dropped or damaged.
 - The product does not operate correctly when you follow the operating instructions.
- Keep your system away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the system gets wet, see the appropriate section in your troubleshooting guide or contact your trained service provider.
- Do not push any objects into the openings of your system. Doing so can cause fire or electric shock by shorting out interior components.
- Use the product only with approved equipment.
- Allow the product to cool before removing covers or touching internal components.
- Operate the product only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local power company.
- To help avoid damaging your system, be sure the voltage selection switch (if provided) on the power supply is set to match the power available at your location:
 - 115 volts (V)/60 hertz (Hz) in most of North and South America and some Far Eastern countries such as South Korea and Taiwan
 - 100 V/50 Hz in eastern Japan and 100 V/60 Hz in western Japan
 - 230 V/50 Hz in most of Europe, the Middle East, and the Far East
- Also, be sure that attached devices are electrically rated to operate with the power available in your location.
- Use only approved power cable(s). If you have not been provided with a power cable for your system or for any AC-powered option intended for your system, purchase a power cable that is approved for use in your country. The power cable must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.
- To help prevent electric shock, plug the system and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a 3-wire cable with properly grounded plugs.

- Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.
- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables and power cables carefully; route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local/national wiring rules.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:
 - Install the power supply before connecting the power cable to the power supply.
 - Unplug the power cable before removing the power supply.
 - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.
- Move products with care; ensure that all casters and/or stabilizers are firmly connected to the system. Avoid sudden stops and uneven surfaces.



General Precautions for Rack-Mountable Products

Observe the following precautions for rack stability and safety. Also, refer to the rack installation documentation accompanying the system and the rack for specific caution statements and procedures.

- Systems are considered to be components in a rack. Thus, "component" refers to any system as well as to various peripherals or supporting hardware.



CAUTION: Installing systems in a rack without the front and side stabilizers installed could cause the rack to tip over, potentially resulting in bodily injury under certain circumstances. Therefore, always install the stabilizers before installing components in the rack. After installing system/components in a rack, never pull more than one component out of the rack on its slide assemblies at one time. The weight of more than one extended component could cause the rack to tip over and may result in serious injury.

- Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and that the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.
- Always load the rack from the bottom up, and load the heaviest item in the rack first.
- Make sure that the rack is level and stable before extending a component from the rack.
- Use caution when pressing the component rail release latches and sliding a component into or out of a rack; the slide rails can pinch your fingers.
- After a component is inserted into the rack, carefully extend the rail into a locking position, and then slide the component into the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Ensure that proper airflow is provided to components in the rack.
- Do not step on or stand on any component when servicing other components in a rack.



NOTE: A qualified electrician must perform all connections to DC power and to safety grounds. All electrical wiring must comply with applicable local or national codes and practices.



CAUTION: Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.



CAUTION: The system chassis must be positively grounded to the rack cabinet frame. Do not attempt to connect power to the system until grounding cables are connected. Completed power and safety ground wiring must be inspected by a qualified electrical inspector. An energy hazard will exist if the safety ground cable is omitted or disconnected.

CAUTION: The DES-6500 chassis system allows a maximum current of 73.6 Amps to all line cards being used. Whatever combination of line cards used do not exceed the total Amp allowance or the system may become unstable.

The following are the maximum currents of all the line cards:



DES-6504: 8.8A MAX

DES-6505: 4.8A MAX

DES-6507: 9.92A MAX

DES-6508: 7.9A MAX

DES-6509: 5.82A MAX

DES-6510: 8.1A MAX

DES-6512: 6.28A MAX

Protecting Against Electrostatic Discharge

Static electricity can harm delicate components inside your system. To prevent static damage, discharge static electricity from your body before you touch any of the electronic components, such as the microprocessor. You can do so by periodically touching an unpainted metal surface on the chassis.

You can also take the following steps to prevent damage from electrostatic discharge (ESD):

1. When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component in your system. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.
2. When transporting a sensitive component, first place it in an antistatic container or packaging.
3. Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads, workbench pads and an antistatic grounding strap.

Introduction

Ethernet Technology

Switch Description

Features

Ports

Front-Panel Components

Side Panel Description

Rear Panel Description

Gigabit Combo Ports

Ethernet Technology

Fast Ethernet Technology

Switch Description

The xStack® DES-6500 layer 3 modular chassis Ethernet switch is a member of the D-Link xStack® family. Ranging from 10/100Mbps edge switches to core gigabit switches, the xStack® switch family has been future-proof designed to provide a stacking architecture with fault tolerance, flexibility, port density, robust security and maximum throughput with a user-friendly management interface for the networking professional.

The xStack® DES-6500 chassis switch is a modular, chassis-based Ethernet backbone switch designed for adaptability and scalability. This switch provides a management platform with a backplane switch capacity of 160 Gbps. The chassis contains slots for the DES-6502 CPU management module and up to eight modules that can provide up to one hundred and ninety-two 10/100 Mbps Fast Ethernet ports or up to ninety-six 1000 Mbps Gigabit Ethernet ports. These modules can be hot-swapped, and the DES-6500 chassis allows the installation of a redundant power supply, for maximum flexibility and reliability. The DES-6511 redundant power supplies operate in a current-sharing mode with automatic fail-over to ensure constant operation of the Switch.

Features

- IEEE 802.3z compliant
- IEEE 802.3x Flow Control in full-duplex compliant
- IEEE 802.3u compliant
- IEEE 802.3ab compliant
- IEEE 802.1p Priority Queues
- IEEE 802.3ad Link Aggregation Control Protocol support.
- IEEE 802.1x Port-based and MAC-based Access Control
- IEEE 802.1Q VLAN
- IEEE 802.1D Spanning Tree, IEEE 802.1W Rapid Spanning Tree and IEEE 802.1s Multiple Spanning Tree support
- Access Control List (ACL) support
- IP Multinetting support
- Protocol VLAN support
- Single IP Management support
- Access Authentication Control utilizing TACACS, XTACACS, TACACS+ and RADIUS protocols
- Simple Network Time Protocol support
- System and Port Utilization support
- System Log Support

- High performance switching engine performs forwarding and filtering at full wire speed up to 160Gbps.
- Full- and half-duplex for all gigabit ports. Full duplex allows the switch port to simultaneously transmit and receive data. It only works with connections to full-duplex-capable end stations and switches. Connections to a hub must take place at half-duplex.
- Non-blocking store and forward switching scheme capability to support rate adaptation and protocol conversion
- Supports by-port Egress/Ingress rate control
- Efficient self-learning and address recognition mechanism enables forwarding rate at wire speed
- Support port-based enable and disable
- Address table: Supports up to 16K MAC addresses per device
- Supports Port-based VLAN Groups
- Port Trunking with flexible load distribution and fail-over function
- IGMP Snooping support
- Layer 3 support including DVMRP, OSPF and RIP
- SNMP support
- Secure Sockets Layer (SSL) and Secure Shell (SSH) support
- System Severity control
- Safeguard Engine support
- Access profile filters for the CPU
- Port Mirroring support
- MIB support for:
 - RFC1213 MIB II
 - RFC1493 Bridge
 - RFC1757 RMON
 - RFC1643 Ether-like MIB
 - RFC2233 Interface MIB
 - IF MIB
 - Private MIB
 - RFC2674 for 802.1p
 - IEEE 802.1x MIB
- RS-232 DCE console port for Switch management
- Provides parallel LED display for port status such as link/act, speed, etc.

The xStack® DES-6500 Layer 3 modular chassis Ethernet switch contains 9 slots to install the following available modules:

- DES-6501 Backplane chassis
- DES-6502 Management Module
- DES-6506 Patch Panel for 24 port RJ45
- DES-6507 12-port 10BASE-T/100BASE-TX/1000BASE-T + Combo 2 SFP
- DES-6508 16-port 10/100M Base-T module
- DES-6509 12-port mini GBIC Fiber Module
- DES-6510 24-port 10/100M RJ21 Module
- DES-6504 12-port 100BASE-FX (SFF) Fast Ethernet Switch module
- DES-6505 8-port 1000Base-SX SC Fiber Module
- DES-6511 Power Supply Module
- DES-6512 2-port 10 GE XFP switch module

DES-6504 12-port 100BASE-FX (SFF) Fast Ethernet Switch module

- Twelve 100BASE-FX (SFF) Fast Ethernet ports
- Fully compliant with IEEE802.3u 100BASE-FX
- IEEE 802.3x compliant Flow Control support for Full-duplex



DES-6505 8-port 1000BASE-SX (SC) Gigabit Ethernet Switch module

- Eight 1000BASE-SX (SC) Gigabit Ethernet ports
- Fully compliant with IEEE802.3z
- Support Full Duplex operations
- IEEE 802.3x compliant Flow Control support for full-duplex



DES-6506 Patch Panel

- A patch panel supporting 24 port RJ45 10/100M base-T Interfaces



DES-6507 12-port 10BASE-T/100BASE-TX/1000BASE-T Switch module

- Twelve 10BASE-T/100BASE-TX/1000BASE-T ports + Combo 2 SFP
- Fully compliant with IEEE802.3, IEEE802.3a, IEEE802.3u, IEEE802.3z
- All of 10/100/1000Mbps ports support auto-negotiation
- Back pressure Flow Control support for Half-duplex mode
- IEEE 802.3x compliant Flow Control support for Full-duplex



DES-6508 16-port 10BASE-T/100BASE-TX Fast Ethernet Switch module

- Sixteen 10BASE-T/100BASE-TX ports
- Fully compliant with IEEE802.3 10BASE-T, IEEE802.3u 100BASE-TX
- All of 10/100Mbps ports support auto-negotiation
- Back pressure Flow Control support for Half-duplex mode
- IEEE 802.3x compliant Flow Control support for Full-duplex



DES-6509 12-port Mini GBIC (SFP) switch module

- Twelve Mini GBIC Gigabit Ethernet ports
- Support 1000BASE-SX/LX SFP module
- Fully compliant with IEEE802.3z
- Support Full Duplex operations
- IEEE 802.3x compliant Flow Control support for full-duplex



DES-6510 RJ21 connectors provide 24-port 10BASE-T/100BASE-TX Fast Ethernet Switch module

- Two RJ21, each support 12-port 10BASE-T/100BASE-TX ports
- Fully compliant with IEEE802.3 10BASE-T, IEEE802.3u 100BASE-TX
- All of 10/100Mbps ports support auto-negotiation
- Back pressure Flow Control support for Half-duplex mode
- IEEE 802.3x compliant Flow Control support for Full-duplex



DES-6511 Power Supply Modules

- Dual power modules design with current sharing design
- Full redundant feature design to ensure continuous operation
- If one power module failed, the other will take over all current supply automatically.
- Hot-swappable/Hot-pluggable capability
- Power management functions
- Input: 90 ~ 264 VAC, 47 ~ 63Hz
- Output: 3.4V: 4A ~ 80A
- 12V: 0.1A ~ 2A



DES-6512 2-port 10 GE XFP Switch Module

- Two 10G XFP Ethernet Ports
- Support XFP MSA compliant transceivers
- Fully compliant with IEEE 802.3ae
- Support Full Duplex Transmissions
- IEEE 802.3x compliant flow control support for full-duplex



Ethernet Technology

Fast Ethernet

The growing importance of LANs and the increasing complexity of desktop computing applications are fueling the need for high performance networks. A number of high-speed LAN technologies are proposed to provide greater bandwidth and improve client/server response times. Among them, Fast Ethernet, or 100BASE-T, provides a non-disruptive, smooth evolution from 10BASE-T technology.

100Mbps Fast Ethernet 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.

The increased speed and extra bandwidth offered by Gigabit Ethernet are essential to coping with the network bottlenecks that frequently develop as computers and their busses get faster and more users use applications that generate more traffic. Upgrading key components, such as your backbone and servers to Gigabit Ethernet can greatly improve network response times as well as significantly speed up the traffic between your subnetworks.

Gigabit Ethernet enables fast optical-fiber 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.

In addition, the phenomenal bandwidth delivered by Gigabit Ethernet is the most cost-effective method to take advantage of today's and tomorrow's rapidly improving switching and routing internetworking technologies.

Switching Technology

Another key development pushing the limits of Ethernet technology is in the field of switching technology. A switch bridges Ethernet packets at the MAC address level of the Ethernet protocol transmitting among connected Ethernet or Fast Ethernet LAN segments.

Switching is a cost-effective way of increasing the total network capacity available to users on a local area network. A switch increases capacity and decreases network loading by making it possible for a local area network to be divided into different segments, which are not competing with each other for network transmission capacity, and therefore decreasing the load on each segment.

The Switch acts as a high-speed selective bridge between the individual segments. Traffic that needs to go from one segment to another (from one port to another) is automatically forwarded by the Switch, without interfering with any other segments (ports). This allows the total network capacity to be multiplied, while still maintaining the same network cabling and adapter cards.

For Fast Ethernet or Gigabit Ethernet networks, a switch is an effective way of eliminating problems of chaining hubs beyond the "two-repeater limit." A switch can be used to split parts of the network into different collision domains, for example, making it possible to expand your Fast Ethernet network beyond the 205-meter network diameter limit for 100BASE-TX networks. Switches supporting both traditional 10Mbps Ethernet and 100Mbps Fast Ethernet are also ideal for bridging between existing 10Mbps networks and new 100Mbps networks.

Switching LAN technology is a marked improvement over the previous generation of network bridges, which were characterized by higher latencies. Routers have also been used to segment local area networks, but the cost of a router and the setup and maintenance required make routers relatively impractical. Today's switches are an ideal solution to most kinds of local area network congestion problems.



NOTE: For customers interested in D-View, D-Link Corporation's proprietary SNMP management software, go to the D-Link Website (www.dlink.com.cn) and download the software and manual.

Front-Panel Components and LED Indicators

The front panel of the Switch consists of LED indicators for Power, System, Reset and Alarm Off. Also on the front panel resides a RS-232 communication port.



Figure 1- 1. DES-6500 Front Panel

Comprehensive LED indicators display the status of the Switch and the network.

LED or Button	Description
Power	This LED will light green after the Switch is powered on to indicate the normal operation of the Switch’s power supplies. An amber LED will appear to indicate abnormal operation of one or more of the Switch’s power supplies. The indicator is dark when the Switch is powered off.
System	This LED will light solid green to indicate normal operation. An amber LED will appear if the Switch begins acting abnormally. (Usually indicating a fatal error).
Reset	Press the button to reset the Switch.
Alarm Off	Press this button to deactivate the Switch’s internal alarm. The internal alarm will sound if any of the line cards power supply fails, or if the safe operating temperature of one or more of the line cards is exceeded.

Installation

Package Contents

Before You Connect to the Network

Installing the Switch without the Rack

Rack Installation

Power On

The Optional Module

Redundant Power System

Package Contents

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

- One xStack[®] DES-6500 layer 3 modular chassis Ethernet switch
- Mounting kit (two brackets and screws)
- Four rubber feet with adhesive backing
- One AC power cord
- RS-232 console cable
- One CD Kit for User's Guide / CLI / D-View module / SNMP module
- This Manual with Registration Card.

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

Before You Connect to the Network

The site where you install the Switch may greatly affect its performance. Please follow these guidelines for setting up the Switch.

- Install the Switch on a sturdy, level surface that can support the weight of the switch. Do not place heavy objects on the Switch.
- The power outlet should be within 1.82 meters (6 feet) of the Switch.
- Visually inspect the power cord and see that it is fully secured to the AC power port.
- Make sure that there is proper heat dissipation from and adequate ventilation around the Switch. Leave at least 10 cm (4 inches) of space at the front and rear of the Switch for ventilation.
- Install the Switch in a fairly cool and dry place for the acceptable temperature and humidity operating ranges.
- Install the Switch in a site free from strong electromagnetic field generators (such as motors), vibration, dust, and direct exposure to sunlight.
- When installing the Switch on a level surface, attach the rubber feet to the bottom of the device. The rubber feet cushion the Switch, protect the casing from scratches and prevent it from scratching other surfaces.

Installing the Switch without the Rack

When installing the Switch on a desktop or shelf, the rubber feet included with the Switch should first be attached. Attach these cushioning feet on the bottom at each corner of the device. Allow enough ventilation space between the Switch and any other objects in the vicinity.

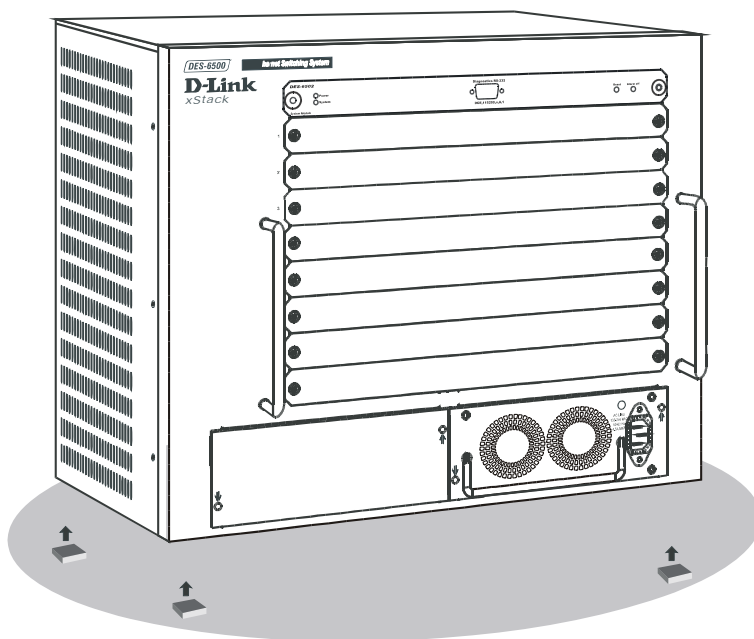


Figure 2- 1. Prepare Switch for installation on a desktop or shelf

Installing the Switch in a Rack

The Switch can be mounted in a standard 19" rack. Use the following diagrams to guide you.

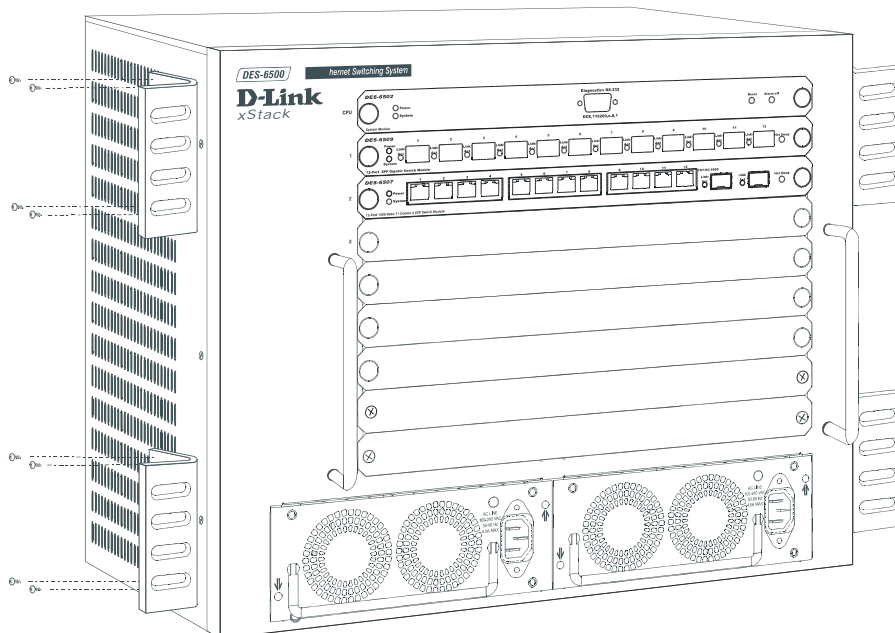


Figure 2- 2. Fasten mounting brackets to Switch

Fasten the mounting brackets to the Switch using the screws provided. With the brackets attached securely, you can mount the Switch in a standard rack as shown in Figure 2-3 on the following page.

Mounting the Switch in a Standard 19" Rack

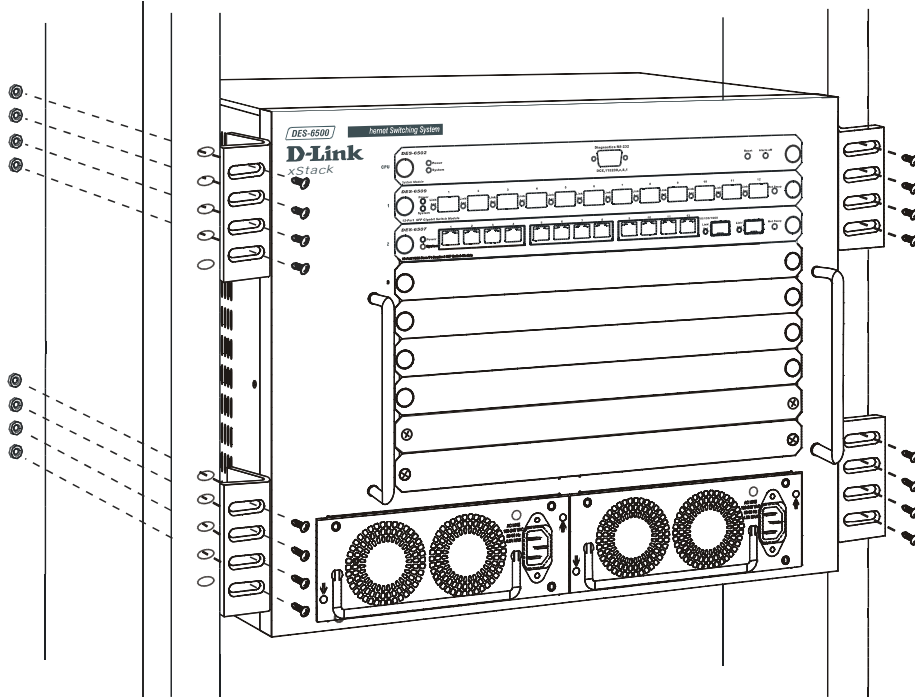


Figure 2- 3. Installing Switch in a rack

Power On

Plug one end of the AC power cord into the power connector of the Switch and the other end into the local power source outlet.

After the Switch is powered on, the LED indicators will momentarily blink. This blinking of the LED indicators represents a reset of the system.

Power Failure

The DES-6500 chassis system allows a maximum current of 73.6 Amps for all line cards. When selecting a line card, ensure that the current of all line cards being used does not exceed the maximum 73.6 Amps that is allowed (For more information regarding the power consumption of this chassis and its line cards refer to **Appendix A** at the end of this manual). If the maximum current is accidentally exceeded, the power supply will shut down due to an inbuilt overcurrent protection safeguard. The user must then unplug the power cord, remove some of the line cards before replugging the power cord again.

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

External Redundant Power System

The Switch supports dual, current-sharing, redundant power supplies, located at the bottom front of the chassis.



Figure 2- 4. Redundant Power Supply

Connecting the Switch

Switch To End Node

Switch to Hub or Switch

Connecting To Network Backbone or Server



NOTE: All high-performance N-Way Ethernet ports can support both MDI-II and MDI-X connections.

Switch to End Node

End nodes include PCs outfitted with a 10, 100 or 1000 Mbps RJ 45 Ethernet Network Interface Card (NIC) and most routers.

An end node can be connected to the Switch via a twisted-pair UTP/STP cable. The end node should be connected to any of the 1000BASE-T ports of the Switch.

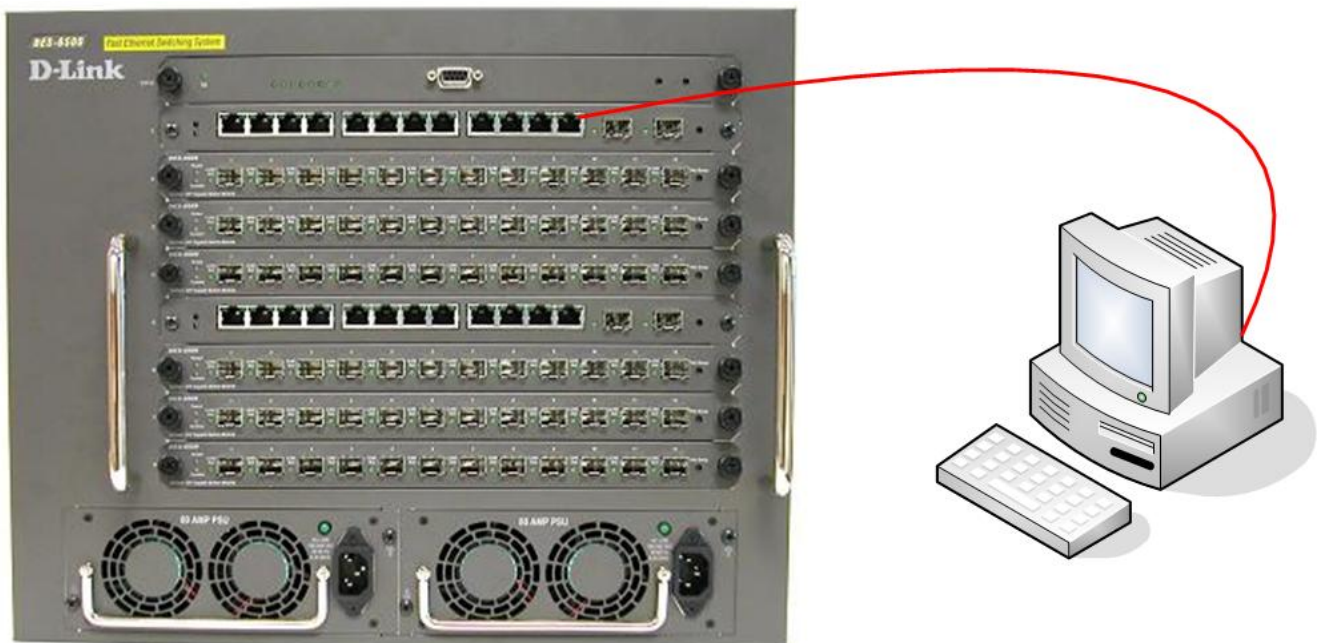


Figure 3- 1. Switch connected to an end node

The Link/Act LEDs for each UTP port will light green or amber when the link is valid. A blinking LED indicates packet activity on that port.

Switch to Hub or Switch

These connections can be accomplished in a number of ways using a normal cable.

- A 10BASE-T hub or switch can be connected to the Switch via a twisted-pair Category 3, 4 or 5 UTP/STP cable.
- A 100BASE-TX hub or switch can be connected to the Switch via a twisted-pair Category 5 UTP/STP cable.
- A 1000BASE-T switch can be connected to the Switch via a twisted pair Category 5e UTP/STP cable.
- A switch supporting a fiber-optic uplink can be connected to the Switch's SFP ports via fiber-optic cabling.

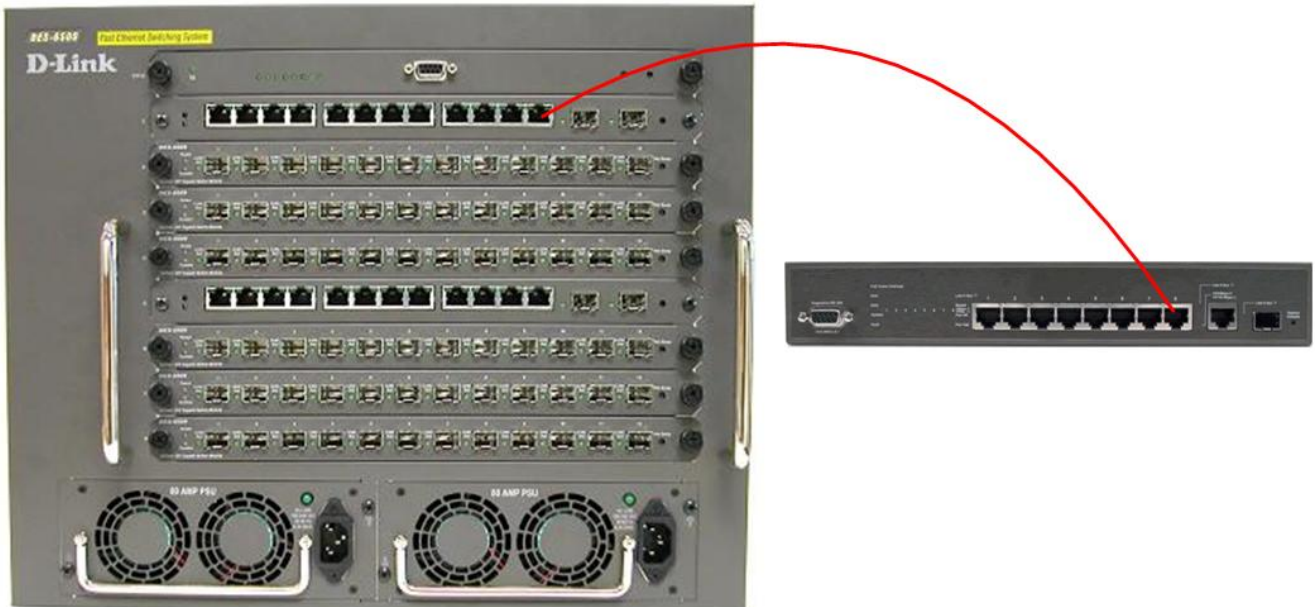


Figure 3- 2. Switch connected to switch using fiber-optic cabling

Using the xStack[®] DES-6500 Layer 3 modular chassis Ethernet switch as a Network Backbone

The xStack[®] DES-6500 chassis switch can be employed as a network backbone for offices or buildings that require many Ethernet connections within a confined space. Once a high-speed line has been connected from the ISP, the xStack[®] DES-6500 chassis switch can farm out up to 196 connections for various end nodes including PCs, printers, hubs, routers or other switches. The topology configurations are endless but be sure that connections coming from the xStack[®] DES-6500 chassis switch are at a equal or slower speed than the ISP uplink to avoid bottlenecking.

The copper ports operate at a speed of 1000, 100 or 10Mbps in full or half duplex mode. The fiber-optic ports can operate at 1000Mbps in full duplex mode only.

Connections to the Gigabit Ethernet ports are made using a fiber-optic cable or Category 5e copper cable, depending on the type of port. A valid connection is indicated when the Link LED is lit.

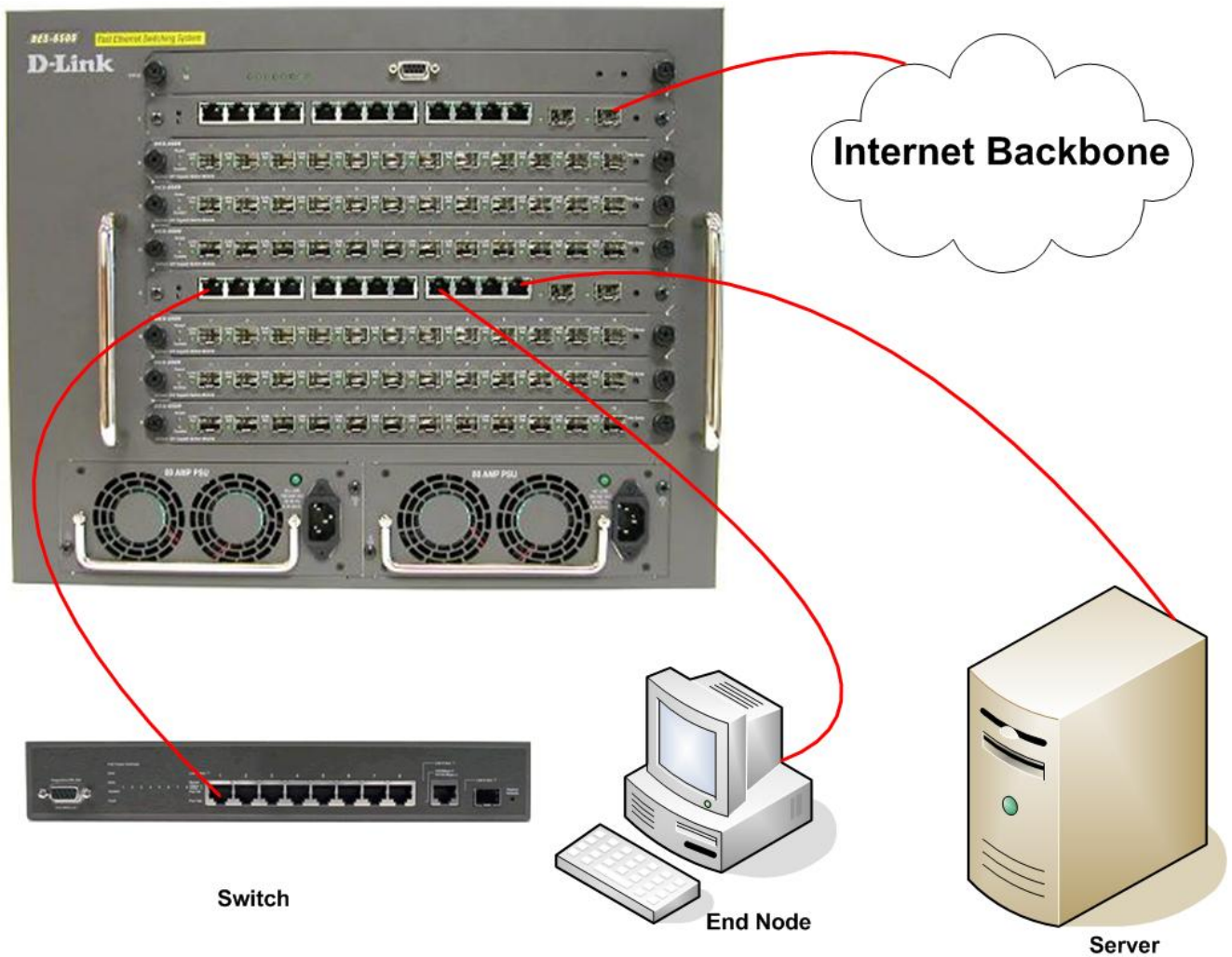


Figure 3- 3. Uplink Connection to a server, PC or switch.

Introduction to Switch Management

Management Options

Web-based Management Interface

SNMP-Based Management

Managing User Accounts

Command Line Console Interface through the Serial Port

Connecting the Console Port (RS-232 DCE)

First Time Connecting to the Switch

Password Protection

SNMP Settings

IP Address Assignment

Connecting Devices to the Switch

Management Options

This system may be managed out-of-band through the console port on the front panel or in-band using Telnet. The user may also choose the web-based management, accessible through a web browser.

Web-based Management Interface

After you have successfully installed the Switch, you can configure the Switch, monitor the LED panel, and display statistics graphically using a web browser, such as Netscape Navigator (version 6.2.3 and higher) or Microsoft® Internet Explorer (version 6.0).

SNMP-Based Management

Users can manage the Switch with an SNMP-compatible console program. The Switch supports SNMP version 1.0, version 2.0c and version 3.0. The SNMP agent decodes the incoming SNMP messages and responds to requests with MIB objects stored in the database. The SNMP agent updates the MIB objects to generate statistics and counters.

Command Line Console Interface through the Serial Port

Users can also connect a computer or terminal to the serial console port to access the Switch. The command-line-driven interface provides complete access to all Switch management features.

Connecting the Console Port (RS-232 DCE)

The Switch provides an RS-232 serial port that enables a connection to a computer or terminal for monitoring and configuring the Switch. This port is a female DB-9 connector, implemented as a Data Communication Equipment (DCE) connection.

To use the console port, you need the following equipment:

- A terminal or a computer with both a serial port and the ability to emulate a terminal.
- A null modem or straight RS-232 cable with a female DB-9 connector for the console port on the Switch.

To connect a terminal to the console port:

1. Connect the female connector of the RS-232 cable directly to the console port on the Switch, and tighten the captive retaining screws.

2. Connect the other end of the cable to a terminal or to the serial connector of a computer running terminal emulation software. Set the terminal emulation software as follows:
3. Select the appropriate serial port (COM port 1 or COM port 2).
4. Set the data rate to 115200 baud.
5. Set the data format to 8 data bits, 1 stop bit, and no parity.
6. Set flow control to none.
7. Under Properties, select VT100 for Emulation mode.
8. Select Terminal keys for Function, Arrow, and Ctrl keys. Ensure that you select Terminal keys (not Windows keys).



NOTE: When you use HyperTerminal with the Microsoft® Windows® 2000 operating system, ensure that you have Windows 2000 Service Pack 2 or later installed. Windows 2000 Service Pack 2 allows you to use arrow keys in HyperTerminal's VT100 emulation. See www.microsoft.com for information on Windows 2000 service packs.

9. After correctly setting up the terminal, plug the power cable into the power receptacle on the back of the Switch. The boot sequence appears in the terminal.
10. After the boot sequence completes, the console login screen displays.
11. If you have not logged into the command line interface (CLI) program, press the Enter key at the User name and password prompts. There is no default user name and password for the Switch. User names and passwords must first be created by the administrator. If user accounts have been previously configured, log in and continue to configure the Switch.
12. Enter the commands to complete desired tasks. Many commands require administrator-level access privileges. Read the next section for more information on setting up user accounts. See the *xStack® DES-6500 Modular Layer 3 Chassis Ethernet Switch CLI* on the documentation CD for a list of all commands and additional information on using the CLI.
13. When tasks have been completed, exit the session with the logout command or close the emulator program.

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

If there are problems making this connection on a PC, make sure the emulation is set to VT-100. Users will be able to set the emulation by clicking on the **File** menu in you HyperTerminal window, clicking on **Properties** in the drop-down menu, and then clicking the **Settings** tab. Here users will find the **Emulation** options. If there is still nothing present on the screen, try rebooting the Switch by disconnecting its power supply.

Once connected to the console, the screen below will appear on your console screen. This is where the user will enter commands to perform all the available management functions. The Switch will prompt the user to enter a user name and a password. Upon the initial connection, there is no user name or password and therefore just press enter twice to access the command line interface.

```
DES-6500 Chassis Ethernet Switch
Command Line Interface

Firmware: Build 3.60.B02
Copyright(C) 2008 D-Link Corporation. All rights reserved.

UserName :
```

Figure 4- 1. Initial screen after first connection.

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."

Upon first connection to the Switch, the user 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.

```
DES-6500 Chassis Ethernet Switch
Command Line Interface

Firmware: Build 3.60.B02
Copyright(C) 2008 D-Link Corporation. All rights reserved.

UserName:
```

Figure 4- 2. Initial screen, first time connecting to the Switch

Press **Enter** in both the Username and Password fields. You will be given access to the command prompt **DES-6500:4#**, as shown below:

There is no initial username or password. Leave the **Username** and **Password** fields blank.

```
DES-6500 Chassis Ethernet Switch
Command Line Interface

Firmware: Build 3.60.B02
Copyright(C) 2008 D-Link Corporation. All rights reserved.

UserName:
PassWord:

DES-6500:4#
```

Figure 4- 3. Command Prompt



NOTE: The first user automatically gets Administrator level privileges. It is recommended to create at least one Admin-level user account for the Switch.

Password Protection

The xStack® DES-6500 chassis switch does not have a default user name and password. One of the first tasks when settings up the Switch is to create user accounts. If logging in using a predefined administrator-level user name, users will have privileged access to the Switch's management software.

After the initial login, define new passwords for both default user names to prevent unauthorized access to the Switch, and record the passwords for future reference.

To create an administrator-level account for the Switch, do the following:

- At the CLI login prompt, enter create account admin followed by the *<user name>* and press the Enter key.
- Users will be asked to provide a password. Type the *<password>* used for the administrator account being created and press the Enter key.
- Users will then be prompted to enter the same password again to verify it. Type the same password and press the Enter key.
- Successful creation of the new administrator account will be verified by a Success message.



NOTE: Passwords are case sensitive. User names and passwords can be up to 15 characters in length.

The sample below illustrates a successful creation of a new administrator-level account with the user name "newmanager".

```
DES-6500:4#create account admin newmanager
Command: create account admin newmanager

Enter a case-sensitive new password:*****
Enter the new password again for confirmation:*****

Success.

DES-6500:4#
```

Figure 4- 4. Create account



NOTICE: CLI configuration commands only modify the running configuration file and are not saved when the Switch is rebooted. To save all your configuration changes in nonvolatile storage, you must use the **save** command to copy the running configuration file to the startup configuration.

SNMP Settings

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the Switch, switch group or network.

Managed devices that support SNMP include software (referred to as an agent), which runs locally on the device. A defined set of variables (managed objects) is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The xStack® DES-6500 chassis switch supports SNMP versions 1, 2c, and 3. Users can specify which version of SNMP to use to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

In SNMP v.1 and v.2c, user authentication is accomplished using 'community strings', which function like passwords. The remote user SNMP application and the Switch SNMP must use the same community string. SNMP packets from any station that has not been authenticated are ignored (dropped).

The default community strings for the Switch used for SNMP v.1 and v.2c management access are:

- public - Allows authorized management stations to retrieve MIB objects.
- private - Allows authorized management stations to retrieve and modify MIB objects.

SNMP v.3 uses a more sophisticated authentication process that is separated into two parts. The first part is to maintain a list of users and their attributes that are allowed to act as SNMP managers. The second part describes what each user on that list can do as an SNMP manager.

The Switch allows groups of users to be listed and configured with a shared set of privileges. The SNMP version may also be set for a listed group of SNMP managers. Thus, users may create a group of SNMP managers that are allowed to view read-only information or receive traps using SNMP v.1 while assigning a higher level of security to another group, granting read/write privileges using SNMP v.3.

Using SNMP v.3 individual users or groups of SNMP managers can be allowed to perform or be restricted from performing specific SNMP management functions. The functions allowed or restricted are defined using the Object Identifier (OID) associated with a specific MIB. An additional layer of security is available for SNMP v.3 in that SNMP messages may be encrypted. To read more about how to configure SNMP v.3 settings for the Switch read the section entitled Management.

Traps

Traps are messages that alert network personnel 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 trap recipient (or network manager). Typical traps include trap messages for Authentication Failure, Topology Change and New Root.

MIBs

Management and counter information are stored by 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. The proprietary MIB may also be retrieved by specifying the MIB Object Identifier. MIB values can be either read-only or read-write.

IP Address Assignment

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. The default Switch IP address can be changed to meet the specification of specific networking address schemes.

The Switch is also assigned a unique MAC address by the factory. This MAC address cannot be changed, and can be found by entering the command "**show switch**" into the command line interface, as shown below.

```
DES-6500:4#show switch
Command: show switch

Device Type       : DES-6500 Chassis Ethernet Switch
MAC Address       : 00-65-00-02-00-00
IP Address        : 10.73.21.11 (Manual)
VLAN Name         : default
Subnet Mask       : 255.0.0.0
Default Gateway   : 0.0.0.0
Boot PROM Version : Build 2.00.B23
Firmware Version  : Build 3.60.B02
Hardware Version  : A1
System Name       :
System Location   :
System Contact    :
Spanning Tree     : Disabled
GVRP              : Disabled
IGMP Snooping     : Disabled
VLAN trunk        : Disabled
802.1x            : Disabled
Jumbo Frame       : Off
Clipaging         : Enabled
Port Mirror       : Disabled
SNTP              : Disabled
DHCP Relay        : Disabled
DNSR Status       : Disabled

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

Figure 4- 5. "show switch" command

The Switch's MAC address can also be found from the Web management program on the **Switch Information (Basic Settings)** window on the **Configuration** menu.

The IP address for the Switch must be set before it can be managed with the Web-based manager. The Switch IP address can be automatically set using BOOTP or DHCP protocols, in which case the actual address assigned to the Switch must be known.

The IP address may be set using the Command Line Interface (CLI) over the console serial port as follows:

Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**. Where the x's represent the IP address to be assigned to the IP interface named System and the y's represent the corresponding subnet mask.

Alternatively, you can enter **config ipif System ipaddress xxx.xxx.xxx.xxx/z**. Where the x's represent the IP address to be assigned to the IP interface named System and the z represents the corresponding number of subnets in CIDR notation.

The IP interface named System on the Switch can be assigned an IP address and subnet mask, which can then be used to connect a management station to the Switch's Telnet or Web-based management agent.

```
DES-6500 Chassis Ethernet Switch
Command Line Interface

Firmware: Build 3.60.B02
Copyright(C) 2008 D-Link Corporation. All rights reserved.

UserName:
PassWord:

DES-6500:4#config ipif System ipaddress 10.53.13.144/255.0.0.0
Command: config ipif System ipaddress 10.53.13.144/8

Success.

DES-6500:4#
```

Figure 4- 6. Assigning the Switch an IP Address

In the above example, the Switch was assigned an IP address of 10.53.13.144 with a subnet mask of 255.0.0.0. The system message **Success** indicates that the command was executed successfully. The Switch can now be configured and managed via Telnet and the CLI or via the Web-based management.

Connecting Devices to the Switch

After you assign IP addresses to the Switch, you can connect devices to the Switch.

To connect a device to an SFP transceiver port:

- Use your cabling requirements to select an appropriate SFP transceiver type.
- Insert the SFP transceiver (sold separately) into the SFP transceiver slot.
- Use the appropriate network cabling to connect a device to the connectors on the SFP transceiver.



NOTICE: When the SFP transceiver acquires a link, the associated integrated 10/100/1000BASE-T port is disabled.

Introduction to Web-based Switch Configuration

Introduction

Logging on to the Web Manager

Web-Based User Interface

Basic Setup

Reboot

Basic Switch Setup

Network Management

Switch Utilities

Network Monitoring

IGMP Snooping Status

Introduction

All software functions of the xStack® DES-6500 chassis switch can be managed, configured and monitored via the embedded web-based (HTML) interface. The Switch can be managed from remote stations anywhere on the network through a standard browser such as Netscape Navigator/Communicator, Mozilla or Microsoft Internet Explorer. The 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.

Logging on to the Web Manager

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** button:



Figure 5- 1. Login Button

This opens the management module's user authentication window, as seen below.



Figure 5- 2. Enter Network Password window

Leave both the **User Name** field and the **Password** field blank and click OK. This will open the Web-based user interface. The Switch management features available in the web-based manager are explained below.

Web-based 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 the system status.

Areas of the User Interface

The figure below shows the user interface. The user interface is divided into three distinct areas as described in the table.

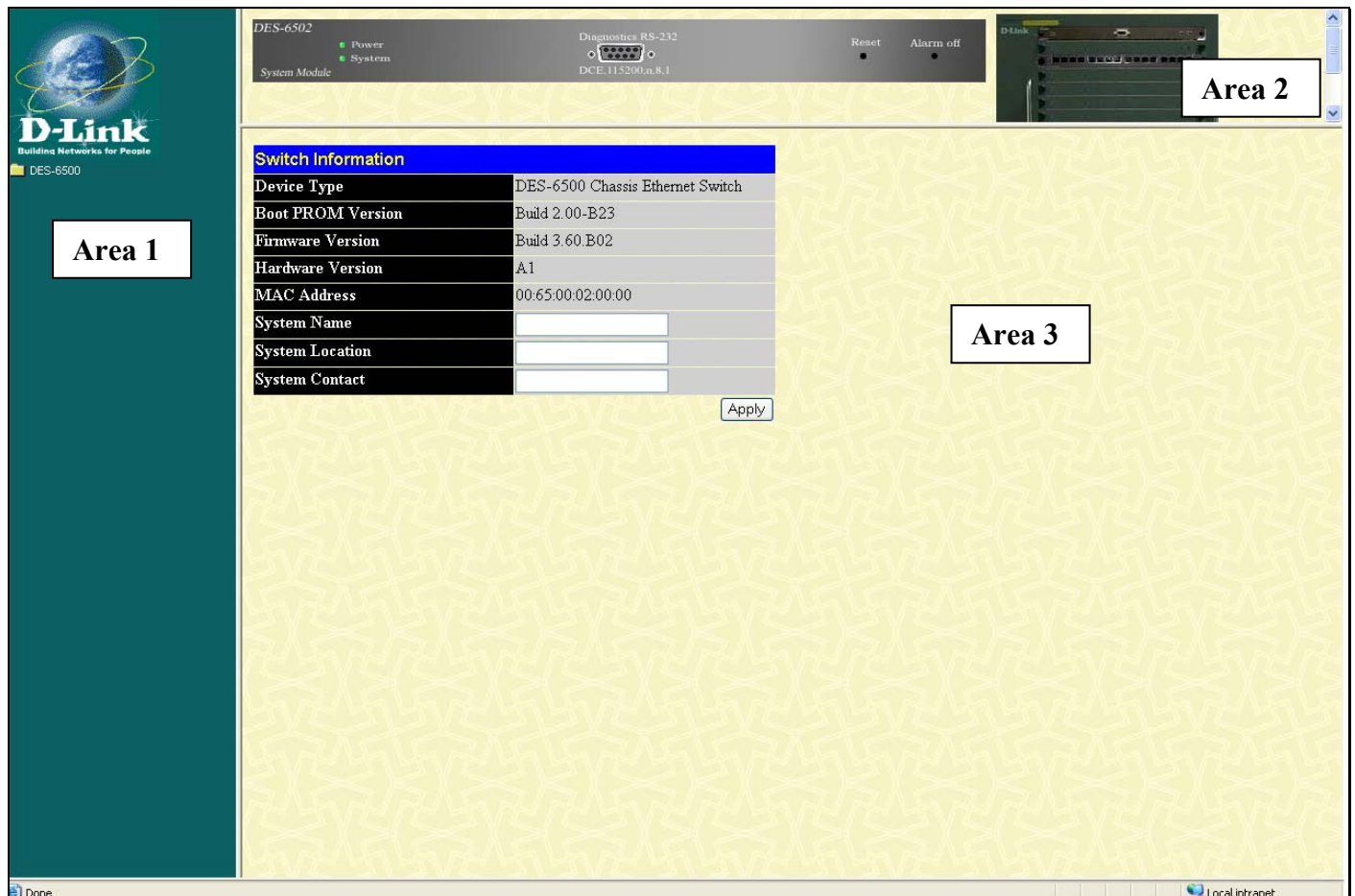


Figure 5- 3. Main Web-Manager Screen

Area	Function
Area 1	Select the menu or window to be displayed. The folder icons can be opened to display the hyper-linked menu buttons and subfolders contained within them. Click the D-Link logo to go to the D-Link website.

Area 2	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 port configuration.
Area 3	Presents switch information based on your selection and the entry of configuration data.



NOTICE: Any changes made to the Switch configuration during the current session must be saved in the Save Changes web menu (explained below) or by using the command line interface (CLI) command `save`.

Web Pages

When you connect to the management mode of the Switch with a web browser, a login screen is displayed. Enter a user name and password to access the Switch's management mode.

Below is a list and description of the main folders available in the web interface:

Configurations - Contains screens concerning configurations for IP Address, Switch Information, Advanced Settings, Port Configuration, Port Mirroring, IGMP, Spanning Tree, Forwarding Filtering, VLANs, Port Bandwidth, SNMP Settings, Port Security, QoS, LACP, Access Profile Table, CPU Interface Filtering, System Log Servers, PAE Access Entity, and Layer 3 IP Networking.

Security Management - Contains screens concerning configurations for Security IP, User Accounts, Access Authentication Control (TACACS), Secure Sockets Layer (SSL), and Secure Shell (SSH).

SNMP Manager – Contains screens and windows concerning the implementation and upkeep of the SNMP Manager of the Switch.

Monitoring - Contains screens concerning monitoring the Switch, pertaining to Port Utilization, CPU Utilization, Packets, Errors Size, MAC Address, IGMP Snooping Group, IGMP Snooping Forwarding, VLAN Status, Router Port, Port Access Control and Layer 3 Feature.

Maintenance - Contains screens concerning configurations and information about Switch maintenance, including TFTP Services, Switch History, Ping Test, Save Changes, Reboot Services and Logout.

Single IP Management - Contains screens concerning information on Single IP Management, including SIM Settings, Topology and Firmware/Configuration downloads.



NOTE: Be sure to configure the user name and password in the User Accounts menu before connecting the Switch to the greater network.

Configuring the Switch

Switch Information

Switch IP Settings

Advanced Settings

Port Configuration

Port Mirroring Configuration

Link Aggregation

IGMP Snooping

Spanning Tree

Forward & Filtering

VLAN

Traffic Control

Port Security

Port Lock Entries

QoS

System Log Server

System Severity Log

SNTP Settings

Access Profile Table

CPU Interface Filtering

Safeguard Engine

Port Access Entity

Layer 3 IP Networking

L3 Global Advanced Settings

IP Interface Table

MD5 Key Configuration

Route Redistribution Settings

Static Default Route

Static ARP Settings

RIP

OSPF

IP Multicast Routing Protocol

DNS Relay

DHCP/Bootp Relay

VRRP

Switch Information

The subsections below describe how to change some of the basic settings for the Switch such as changing IP settings and assigning user names and passwords for management access privileges, as well as how to save the changes and restart the Switch.

Click the **Switch Information** link in the **Configuration** menu.

Switch Information	
Device Type	DES-6500 Chassis Ethernet Switch
Boot PROM Version	Build 2.00-B23
Firmware Version	Build 3.60.B02
Hardware Version	A1
MAC Address	00:65:00:02:00:00
System Name	<input type="text"/>
System Location	<input type="text"/>
System Contact	<input type="text"/>

Figure 6- 1. Switch Information - Basic Settings

The **Switch Information** window shows the **Switch's MAC Address** (assigned by the factory and unchangeable), the **Boot PROM**, **Firmware Version**, and **Hardware Version**. 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. The user may also enter a **System Name**, **System Location** and **System Contact** to aid in defining the Switch, to the user's preference.



NOTE: Please check the firmware version of the CPU and line cards of the xStack® DES-6500 chassis switch before upgrading to firmware release R3.00.B33. For firmware upgrading information, cautions and procedures for release 3, please see Appendix B at the end of the manual.

Switch IP Settings

The IP Address may initially be set using the console interface prior to connecting to it through the Ethernet. If the Switch IP address has not yet been changed, read the introduction of the *xStack® DES-6500 Modular Layer 3 Chassis Ethernet Switch CLI* or return to Section 4 of this manual for more information.

To change IP settings using the web manager you must access the IP Address menu located in the Configuration folder.

To configure the Switch's IP address:

Open the **Configuration** folder and click the **IP Address** menu link. The web manager will display the Switch's current IP settings in the IP configuration menu, as seen below.

Figure 6- 2. IP Address Settings window

To manually assign the Switch's IP address, subnet mask, and default gateway address:

1. Select *Manual* from the **Get IP From** drop-down menu.
2. Enter the appropriate **IP Address** and **Subnet Mask**.
3. To access the Switch from a different subnet from the one it is installed on, enter the IP address of the **Default Gateway**. If managing the Switch from the subnet on which it is installed, users may leave the default address (0.0.0.0) in this field.
4. If no VLANs have been previously configured on the Switch, users may use the *default VLAN Name*. The *default VLAN* contains all of the Switch ports as members. If VLANs have been previously configured on the Switch, enter the *VLAN ID* of the VLAN that contains the port connected to the management station that will access the Switch. The Switch will allow management access from stations with the same VID listed here.



NOTE: The Switch's factory default IP address is 10.90.90.90 with a subnet mask of 255.0.0.0 and a default gateway of 0.0.0.0.

To use the BOOTP or DHCP protocols to assign the Switch an IP address, subnet mask, and default gateway address:

Use the **Get IP From:** *<Manual>* pull-down menu to choose from *BOOTP* or *DHCP*. This selects how the Switch will be assigned an IP address on the next reboot.

The IP Address Settings options are:

Parameter	Description
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.
DHCP	The Switch will send out a DHCP broadcast request when it is powered up. The DHCP protocol allows IP addresses, network masks, and default gateways to be assigned by a DHCP server. If this option is set, the Switch will first look for a DHCP 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.
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.
VLAN Name	This allows the entry of a VLAN Name from which a management station will be allowed to manage the Switch using TCP/IP (in-band via web manager or Telnet). Management stations that are on VLANs other than the one entered here will not be able to manage the Switch in-band unless their IP addresses are entered in the Security IP Management menu. If VLANs have not yet been configured for the Switch, the default VLAN contains all of the Switch's ports. There are no entries in the Security IP Management table, by default, so any management station that can connect to the Switch can access the Switch until a management VLAN is specified or Management Station IP Addresses are assigned.

Click **Apply** to implement changes made.

Setting the Switch's IP Address using the Console Interface

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 IP address for the Switch must be set before it can be managed with the Web-based manager. The Switch IP address can be automatically set using BOOTP or DHCP protocols, in which case the actual address assigned to the Switch must be known. The IP address may be set using the Command Line Interface (CLI) over the console serial port as follows:

- Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**. Where the x's represent the IP address to be assigned to the IP interface named System and the y's represent the corresponding subnet mask.
- Alternatively, you can enter **config ipif System ipaddress xxx.xxx.xxx.xxx/z**. Where the x's represent the IP address to be assigned to the IP interface named System and the z represents the corresponding number of subnets in CIDR notation.

The IP interface named System on the Switch can be assigned an IP address and subnet mask, which can then be used to connect a management station to the Switch's Telnet or Web-based management agent.

The system message **Success** indicates that the command was executed successfully. The Switch can now be configured and managed via Telnet and the CLI or via the Web-based management agent using the above IP address to connect to the Switch.

Advanced Settings

The **Advanced Settings** window contains the main settings for all major functions for the Switch. To view the **Advanced Settings** window, click its link in the **Configuration** folder. This will enable the following window to be viewed and configured.

Advanced Settings	
Serial Port Auto Logout	Never
Serial Port Baud Rate	115200
MAC Address Aging Time (10-1000000)	300
IGMP Snooping	Disabled
Multicast Router Only	Disabled
GVRP Status	Disabled
Telnet Status	Enabled
Telnet Port Number (1-65535)	23
Web Status	Enabled
Web Port Number (1-65535)	80
RMON Status	Disabled
Link Aggregation Algorithm	IP Source
Switch 802.1x	Disabled
Auth Protocol	Radius Eap
HOL Prevention	Enabled
Jumbo Frame	Disabled
Syslog state	Disabled
Apply	

Figure 6- 3. Switch Information (Advanced Settings)

Parameter	Description
Serial Port Auto Logout Time	Select the logout time used for the console interface. This automatically logs the user out after an idle period of time, as defined. Choose from the following options: <i>2 Minutes</i> , <i>5 Minutes</i> , <i>10 Minutes</i> , <i>15 Minutes</i> or <i>Never</i> . The default setting is <i>10 minutes</i> .
Serial Port Baud Rate	This field specifies the baud rate for the serial port on the Switch. This fields menu is set at 115200 and cannot be changed.
MAC Address Aging Time (10-1000000)	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 default age-out time for the Switch is 300 seconds. To change this, type in a different value representing the MAC address age-out time in seconds. The MAC Address Aging Time can be set to any value between 10 and 1,000,000 seconds.
IGMP Snooping	To enable system-wide IGMP Snooping capability select <i>Enabled</i> . IGMP snooping is <i>Disabled</i> by default. Enabling IGMP snooping allows you to specify use of a multicast router only (see below). To configure IGMP Snooping for individual VLANs, use the IGMP Snooping page under the IGMP folder.
Multicast router Only	This field specifies that the Switch should only forward all multicast traffic to a multicast-enabled router, if enabled. Otherwise, the Switch will forward all multicast traffic to any IP router. The default is <i>Disabled</i> .

GVRP Status	Use this pull-down menu to enable or disable GVRP on the Switch.
Telnet Status	Telnet configuration is <i>Enabled</i> by default. If you do not want to allow configuration of the system through Telnet, choose <i>Disabled</i> .
Telnet TCP Port Number (1-65535)	The TCP port number. TCP ports are numbered between 1 and 65535. The "well-known" TCP port for the Web-interface protocol is 80.
Web Status	Web-based management is <i>Enabled</i> by default. If you choose to disable this by selecting <i>Disabled</i> , you will lose the ability to configure the system through the web interface as soon as these settings are applied.
RMON Status	Remote monitoring (RMON) of the Switch is <i>Enabled</i> or <i>Disabled</i> here.
Link Aggregation Algorithm	The algorithm that the Switch uses to balance the load across the ports that make up the port trunk group is defined by this definition. Choose <i>MAC Source</i> , <i>MAC Destination</i> , <i>MAC Src & Dest</i> , <i>IP Source</i> , <i>IP Destination</i> or <i>IP Src & Dest</i> (See the Link Aggregation section of this manual for more information).
Switch 802.1x	<p>The Switch's 802.1x function may be enabled by port or by MAC Address; the default is <i>Disabled</i>. This field must be enabled to view and configure certain windows for 802.1x. More information regarding 802.1x, its functions and implementation can be found later in this section, under the Port Access Entity folder.</p> <p>Port-Based 802.1x specifies that ports configured for 802.1x are initialized based on the port number only and are subject to any authorization parameters configured.</p> <p>MAC-based Authorization specifies that ports configured for 802.1x are initialized based on the port number and the MAC address of the computer being authorized and are then subject to any authorization parameters configured.</p>
Auth Protocol	The user may use the pull down menu to choose between <i>radius eap</i> and <i>radius pap</i> for the 802.1x authentication protocol on the Switch. The default setting is <i>radius eap</i> .
HOL Prevention	This field will enable or disable Head of Line Prevention on the Switch. The default is <i>Enabled</i> .
Jumbo Frame	This field will enable or disable the Jumbo Frame function on the Switch. The default is <i>Disabled</i> . The Switch supports Jumbo frames up to 9216 bytes.
Syslog State	Enables or disables Syslog State; default is <i>Disabled</i> .

Click **Apply** to implement changes made.

Port Configuration

This section contains information for configuring various attributes and properties for individual physical ports, including port speed and address learning. Clicking on **Port Configurations** in the **Configuration** menu will display the following window for the user:

Port Configuration								
Unit	From	To	State	Speed/Duplex	Flow Control	Learning	Description	Apply
1	Port 1	Port 1	Enabled	100M/Full	Disabled	Enabled		Apply

The Port Information Table						
Port	State	Speed/Duplex	Flow Control	Connection	Learning	Description
1	Enabled	100M/Full	Disabled	Link Down	Enabled	
2	Enabled	100M/Full	Disabled	Link Down	Enabled	
3	Enabled	100M/Full	Disabled	Link Down	Enabled	
4	Enabled	100M/Full	Disabled	Link Down	Enabled	
5	Enabled	100M/Full	Disabled	Link Down	Enabled	
6	Enabled	100M/Full	Disabled	Link Down	Enabled	
7	Enabled	100M/Full	Disabled	Link Down	Enabled	
8	Enabled	100M/Full	Disabled	Link Down	Enabled	
9	Enabled	100M/Full	Disabled	Link Down	Enabled	
10	Enabled	100M/Full	Disabled	Link Down	Enabled	
11	Enabled	100M/Full	Disabled	Link Down	Enabled	
12	Enabled	100M/Full	Disabled	Link Down	Enabled	

Figure 6- 4. Port Configuration and The Port Information Table window

To configure switch ports:

1. Choose the port or sequential range of ports using the **From...To...** port pull-down menus, and the **Unit** ID of the Switch to be configured.
2. Use the remaining pull-down menus to configure the parameters described below:

Parameter	Description
State	Toggle the State <Enabled> field to either enable or disable a given port or group of ports.
Speed/Duplex	<p>Toggle the Speed/Duplex field to either select the speed and duplex/half-duplex state of the port. <i>Auto</i> denotes auto-negotiation between 10 and 100 Mbps devices, in full- or half-duplex or 1000 Mbps in Full duplex only. The <i>Auto</i> 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 <i>Auto</i>, <i>10M/Half</i>, <i>10M/Full</i>, <i>100M/Half</i> and <i>100M/Full</i>, <i>1000M/Full_M</i>, <i>1000M/Full_S</i> and <i>1000/Full_N</i>. There is no automatic adjustment of port settings with any option other than <i>Auto</i>.</p> <p>The Switch allows the user to configure two types of gigabit connections; <i>1000M/Full_M</i> and <i>1000M/Full_S</i>. Gigabit connections are only supported in full duplex connections and take on certain characteristics that are different from the other choices listed.</p> <p>The <i>1000M/Full_M</i> (master) and <i>1000M/Full_S</i> (slave) parameters refer to connections running a 1000BASE-T cable for connection between the Switch port and other device capable of a gigabit connection. The master setting (<i>1000M/Full_M</i>) will allow the port to advertise capabilities related to duplex, speed and physical layer type. The master setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing the timing control between the two physical layers. The timing control is set on a master physical layer by a local source. The slave setting (<i>1000M/Full_S</i>) uses loop timing, where the timing comes from a data stream received from the master. If one connection is set for <i>1000M/Full_M</i>, the other side of the connection must be set for <i>1000M/Full_S</i>. Any other configuration will result in a link down status for both ports.</p> <p>Fiber-optic ports are statically set and unchangeable at 1000Mbps in Full-Duplex. The user may configure these ports to be <i>Auto</i> or <i>1000Full_N</i>.</p>

Flow Control	Displays the flow control scheme used for the various port configurations. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use backpressure flow control, and <i>Auto</i> ports use an automatic selection of the two. The default is <i>Disabled</i> .
Learning	Enable or disable MAC address learning for the selected ports. When <i>Enabled</i> , destination and source MAC addresses are automatically listed in the forwarding table. When learning is <i>Disabled</i> , MAC addresses must be manually entered into the forwarding table. This is sometimes done for reasons of security or efficiency. See the section on Forwarding/Filtering for information on entering MAC addresses into the forwarding table. The default setting is <i>Enabled</i> .
Description	Enter a description of the port, if needed. This description can be no longer than 32 characters.

Click **Apply** to implement the new settings on the Switch.

Port Mirroring Configuration

The Switch allows you to copy frames transmitted and received on a port and redirect the copies to another port. You can attach a monitoring device to the mirrored port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port. This is useful for network monitoring and troubleshooting purposes. To view the **Port Mirroring** window, click **Port Mirroring** in the **Configuration** folder.

Port Mirroring Configuration

Target Port Unit: 1 Port: Port 1

Status: Disabled

Source Port Unit: 1

Port Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
None	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ingress	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Egress	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Both	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Apply

Note(1): The "Source Port" and "Target Port" should be different, or the setup will be invalid.

Note(2): The "Target Port" should be a non-trunked port.

Figure 6- 5. Port Mirroring window

To configure a mirror port:

- Select the **Source Port** from where to copy frames and the **Target Port**, which receives the copies from the source port.
- Select the **Source Direction**, **Ingress**, **Egress**, or **Both** and change the **Status** drop-down menu to *Enabled*.
- Click **Apply** to let the changes take effect.



NOTE: Users cannot mirror a fast port onto a slower port. For example, attempting to mirror the traffic from a 100 Mbps port onto a 10 Mbps port may cause throughput problems. The port from which frames are being copied should always support an equal or lower speed than the port which is sending the copies.

In addition, the target port for the mirroring cannot be a member of a trunk group.

Please note a target port and a source port cannot be the same port.

Link Aggregation

Understanding Port Trunk Groups

Port trunk groups are used to combine a number of ports together to make a single high-bandwidth data pipeline.

The xStack® DES-6500 chassis switch supports up to 32 port trunk groups with 2 to 8 ports in each group. A potential bit rate of 8000 Mbps can be achieved.

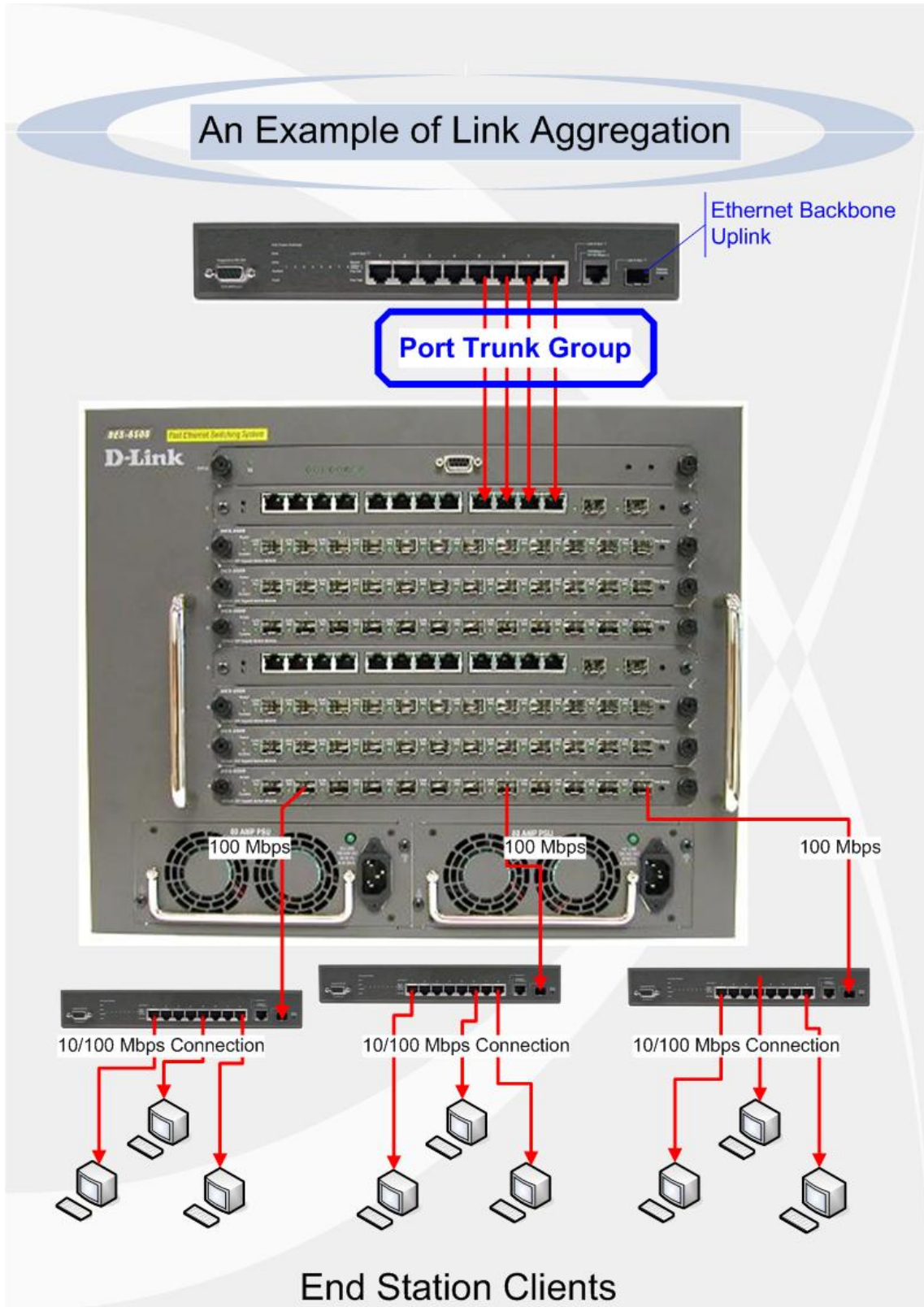


Figure 6- 6. Example of Port Trunk Group

The Switch treats all ports in a trunk group as a single port. 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.



NOTE: If any ports within the trunk group become disconnected, packets intended for the disconnected port will be load shared among the other uplinked ports of the link aggregation group.

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, to the backbone of a network.

The Switch allows the creation of up to 32 link aggregation groups, each group consisting of 2 to 8 links (ports). All of the ports in the group must be members of the same VLAN, and their STP status, static multicast, traffic control, traffic segmentation and 802.1p default priority configurations must be identical. Port locking, port mirroring and 802.1X must not be enabled on the trunk group. Further, the aggregated links must all be of the same speed and should be configured as full-duplex.

The Master Port of the group is to be configured by the user, and all configuration options, including the VLAN configuration that can be applied to the Master Port, are applied to the entire link aggregation group.

Load balancing is automatically applied to the ports in the aggregated group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

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 Master 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 port trunking, open the **Link Aggregation** folder and click on the **Link Aggregation Configuration** hyperlink in the **Configuration** folder to bring up the **Link Aggregation Group Entries** table:

Current Link Aggregation Group Entries			
Group ID	State	Type	Delete
1	Enabled	LACP	

Figure 6- 7. Port Link Aggregation Group Entries window

To configure port trunk groups, click the **Add** button to add a new trunk group and use the **Link Aggregation Settings** menu (see example below) to set up trunk groups. To modify a port trunk group, click the hyperlinked group number corresponding to the entry you wish to alter. To delete a port trunk group, click the corresponding under the **Delete** heading in the **Current Link Aggregation Group Entries** table.

Link Aggregation Group Configuration																																																	
Group ID	<input type="text"/>																																																
Type	LACP																																																
State	Disabled																																																
Master Port	1 Port 1																																																
Unit	1																																																
Choose Member Ports	<table border="1"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td> </tr> <tr> <td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td> </tr> </table>	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24																										
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																										
Active Ports																																																	
Flooding Port	X																																																
Apply																																																	
<p>Note(1): It is only valid to set up at most 8 member ports of any one trunk group and a port can be a member of only one trunk group at a time.</p> <p>Show All Link Aggregation Group Entries</p>																																																	

Figure 6- 8. Link Aggregation Group Configuration window – Add

Link Aggregation Group Configuration																																																	
Group ID	1																																																
Type	LACP																																																
State	Enabled																																																
Master Port	1 Port 1																																																
Unit	1																																																
Choose Member Ports	<table border="1"> <tr> <td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td> </tr> <tr> <td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td> </tr> </table>	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24																										
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																										
Active Ports																																																	
Flooding Port	X																																																
Apply																																																	
<p>Note(1): It is only valid to set up at most 8 member ports of any one trunk group and a port can be a member of only one trunk group at a time.</p> <p>Show All Link Aggregation Group Entries</p>																																																	

Figure 6- 9. Link Aggregation Group Configuration window - Modify

The user-changeable parameters are as follows:

Parameter	Description
Group ID	Select an ID number for the group, between 1 and 32.
Type	This pull-down menu allows you to select between <i>Static</i> and <i>LACP</i> (Link Aggregation Control Protocol). LACP allows for the automatic detection of links in a Port Trunking Group.
State	Trunk groups can be toggled between <i>Enabled</i> and <i>Disabled</i> . This is used to turn a port trunking 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.
Master Port	Choose the Master Port for the trunk group using the pull down menu.

Unit	Choose the unit of the switch in the chassis to be configured.
Choose Member Ports	Choose the members of a trunked group. 2 to 8 ports can be assigned to an individual group.
Active Port	Shows the port that is currently forwarding packets.
Flooding Port	A trunking group must designate one port to allow transmission of broadcasts and unknown unicasts.

After setting the previous parameters, click **Apply** to allow changes to be implemented. Successfully created trunk groups will be shown in the **Current Link Aggregation Group Entries**.

LACP Port Settings

The **LACP Port Settings** window is used in conjunction with the **Link Aggregation** window to create port trunking groups on the Switch. Using the following window, the user may set which ports will be active and passive in processing and sending LACP control frames.

LACP Settings				
Unit	From	To	Mode	Apply
1	Port 1	Port 1	Passive	Apply
Port LACP Table				
Port	Activity			
1	Passive			
2	Passive			
3	Passive			
4	Passive			
5	Passive			
6	Passive			
7	Passive			
8	Passive			
9	Passive			
10	Passive			
11	Passive			
12	Passive			

Figure 6- 10. LACP Port Setting and LACP Port Information window

The user may set the following parameters:

Parameter	Description
Unit	Choose the switch in the chassis to be configured by using the pull-down menu.
From/To	A consecutive group of ports may be configured starting with the selected port.
Mode	<p><i>Active</i> - Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP.</p> <p><i>Passive</i> - LACP ports that are designated as passive cannot initially send LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, one end of the connection must have "active" LACP ports (see above).</p>

After setting the previous parameters, click **Apply** to allow your changes to be implemented. The **LACP Port Table** shows which ports are active and/or passive.

IGMP Snooping

Internet Group Management Protocol (IGMP) snooping allows the Switch to recognize IGMP queries and reports sent between network stations or devices and an IGMP host. When enabled for IGMP snooping, the Switch can open or close a port to a specific device based on IGMP messages passing through the Switch.

In order to use IGMP Snooping it must first be enabled for the entire Switch (see **Advanced Settings**). You may then fine-tune the settings for each VLAN using the **IGMP Snooping** link in the **Configuration** folder. When enabled for IGMP snooping, the Switch can open or close a port to a specific Multicast group member based on IGMP messages sent from the device to the IGMP host or vice versa. The Switch monitors IGMP messages and discontinues forwarding multicast packets when there are no longer hosts requesting that they continue. Use the **IGMP Snooping Group Entry Table** to view IGMP Snooping status. To modify settings, click the **Modify** button for the VLAN Name entry you want to change.

Use the **IGMP Snooping Settings** window to view **IGMP Snooping** settings. To modify the settings, click the **Modify** button of the VLAN ID you want to change.

Total Entries : 1				
IGMP Snooping Settings				
VLAN ID	VLAN Name	State	Querier State	Modify
1	default	Disabled	Disabled	<input type="button" value="Modify"/>

Figure 6- 11. Current IGMP Snooping Group Entries

Clicking the **Modify** button will open the **IGMP Snooping Settings** menu, shown below:

IGMP Snooping Settings	
VLAN ID	<input type="text" value="1"/>
VLAN Name	<input type="text" value="default"/>
Query Interval (1-65535)	<input type="text" value="125"/>
Max Response Time (1-25)	<input type="text" value="10"/>
Robustness Value (1-255)	<input type="text" value="2"/>
Last Member Query Interval (1-25)	<input type="text" value="1"/>
Host Timeout (1-16711450)	<input type="text" value="260"/>
Router Timeout (1-16711450)	<input type="text" value="260"/>
Leave Timer (1-16711450)	<input type="text" value="2"/>
Querier State	<input type="text" value="Disabled"/>
Querier Router Behavior	Non-Querier
State	<input type="text" value="Disabled"/>
<input type="button" value="Apply"/>	
Show All IGMP Group Entries	

Figure 6- 12. IGMP Snooping Settings-Edit window

The following parameters may be viewed or modified:

Parameter	Description
VLAN ID	This is the VLAN ID that, along with the VLAN Name , identifies the VLAN for which to modify the IGMP Snooping Settings .

VLAN Name	This is the VLAN Name that, along with the VLAN ID , identifies the VLAN for which to modify the IGMP Snooping Settings .
Query Interval	The Query Interval field is used to set the time (in seconds) between transmitting IGMP queries. Entries between 1 and 65535 seconds are allowed. Default = 125.
Max Response Time	This determines the maximum amount of time in seconds allowed before sending an IGMP response report. The Max Response Time field allows an entry between 1 and 25 (seconds). Default = 10.
Robustness Value	Adjust this variable according to expected packet loss. If packet loss on the VLAN is expected to be high, the Robustness Variable should be increased to accommodate increased packet loss. This entry field allows an entry of 1 to 255. Default = 2.
Last Member Query Interval	This field specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. Default = 1.
Host Timeout	This is the maximum amount of time in seconds allowed for a host to continue membership in a multicast group without the Switch receiving a host membership report. Default = 260.
Router Timeout	This is the maximum amount of time in seconds a route is kept in the forwarding table without receiving a membership report. Default = 260.
Leave Timer	This specifies the maximum amount of time in seconds between the Switch receiving a leave group message from a host, and the Switch issuing a group membership query. If no response to the membership query is received before the Leave Timer expires, the (multicast) forwarding entry for that host is deleted.
Querier State	Choose <i>Enabled</i> to enable transmitting IGMP Query packets or <i>Disabled</i> to disable. The default is <i>Disabled</i> .
Querier Router Behavior	This read-only field describes the behavior of the router for sending query packets. <i>Querier</i> will denote that the router is sending out IGMP query packets. <i>Non-Querier</i> will denote that the router is not sending out IGMP query packets. This field will only read <i>Querier</i> when the Querier State and the State fields have been Enabled.
State	Select <i>Enabled</i> to implement IGMP Snooping. This field is <i>Disabled</i> by default.

Click **Apply** to implement the new settings. Click the [Show All IGMP Snooping Entries](#) link to return to the **Current IGMP Snooping Group Entries** window.

Static Router Port Settings

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 (IGMP) coming from the network to be propagated to the router.

A router port has the following behavior:

- 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 multicast router connected to the router port of a Layer 3 switch would not be able to receive UDP data streams 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 or PIM-DM multicast packets are detected flowing into a port.

Open the **IGMP Snooping** folder and then click on the **Static Router Ports Settings** link to open the **Static Router Ports Entries** page, as shown below.

Static Router Port Settings		
VLAN ID	VLAN Name	Modify
1	default	Modify
2	v2	Modify
4094	v4094	Modify

Figure 6- 13. Static Router Ports Settings window

The **Static Router Ports Settings** page (shown above) displays all of the current entries to the Switch's static router port table. To modify an entry, click the **Modify** button. This will open the **Static Router Ports Settings - Edit** page, as shown below.

Static Router Ports Settings																								
VID	1																							
VLAN Name	default																							
Unit	1																							
Port Settings	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Static	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Forbidden	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Apply																								
Show All Static Router Ports Entries																								

Figure 6- 14. Static Router Ports Settings - Edit window

The following parameters can be set:

Parameter	Description
VID (VLAN ID)	Enter the VLAN ID which, along with the VLAN Name, identifies the VLAN where the multicast router is attached.
VLAN Name	This is the name of the VLAN where the multicast router is attached.
Unit	Choose the Switch ID number of the line card in the chassis to be modified.
Port Settings	These are the ports on the Switch that will have a multicast router attached to them. Static – Choose these ports to be connected to a multicast enabled router. Forbidden – Choose these ports to be forbidden from being connected to a multicast enabled router.

Click **Apply** to implement the new settings, Click the [Show All Static Router Port Entries](#) link to return to the **Current Static Router Port Entries** window.

Spanning Tree

This Switch supports three versions of the Spanning Tree Protocol; 802.1d STP, 802.1w Rapid STP and 802.1s MSTP. 802.1d STP will be familiar to most networking professionals. However, since 802.1w RSTP and 802.1s MSTP has been recently introduced to D-Link managed Ethernet switches, a brief introduction to the technology is provided below followed by a description of how to set up 802.1d STP, 802.1w RSTP and 802.1s MSTP.

802.1s MSTP

Multiple Spanning Tree Protocol, or MSTP, is a standard defined by the IEEE community that allows multiple VLANs to be mapped to a single spanning tree instance, which will provide multiple pathways across the network. Therefore, these MSTP configurations will balance the traffic load, preventing wide scale disruptions when a single spanning tree instance fails. This will allow for faster convergences of new topologies for the failed instance. Frames designated for these VLANs will be processed quickly and completely throughout interconnected bridges utilizing either of the three spanning tree protocols (STP, RSTP or MSTP).

This protocol will also tag BPDU packets so receiving devices can distinguish spanning tree instances, spanning tree regions and the VLANs associated with them. These instances will be classified by an MSTI ID. MSTP will connect multiple spanning trees with a Common and Internal Spanning Tree (CIST). The CIST will automatically determine each MSTP region, its maximum possible extent and will appear as one virtual bridge that runs a single spanning tree. Consequentially, frames assigned to different VLANs will follow different data routes within administratively established regions on the network, continuing to allow simple and full processing of frames, regardless of administrative errors in defining VLANs and their respective spanning trees.

Each switch utilizing the MSTP on a network will have a single MSTP configuration that will have the following three attributes:

1. A configuration name defined by an alphanumeric string of up to 32 characters (defined in the **STP Bridge Global Settings** window in the **Configuration Name** field).
2. A configuration revision number (named here as a **Revision Level** and found in the **STP Bridge Global Settings** window) and;
3. A 4096 element table (defined here as a **VID List** in the **MST Configuration Table** window) which will associate each of the possible 4096 VLANs supported by the Switch for a given instance.

To utilize the MSTP function on the Switch, three steps need to be taken:

1. The Switch must be set to the MSTP setting (found in the **STP Bridge Global Settings** window in the **STP Version** field)
2. The correct spanning tree priority for the MSTP instance must be entered (defined here as a **Priority** in the **MST Configuration Table** window when configuring an **MSTI ID** settings).
3. VLANs that will be shared must be added to the **MSTP Instance ID** (defined here as a **VID List** in the **MST Configuration Table** window when configuring an **MSTI ID** settings).

802.1w Rapid Spanning Tree

The Switch implements three versions of the Spanning Tree Protocol, the Multiple Spanning Tree Protocol (MSTP) as defined by the IEEE 802.1s, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1w specification and a version compatible with the IEEE 802.1d STP. RSTP can operate with legacy equipment implementing IEEE 802.1d, however the advantages of using RSTP will be lost.

The IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1d STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations, in particular, certain Layer 3 functions that are increasingly handled by Ethernet switches. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

Port Transition States

An essential difference between the three protocols is in the way ports transition to a forwarding state and in the way this transition relates to the role of the port (forwarding or not forwarding) in the topology. MSTP and RSTP combine the transition states disabled, blocking and listening used in 802.1d and creates a single state Discarding. In either case, ports do not forward packets. In the STP port transition states disabled, blocking or listening or in the RSTP/MSTP port state discarding, there is no functional difference, the port is not active in the network topology. Table 6-1 below compares how the three protocols differ regarding the port state transition.

All three protocols calculate a stable topology in the same way. Every segment will have a single path to the root bridge. All bridges listen for BPDUs. However, BPDUs are sent more frequently - with every Hello packet. BPDUs are sent even if a BDU packet was not received. Therefore, each link between bridges is sensitive to the status of the link. Ultimately this difference results in faster detection of failed links, and thus faster topology adjustment. A drawback of 802.1d is this absence of immediate feedback from adjacent bridges.

802.1s MSTP	802.1w RSTP	802.1d STP	Forwarding	Learning
Discarding	Discarding	Disabled	No	No
Discarding	Discarding	Blocking	No	No
Discarding	Discarding	Listening	No	No
Learning	Learning	Learning	No	Yes
Forwarding	Forwarding	Forwarding	Yes	Yes

Table 6- 1. Comparing Port States

RSTP is capable of a more rapid transition to a forwarding state - it no longer relies on timer configurations - RSTP compliant bridges are sensitive to feedback from other RSTP compliant bridge links. Ports do not need to wait for the topology to stabilize before transitioning to a forwarding state. In order to allow this rapid transition, the protocol introduces two new variables: the edge port and the point-to-point (P2P) port.

Edge Port

The edge port is a configurable designation used for a port that is directly connected to a segment where a loop cannot be created. An example would be a port connected directly to a single workstation. Ports that are designated as edge ports transition to a forwarding state immediately without going through the listening and learning states. An edge port loses its status if it receives a BDU packet, immediately becoming a normal spanning tree port.

P2P Port

A P2P port is also capable of rapid transition. P2P ports may be used to connect to other bridges. Under RSTP/MSTP, all ports operating in full-duplex mode are considered to be P2P ports, unless manually overridden through configuration.

802.1d / 802.1w / 802.1s Compatibility

MSTP or RSTP can interoperate with legacy equipment and is capable of automatically adjusting BDU packets to 802.1d format when necessary. However, any segment using 802.1d STP will not benefit from the rapid transition and rapid topology change detection of MSTP or RSTP. The protocol also provides for a variable used for migration in the event that legacy equipment on a segment is updated to use RSTP or MSTP.

The Spanning Tree Protocol (STP) operates on two levels:

1. On the switch level, the settings are globally implemented.
2. On the port level, the settings are implemented on a per user-defined group of ports basis.

STP Loopback Detection

When connected to other switches, STP is an important configuration in consistency for delivering packets to ports and can greatly improve the throughput of your switch. Yet, even this function can malfunction with the emergence of STP BPDU packets that occasionally loopback to the Switch, such as BPDU packets looped back from an unmanaged switch connected to the DES-6500. To maintain the consistency of the throughput, the DES-6500 now implements the STP loopback detection function.

When the STP Loopback Detection function is enabled, the Switch will be protected against a loop occurring between switches. Once a BPDU packet returns to the Switch, this function will detect that there is an anomaly occurring and will place the receiving port in an error-disabled state. Consequentially, a message will be placed in the Switch's Syslog and will be defined there as "BPDU Loop Back on Port #".

Setting the Loopback Timer

The loopback timer plays a key role in the next step the switch will take to resolve this problem. Choosing a non-zero value on the timer will enable the Auto-Recovery Mechanism. When the timer expires, the switch will again look for its returning BPDU packet on the same port. If no returning packet is received, the Switch will recover the port as a Designated Port in the Discarding State. If another returning BPDU packet is received, the port will remain in a blocked state, the timer will reset to the specified value, restart, and the process will begin again.

For those who choose not to employ this function, the Loopback Recovery time must be set to zero. In this case, when a BPDU packet is returned to the Switch, the port will be placed in a blocking state and a message will be sent to the Syslog of the Switch. To recover the port, the administrator must disable the state of the problematic port and enable it again. This is the only method available to recover the port when the Loopback Recover Timer is set to 0.

Regulations and Restrictions for the Loopback Detection Function

- All three versions of STP (STP, RSTP and MSTP) can enable this feature.
- May be configured globally (STP Global Bridge Settings), or per port (MSTP Port Information).
- Neighbor switches of the DES-6500 must have the capability to forward BPDU packets. Switches that fail to meet this requirement will disable this function for the port in question on the DES-6500.
- The default setting for this function is disabled.
- The default setting for the Loopback timer is 60 seconds.
- This setting will only be operational if the interface is STP-enabled.
- The Loopback Detection feature can only prevent BPDU loops on the DES-6500 designated ports. It can detect a loop condition occurring on the user's side connected to the edge port, but it cannot detect the Loopback condition on the elected root port of STP on another switch.

STP Bridge Global Settings

To open the following window, open the **Spanning Tree** folder in the **Configuration** menu and click the **STP Bridge Global Settings** link.

Figure 6- 15. STP Bridge Global Settings – STP compatible and RSTP (default)

Figure 6- 16. STP Bridge Global Settings - MSTP

The following parameters can be set:

Parameter	Description
STP Status	Use the pull-down menu to enable or disable STP globally on the Switch. The default is <i>Disabled</i> .
STP Version	Use the pull-down menu to choose the desired version of STP to be implemented on the Switch. There are three choices: <i>STP</i> - Select this parameter to set the Spanning Tree Protocol(STP) globally on the switch. <i>RSTP</i> - Select this parameter to set the Rapid Spanning Tree Protocol (RSTP) globally on the Switch. <i>MSTP</i> - Select this parameter to set the Multiple Spanning Tree Protocol (MSTP) globally on the Switch.
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. This field will only appear here when STP or RSTP is selected for the STP Version. For MSTP, the Hello Time must be set on a port per port basis. See the STP Port Settings section for further details.

Max Age	The Max Age may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the 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. The user may choose a time between 6 and 40 seconds. The default value is 20.
Forward Delay	The Forward Delay can be from 4 to 30 seconds. Any port on the Switch spends this time in the listening state while moving from the blocking state to the forwarding state.
Max Hops	Used to set the number of hops between devices in a spanning tree region before the BPDU (bridge protocol data unit) packet sent by the Switch will be discarded. Each switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BPDU packet and the information held for the port will age out. The user may set a hop count from 1 to 20. The default is 20.
TX Hold Count	Used to set the maximum number of Hello packets transmitted per interval. The count can be specified from 1 to 10. The default is 3.
Forwarding BPDU	This field can be <i>Enabled</i> or <i>Disabled</i> . When <i>Enabled</i> , it allows the forwarding of STP BPDU packets from other network devices. The default is Enabled.
Loopback Detection	This feature is used to temporarily block STP on the Switch when a BPDU packet has been looped back to the switch. When the Switch detects its own BPDU packet coming back, it signifies a loop on the network. STP will automatically be blocked and an alert will be sent to the administrator. The LBD STP port will restart (change to discarding state) when the LBD Recover Timer times out. The user may enable or disable this function using the pull-down menu. The default is Enabled.
LBD Recover Timer	This field will set the time the STP port will wait before recovering the STP state set. 0 will denote that the LBD will never time out or restart until the administrator personally changes it. The user may also set a time between 60 and 1000000 seconds. The default is 60 seconds.

Click **Apply** to implement changes made.



NOTE: The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur. Observe the following formulas when setting the above parameters:

Max. Age $\leq 2 \times$ (Forward Delay - 1 second)

Max. Age $\geq 2 \times$ (Hello Time + 1 second)

MST Configuration Identification

The following screens in the **MST Configuration Table** window allow the user to configure a MSTI instance on the Switch. These settings will uniquely identify a multiple spanning tree instance set on the Switch. The Switch initially possesses one *CIST* or Common Internal Spanning Tree of which the user may modify the parameters for but cannot change the MSTI ID for, and cannot be deleted. To view the **MST Configuration Identification** window, click **Configuration > Spanning Tree > MST Configuration Identification**:

MST Configuration Identification		
Configuration Name	Revision Level	
00:65:00:02:00:00	0	
MSTI ID	VID List	Delete
CIST	1-4094	Can't be Deleted!

MST Configuration Identification Settings	
Configuration Name	<input type="text" value="00:65:00:02:00:00"/>
Revision Level(0-65535)	<input type="text" value="0"/>
<input type="button" value="Apply"/>	

Figure 6- 17. MST Configuration Identification window

The window above contains the following information:

Parameter	Description
Configuration Name	A previously configured name set on the Switch to uniquely identify the MSTI (Multiple Spanning Tree Instance). If a configuration name is not set, this field will show the MAC address to the device running MSTP.
Revision Level	This value, along with the Configuration Name will identify the MSTP region configured on the Switch.
MSTI ID	This field shows the MSTI IDs currently set on the Switch. This field will always have the CIST MSTI, which may be configured but not deleted. Clicking the hyperlinked name will open a new window for configuring parameters associated with that particular MSTI.
VID List	This field displays the VLAN IDs associated with the specific MSTI.

To delete a previously set MSTI Instance ID, click the corresponding under the **Delete** heading in the **MST Configuration Identification** window. Clicking the **Add** button will reveal the following window to configure:

Instance ID Settings	
MSTI ID	<input type="text"/>
Type	Create ▾
VID List (1-4094)	<input type="checkbox"/> <input type="text"/>
<input type="button" value="Apply"/>	
Show MST Configuration Table	

Figure 6- 18. Instance ID Settings window- Add

The user may configure the following parameters to create a MSTI in the Switch.

Parameter	Description
MSTI ID	Enter a number between 1 and 15 to set a new MSTI on the Switch.
Type	<i>Create</i> is selected to create a new MSTI. No other choices are available for this field when creating a new MSTI.
VID List (1-4094)	This field is used to specify the VID range from configured VLANs set on the Switch. Supported VIDs on the Switch range from ID number 1 to 4094.

Click **Apply** to implement changes made.

To configure the settings for the CIST, click on its hyperlinked **MSTI ID** number in the **MST Configuration Identification** window, which will reveal the following window to configure:

Figure 6- 19. Instance ID Settings window - CIST modify

The user may configure the following parameters to configure the CIST on the Switch.

Parameter	Description
MSTI ID	The MSTI ID of the CIST is 0 and cannot be altered.
Type	This field allows the user to choose a desired method for altering the MSTI settings. The user has 2 choices. <ul style="list-style-type: none"> • <i>Add VID</i> - Select this parameter to add VIDs to the MSTI ID, in conjunction with the VID List parameter. • <i>Remove VID</i> - Select this parameter to remove VIDs from the MSTI ID, in conjunction with the VID List parameter.
VID List (1-4094)	This field is used to specify the VID range from configured VLANs set on the Switch. Supported VIDs on the Switch range from ID number 1 to 4094.

Click **Apply** to implement changes made.

To configure the parameters for a previously set MSTI, click on its hyperlinked **MSTI ID** number, which will reveal the following screen for configuration.

Figure 6- 20. Instance ID Settings window - Modify

The user may configure the following parameters for a MSTI on the Switch.

Parameter	Description
MSTI ID	Displays the MSTI ID previously set by the user.
Type	<p>This field allows the user to choose a desired method for altering the MSTI settings. The user has 2 choices.</p> <ul style="list-style-type: none"> • <i>Add VID</i> - Select this parameter to add VIDs to the MSTI ID, in conjunction with the VID List parameter. • <i>Remove VID</i> - Select this parameter to remove VIDs from the MSTI ID, in conjunction with the VID List parameter.
VID List (1-4094)	This field is used to specify the VID range from configured VLANs set on the Switch that the user wishes to add to this MSTI ID. Supported VIDs on the Switch range from ID number 1 to 4094. This parameter can only be utilized if the Type chosen is <i>Add</i> or <i>Remove</i> .

Click **Apply** to implement changes made.

MSTP Port Information

This window displays the current MSTI configuration settings and can be used to update the port configuration for an MSTI ID. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for interfaces to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest port number into the forwarding state and other interfaces will be blocked. Remember that lower priority values mean higher priorities for forwarding packets.

To view the following window, click **Configuration > Spanning Tree > MSTI Port Information**:

Unit	Port	Apply
1	Port1	Apply

MSTP Port Information-Port 1 of Unit 1					
Msti	Designated Bridge	Internal PathCost	Prio	Status	Role
0	N/A	200000	128	Disabled	Disabled

Figure 6- 21. MSTP Port Information window

To view the MSTI settings for a particular port, select the **Port** number, located in the top left hand corner of the screen and click **Apply**. To modify the settings for a particular **MSTI Instance**, click on its hyperlinked MSTI ID, which will reveal the following window.

MSTI Settings-Port 1 of Unit 1	
Instance ID	1
Internal cost(0=Auto)	0
Priority	128
Apply	
Show MSTP Port Information Table-Port 1 of Unit 1	

Figure 6- 22. MSTI Settings window

Parameter	Description
Instance ID	Displays the MSTI ID of the instance being configured. An entry of 0 in this field represents the CIST (default MSTI).
Internal cost	<p>This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within a STP instance. The default setting is 0 (auto). There are two options:</p> <ul style="list-style-type: none"> <i>0 (auto)</i> - Selecting this parameter for the <i>internalCost</i> will set quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface. <i>value 1-2000000</i> - Selecting this parameter with a value in the range of 1-2000000 will set the quickest route when a loop occurs. A lower Internal cost represents a quicker transmission.
Priority	Enter a value between 0 and 240 to set the priority for the port interface. A higher priority will designate the interface to forward packets first. A lower number denotes a higher priority. This entry must be divisible by 16. The default priority setting is 128.

Click **Apply** to implement changes made.

STP Instance Settings

The following window displays MSTIs currently set on the Switch. To view the following table, click **Configuration > Spanning Tree > STP Instance Settings**:

STP Instance Settings			
Instance Type	Instance Status	Instance Priority	Priority
CIST	Enabled	32768(bridge priority : 32768, sys ID ext : 0)	<input type="button" value="Modify"/>
MSTI(1)	Enabled	32769(bridge priority : 32768, sys ID ext : 1)	<input type="button" value="Modify"/>

Figure 6- 23. STP Instance Settings

The following information is displayed:

Parameter	Description
Instance Type	Displays the instance type(s) currently configured on the Switch. Each instance type is classified by a MSTI ID. CIST refers to the default MSTI configuration set on the Switch.
Instance Status	Displays the current status of the corresponding MSTI ID.
Instance Priority	Displays the priority of the corresponding MSTI Instance Type. The lowest priority will be the root bridge.
Priority	Click the Modify button to change the priority of the MSTI. This will open the Instance ID Settings window to configure. The Type field in this window will be permanently set to <i>Set Priority Only</i> . Enter the new priority in the Priority field and click Apply to implement the new priority setting.

Click **Apply** to implement changes made.

Clicking the hyperlinked name will allow the user to view the current parameters set for the MSTI Instance.

STP Instance Operational Status	
Designated Root Bridge	4096/00-01-27-32-26-95
External Root Cost	200004
Regional Root Bridge	32768/00-53-13-1a-33-24
Internal Root Cost	0
Designated Bridge	32768/00-50-ba-71-20-d6
Root Port	1
Max Age	20
Forward Delay	15
Last Topology Change	177
Topology Changes Count	157
Show STP Instance Table	



NOTE: In order to enable the hyperlink under the **Instance Type** heading in the **STP Instance Settings** window, users must first enable STP and set the version to MSTP. These settings are found in the **STP Bridge Global Settings** window mentioned previously in this chapter.

Figure 6- 24. STP Instance Operational Status – CIST

STP Instance Operational Status	
Regional Root Bridge	32770/00-53-13-1a-33-24
Internal Root Cost	0
Designated Bridge	32770/00-53-13-1a-33-24
Root Port	None
Remaining Hops	20
Last Topology Change	288
Topology Changes Count	3
Show STP Instance Table	

Figure 6- 25. STP Instance Operational Status – Previously Configured MSTI

The following parameters may be viewed in the **STP Instance Operational Status** windows:

Parameter	Description
Designated Root Bridge	This field will show the priority and MAC address of the Root Bridge.
External Root Cost	<p>This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is 0 (auto).</p> <ul style="list-style-type: none"> • <i>0 (auto)</i> - Setting 0 for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000. • <i>value 1-200000000</i> - Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.
Regional Root Bridge	This field will show the priority and MAC address of the Regional (Internal) Root Bridge. This MAC address should be the MAC address of the Switch.
Internal Root Cost	<p>This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within a STP instance. The default setting is 0 (auto). There are two options:</p> <ul style="list-style-type: none"> • <i>0 (auto)</i> - Selecting this parameter for the <i>internalCost</i> will set quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface. • <i>value 1-2000000</i> - Selecting this parameter with a value in the range of 1-2000000 will set the quickest route when a loop occurs. A lower Internal cost represents a quicker transmission.
Designated Bridge	This field will show the priority and MAC address of the Designated Bridge. The information shown in this table comes from a BPDU packet originating from this bridge.
Root Port	This is the port on the Switch that is physically connected to the Root Bridge.
Max Age	The Max Age may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the 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. The user may choose a time between 6 and 40 seconds. The default value is 20.
Forward Delay	The Forward Delay can be from 4 to 30 seconds. Any port on the Switch spends this time in the listening state while moving from the blocking state to the forwarding state.
Last Topology Change	This field shows the time, in seconds, since the last spanning tree topology change.
Topology Changes Count	This field displays the number of times that the spanning tree topology has changed since the original initial boot up of the Switch.

STP Port Settings

STP can be set up on a port per port basis. To view the following window click **Configuration > Spanning Tree > STP Port Settings**:

STP Port Settings									
Unit	From	To	External Cost (0=Auto)	Hello Time	Migrate	Edge	P2P	State	LBD State
1	Port 1	Port 1	0		No	False	True	Enabled	Disabled
Apply									
STP Port Information Table-Unit 1									
Port	External Cost	Hello Time	Edge	P2P	Port STP	LBD State			
1	AUTO/200000	2/2	No/No	Auto/Yes	Enabled	No			
2	AUTO/200000	2/2	No/No	Auto/Yes	Enabled	No			
3	AUTO/200000	2/2	No/No	Auto/Yes	Enabled	No			
4	AUTO/200000	2/2	No/No	Auto/Yes	Enabled	No			
5	AUTO/200000	2/2	No/No	Auto/Yes	Enabled	No			
6	AUTO/200000	2/2	No/No	Auto/Yes	Enabled	No			
7	AUTO/200000	2/2	No/No	Auto/Yes	Enabled	No			
8	AUTO/200000	2/2	No/No	Auto/Yes	Enabled	No			
9	AUTO/200000	2/2	No/No	Auto/Yes	Enabled	No			
10	AUTO/200000	2/2	No/No	Auto/Yes	Enabled	No			
11	AUTO/200000	2/2	No/No	Auto/Yes	Enabled	No			
12	AUTO/200000	2/2	No/No	Auto/Yes	Enabled	No			

Figure 6- 26. STP Port Settings and Table window

In addition to setting Spanning Tree parameters for use on the switch level, the Switch 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 based on 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.

It is advisable to define an STP Group to correspond to a VLAN group of ports.

The following fields can be set:

Parameter	Description
Unit	Choose the Switch ID number of the Switch in the switch stack to be modified.
From/To	A consecutive group of ports may be configured starting with the selected port.
External Cost	<p>External Cost - This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is 0 (auto).</p> <ul style="list-style-type: none"> • <i>0 (auto)</i> - Setting 0 for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000. • <i>value 1-200000000</i> - Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.
Hello Time	The time interval between the transmission of configuration messages by the designated port, to other devices on the bridged LAN, thus stating that the Switch is still functioning. The user may choose a time between 1 and 10 seconds. The default is 2 seconds. This field is only operable when the Switch is enabled for MSTP.

Migration	Setting this parameter as "yes" will set the ports to send out BPDU packets to other bridges, requesting information on their STP setting. If the Switch is configured for RSTP, the port will be capable to migrate from 802.1d STP to 802.1w RSTP. If the Switch is configured for MSTP, the port is capable of migrating from 802.1d STP to 802.1s MSTP. RSTP and MSTP can coexist with standard STP, however the benefits of RSTP and MSTP are not realized on a port where an 802.1d network connects to an 802.1w or 802.1s enabled network. Migration should be set as yes on ports connected to network stations or segments that are capable of being upgraded to 802.1w RSTP or 802.1s MSTP on all or some portion of the segment.
Edge	Choosing the true parameter designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received, it automatically loses edge port status. Choosing the false parameter indicates that the port does not have edge port status.
P2P	Choosing the <i>True</i> parameter indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports, however they are restricted in that a P2P port must operate in full-duplex. Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A p2p value of <i>false</i> indicates that the port cannot have p2p status. <i>Auto</i> allows the port to have p2p status whenever possible and operate as if the p2p status were true. If the port cannot maintain this status, (for example if the port is forced to half-duplex operation) the p2p status changes to operate as if the p2p value were <i>False</i> . The default setting for this parameter is <i>True</i> .
State	This drop-down menu allows you to enable or disable STP for the selected group of ports. The default is <i>Enabled</i> .
LBD State	Use the pull-down menu to enable or disable the loop-back detection function on the switch for the ports configured above. For more information on this function, see the STP Loopback Detection section.

Click **Apply** to implement changes made.

Forwarding & Filtering

Unicast Forwarding

Open the **Forwarding & Filtering** folder in the **Configuration** menu and click on the **Unicast Forwarding** link. This will open the **Setup Static Unicast Forwarding Table**, as shown below:

The screenshot shows two windows. The top window, titled "Setup Static Unicast Forwarding Table", has a header bar and a table with four columns: "VLAN ID", "MAC Address", "Unit", and "Port". The "VLAN ID" field contains "1", "MAC Address" contains "00:00:00:00:00:00", "Unit" is a dropdown set to "1", and "Port" is a dropdown set to "Port 1". An "Add" button is located to the right of the table. Below this is a second window titled "Static Unicast Forwarding Table" with a header bar and a table with six columns: "MAC Address", "VID", "VLAN Name", "Unit", "Port", and "Delete". The table is currently empty, and the text "End of data!" is displayed at the bottom.

Figure 6- 27. Setup Static Unicast Forwarding Table and Static Unicast Forwarding Table window

To add or edit an entry, define the following parameters and then click **Add**:

Parameter	Description
VLAN ID (VID)	The VLAN ID number of the VLAN on which the above Unicast MAC address resides.
MAC Address	The MAC address to which packets will be statically forwarded. This must be a unicast MAC address.
Unit	Choose the Switch ID number of the line card in the chassis to be modified.
Port	Allows the selection of the port number on which the MAC address entered above resides.

Click **Apply** to implement the changes made. Current entries can be found in the **Static Unicast Forwarding Table** as shown in the bottom half of the figure above. To delete an entry in the **Static Unicast Forwarding Table**, click the corresponding **X** under the **Delete** heading.

Static Multicast Forwarding

The following figure and table describe how to set up **Multicast Forwarding** on the Switch. Open the **Forwarding & Filtering** folder in the **Configuration** menu, and click on the **Multicast Forwarding** link to see the entry screen below:

The screenshot shows two windows. The top window, titled "Static Multicast Forwarding Settings", has a header bar and a section titled "Add new Multicast Forwarding Settings" with an "Add" button. Below this is a second window titled "Current Multicast Forwarding Entries" with a header bar and a table with five columns: "VLAN ID", "MAC Address", "Type", "Modify", and "Delete". The table is currently empty.

Figure 6- 28. Static Multicast Forwarding Settings and Current Multicast Forwarding Entries window

The **Static Multicast Forwarding Settings** page displays all of the entries made into the Switch's static multicast forwarding table. Click the **Add** button to open the **Setup Static Multicast Forwarding Table**, as shown below:

Setup Static Multicast Forwarding Table																								
Unit	VID	Multicast MAC Address																						
1		00:00:00:00:00:00																						
Port Settings	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
None	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Egress	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
																							Apply	
Show All Multicast Forwarding Entries																								

Figure 6- 29. Setup Static Multicast Forwarding Table

The following parameters can be set:

Parameter	Description
Unit	Choose the Switch ID number of the Switch in the switch stack to be modified.
VID	The VLAN ID of the VLAN to which the corresponding MAC address belongs.
Multicast MAC Address	The MAC address of the static source of multicast packets. This must be a multicast MAC address.
Port	Allows the selection of ports that will be members of the static multicast group. The options are: <i>None</i> - No restrictions on the port dynamically joining the multicast group. When None is chosen, the port will not be a member of the Static Multicast Group. <i>Egress</i> - The port is a static member of the multicast group.

Click **Apply** to implement the changes made. To delete an entry in the **Static Multicast Forwarding Table**, click the corresponding under the **Delete** heading. Click the [Show All Multicast Forwarding Entries](#) link to return to the **Static Multicast Forwarding Settings** window.

VLANs

Understanding IEEE 802.1p Priority

Priority tagging is a function defined by the IEEE 802.1p standard designed to provide a means of managing traffic on a network where many different types of data may be transmitted simultaneously. It is intended to alleviate problems associated with the delivery of time critical data over congested networks. The quality of applications that are dependent on such time critical data, such as video conferencing, can be severely and adversely affected by even very small delays in transmission.

Network devices that are in compliance with the IEEE 802.1p standard have the ability to recognize the priority level of data packets. These devices can also assign a priority label or tag to packets. Compliant devices can also strip priority tags from packets. This priority tag determines the packet's degree of expeditiousness and determines the queue to which it will be assigned.

Priority tags are given values from 0 to 7 with 0 being assigned to the lowest priority data and 7 assigned to the highest. The highest priority tag 7 is generally only used for data associated with video or audio applications, which are sensitive to even slight delays, or for data from specified end users whose data transmissions warrant special consideration.

The Switch allows you to further tailor how priority tagged data packets are handled on your network. Using queues to manage priority tagged data allows you to specify its relative priority to suit the needs of your network. There may be circumstances where it would be advantageous to group two or more differently tagged packets into the same queue. Generally, however, it is recommended that the highest priority queue, Queue 1, be reserved for data packets with a priority value of 7. Packets that have not been given any priority value are placed in Queue 0 and thus given the lowest priority for delivery.

A weighted round robin system is employed on the Switch to determine the rate at which the queues are emptied of packets. The ratio used for clearing the queues is 4:1. This means that the highest priority queue, Queue 1, will clear 4 packets for every 1 packet cleared from Queue 0.

Remember, the priority queue settings on the Switch are for all ports, and all devices connected to the Switch will be affected. This priority queuing system will be especially beneficial if your network employs switches with the capability of assigning priority tags.

VLAN Description

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 in the xStack[®] DES-6500 Modular Layer 3 Chassis Ethernet Switch

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.

The xStack[®] DES-6500 chassis switch supports IEEE 802.1Q VLANs, Port-Based VLANs and Protocol-Based 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.

The Switch's default is to assign all ports to a single 802.1Q VLAN named "default."

The "default" VLAN has a VID = 1.

The member ports of Port-based VLANs may overlap, if desired.

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 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 allows 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 whether to filter or forward the packet.
 - Egress rules - determines if the packet must be sent tagged or untagged.

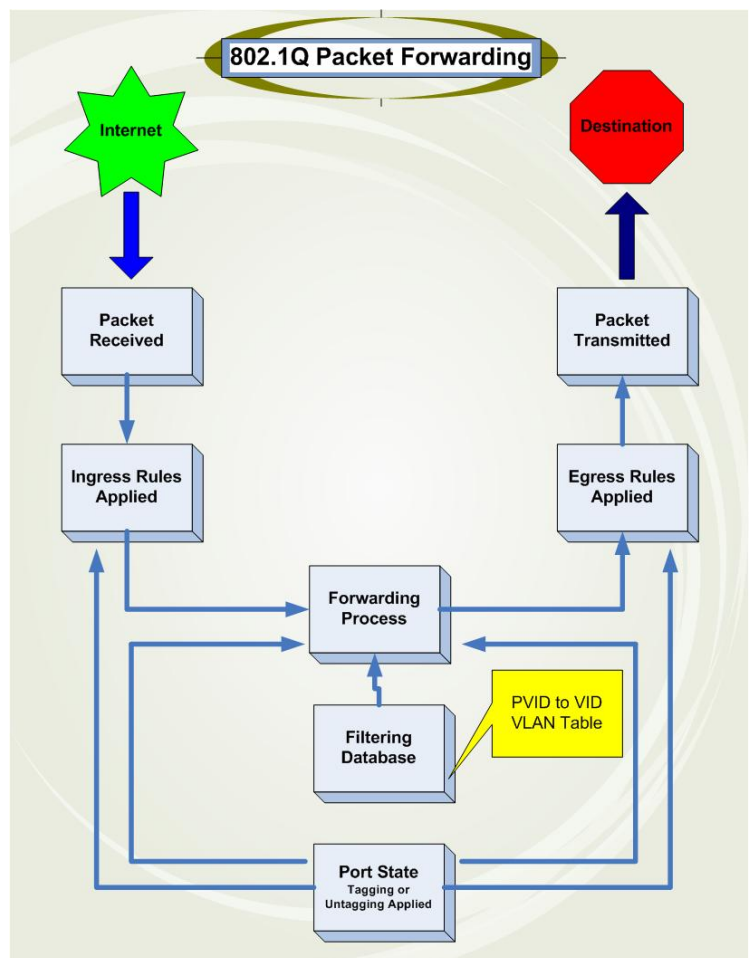


Figure 6- 30. IEEE 802.1Q Packet Forwarding

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 of 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 four octets. All of the information originally contained in the packet is retained.

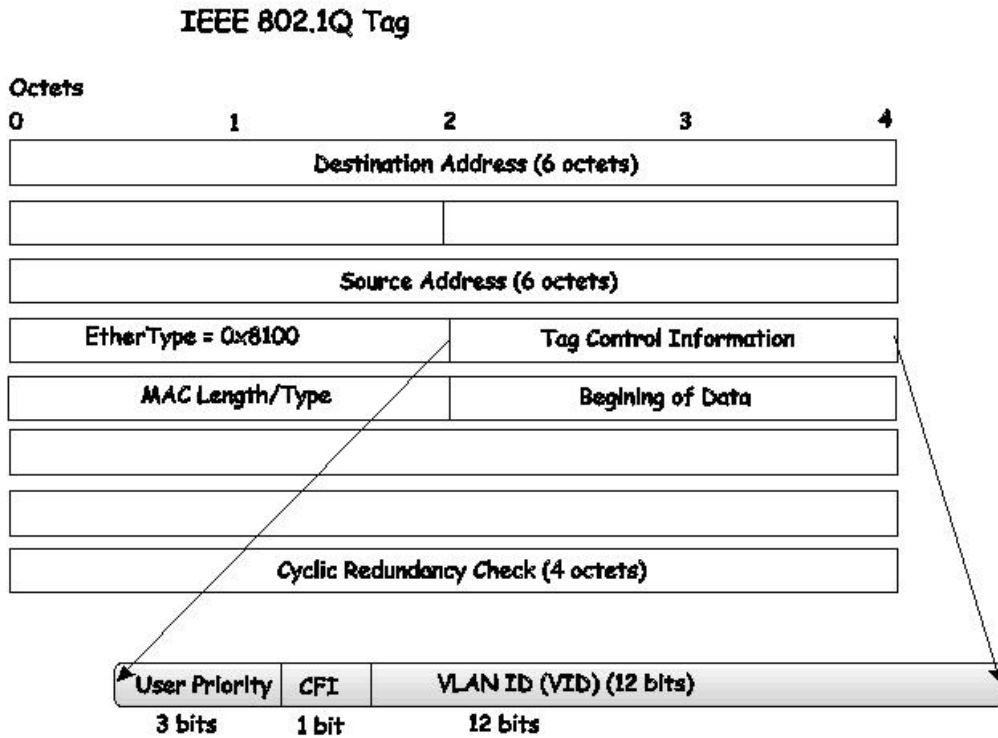


Figure 6- 31. IEEE 802.1Q Tag

The EtherType and VLAN ID are inserted after the MAC source address, but before the original 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.

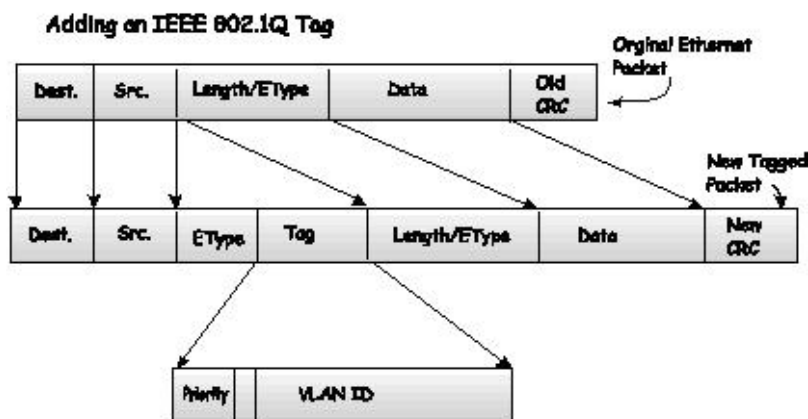


Figure 6- 32. Adding an IEEE 802.1Q Tag

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 of 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.

Default VLANs

The Switch initially configures one VLAN, VID = 1, called "default." The factory default setting assigns all ports on the Switch to the "default." As new VLANs are configured in Port-based mode, their respective member ports are removed from the "default."

Packets cannot cross VLANs. If a member of one VLAN wants to connect to another VLAN, the link must be through an external router.



NOTE: If no VLANs are configured on the Switch, 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.

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

Table 6- 2. VLAN Example - Assigned Ports

Port-based VLANs

Port-based VLANs limit traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department.

On port-based VLANs, NICs do not need to be able to identify 802.1Q tags in packet headers. NICs send and receive normal Ethernet packets. If the packet's destination lies on the same segment, communications take place using normal Ethernet protocols. Even though this is always the case, when the destination for a packet lies on another switch port, VLAN considerations come into play to decide if the packet is dropped by the Switch or delivered.

VLAN Segmentation

Take for example a packet that is transmitted by a machine on Port 1 that is a member of VLAN 2. If the destination lies on another port (found through a normal forwarding table lookup), the Switch then looks to see if the other port (Port 10) is a member of VLAN 2 (and can therefore receive VLAN 2 packets). If Port 10 is not a member of VLAN 2, then the packet will be dropped by the Switch and will not reach its destination. If Port 10 is a member of VLAN 2, the packet will go through. This selective forwarding feature based on VLAN criteria is how VLANs segment networks. The key point being that Port 1 will only transmit on VLAN 2.

Certain network resources can be shared across VLANs. This is achieved by setting up overlapping VLANs. That is ports can belong to more than one VLAN group. For example, setting VLAN 1 members to ports 1, 2, 3, and 4 and VLAN 2 members to ports 1, 5, 6, and 7. Port 1 belongs to two VLAN groups. Ports 8, 9, and 10 are not configured to any VLAN group. This means ports 8, 9, and 10 are in the same VLAN group.

VLAN and Trunk Groups

The members of a trunk group have the same VLAN setting. Any VLAN setting on the members of a trunk group will apply to the other member ports.



NOTE: In order to use VLAN segmentation in conjunction with port trunk groups, first set the port trunk group(s), and then configure VLAN settings. If changing the port trunk grouping with VLANs already in place, reconfiguring the VLAN settings after changing the port trunk group settings will not be necessary. VLAN settings will automatically change in conjunction with the change of the port trunk group settings.

Protocol VLANs

The xStack[®] DES-6500 chassis switch incorporates protocol-based VLANs. This standard, defined by the IEEE 802.1v standard maps packets to protocol-defined VLANs by examining the type octet within the packet header to discover the type of protocol associated with it. After assessing the protocol, the Switch will forward the packets to all ports within the protocol-assigned VLAN. This feature will benefit the administrator by better balancing load sharing and enhancing traffic classification. The Switch supports fourteen (14) pre-defined protocols for configuration. The user may also choose a protocol that is not one of the fourteen defined protocols by properly configuring the *userDefined* protocol VLAN. The supported protocols for the protocol VLAN function on this switch include IP, IPX, DEC LAT, SNAP, NetBIOS, AppleTalk, XNS, SNA, IPv6, RARP and VINES.

The following is a list of type headers for each protocol listed for VLAN configuration.

Protocol	Type Header in Hexadecimal Form
IP over Ethernet	0x0800
IPX 802.3	0xFFFF
IPX 802.2	0xE0E0
IPX SNAP	0x8137
IPX over Ethernet2	0x8137
decLAT	0x6000
SNA 802.2	0x0404
netBios	0xF0F0
XNS	0x0600
VINES	0x0BAD
IPV6	0x86DD
AppleTalk	0x809B
RARP	0x8035
SNA over Ethernet2	0x80D5

Table 6- 3. Protocol VLAN and the corresponding type header

In configuring the user-defined protocol, the administrator must make sure that the pre-defined user type header does not match any other type header. A match may cause discrepancies within the local network and failure to define the VLAN to which to forward packets.

VLAN Entry

In the **Configuration** folder, open the **VLAN** folder and click the **VLAN Entry** link to open the following window:

Total Entries : 1			
Add			
Current 802.1Q VLANs Entries			
VLAN ID	VLAN name	Advertisement	Delete
1	default	Enabled	X

Figure 6- 33. Current 802.1Q Static VLANs Entries window

The **802.1Q Static VLANs** menu lists all previously configured VLANs by **VLAN ID** and **VLAN Name**. To delete an existing 802.1Q VLAN, click the corresponding **X** button under the **Delete** heading.

To create a new 802.1Q VLAN, click the **Add** button in the **802.1Q Static VLANs** menu. A new menu will appear, as shown below, to configure the port settings and to assign a unique name and number to the new VLAN. See the table below for a description of the parameters in the new menu.

802.1Q VLANs																								
Unit	VID	VLAN Name																		Advertisement				
1																				Disabled				
Type	Protocol ID			User Defined Packet ID												Encap								
	port																							
Port Settings	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Tag	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Egress	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Forbidden	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Member																								
																								Apply
Show All Static VLAN Entries																								

Figure 6- 34. 802.1Q Static VLANs - Add

To return to the **Current 802.1Q Static VLANs Entries** window, click the [Show All Static VLAN Entries](#) link. To change an existing 802.1Q VLAN entry, click the hyperlinked **VLAN ID** button of the corresponding entry to modify. A new menu will appear to configure the port settings and to assign a unique name and number to the new VLAN. See the table below for a description of the parameters in the new menu.

802.1Q VLANs																								
Unit	VID	VLAN Name																		Advertisement				
1	1	default																		Enabled				
Type	Protocol ID			User Defined Packet ID												Encap								
1QVLAN	port																							
Port Settings	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Tag	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
None	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Egress	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Forbidden	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Member	1:1-1:12,2:1-2:8,3:1-3:16,4:1-4:24																							
																								Apply
Show All Static VLAN Entries																								

Figure 6- 35. 802.1Q Static VLANs Entry Settings - Modify

The following fields can then be set in either the **Add** or **Modify 802.1Q Static VLANs** menus:

Parameter	Description
Unit	Choose the Switch ID number of the line card in the chassis to be modified.
VID (VLAN ID)	Allows the entry of a VLAN ID in the Add dialog box, or displays the VLAN ID of an existing VLAN in the Modify dialog box. VLANs can be identified by either the VID or the VLAN name.
VLAN Name	Allows the entry of a name for the new VLAN in the Add dialog box, or will display the VLAN name.
Advertisement	Enabling this function will allow the Switch to send out GVRP packets to outside sources, notifying that they may join the existing VLAN.
Type	Displays the type of protocol associated with this VLAN.
Protocol ID	<p>The following parameters allow for the creation of protocol-based VLANs. The Switch supports 14 pre-configured protocol-based VLANs plus one user-defined protocol based VLAN where the administrator may configure the settings for the appropriate protocol and forwarding of packets (15 total). Selecting a specific protocol will indicate which protocol will be utilized in determining the VLAN ownership of a tagged packet. Pre-set protocol-based VLANs on the Switch include:</p> <p><i>port</i> – Using this parameter will allow the creation of a normal 802.1Q VLAN on the Switch.</p> <p><i>ip</i> – Using this parameter will instruct the Switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is based on the Ethernet protocol.</p> <p><i>rarp</i> - Using this parameter will instruct the Switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by the Reverse Address Resolution (RARP) Protocol.</p> <p><i>ipx802dot3</i> - Using this parameter will instruct the Switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by Novell NetWare 802.3 (IPX - Internet Packet Exchange).</p> <p><i>ipx802dot2</i> - Using this parameter will instruct the Switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by Novell NetWare 802.2 (IPX - Internet Packet Exchange).</p> <p><i>ipxSnap</i> - Using this parameter will instruct the Switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by Novell and the Sub Network Access Protocol (SNAP).</p> <p><i>ipxEthernet2</i> - Using this parameter will instruct the Switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by Novell Ethernet II Protocol.</p> <p><i>appleTalk</i> - Using this parameter will instruct the Switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by the AppleTalk protocol.</p> <p><i>decLAT</i> - Using this parameter will instruct the Switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by the Digital Equipment Corporation (DEC) Local Area Transport (LAT) protocol.</p> <p><i>sna802dot2</i> - Using this parameter will instruct the Switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by the Systems Network Architecture (SNA) 802.2 Protocol.</p> <p><i>snaEthernet2</i> - Using this parameter will instruct the Switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by the Systems Network Architecture (SNA) Ethernet II Protocol.</p> <p><i>netBios</i> - Using this parameter will instruct the Switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by the NetBIOS Protocol.</p> <p><i>xns</i> - Using this parameter will instruct the Switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by the Xerox Network Systems (XNS) Protocol.</p>

	<p><i>vines</i> - Using this parameter will instruct the Switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by the Banyan Virtual Integrated Network Service (VINES) Protocol.</p> <p><i>ipV6</i> - Using this parameter will instruct the Switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol. This packet header information is defined by the Internet Protocol Version 6 (IPv6) Protocol.</p> <p><i>userDefined</i> - Using this parameter will instruct the Switch to forward packets to this VLAN if the tag in the packet header is concurrent with this protocol defined by the user. This packet header information is defined by entering the following information:</p> <p><i>User Defined Pid</i> - Specifies that the VLAN will only accept packets with this hexadecimal 802.1Q Ethernet type value in the packet header. The user may define an entry, in the hexadecimal form (ffff) to define the packet identification. <i>(The user only need enter the final four integers of the hexadecimal format to define the packet ID – {hex 0x0 0xffff})</i> This field is only operable if <i>userDefined</i> is selected in the Protocol ID field.</p> <p><i>encap [ethernet llc snap all]</i> – Specifies that the Switch will examine the octet of the packet header referring to one of the protocols listed (Ethernet, LLC or SNAP), looking for a match of the hexadecimal value previously entered . <i>all</i> will instruct the Switch to examine the total packet header. After a match is found, the Switch will forward the packet to this VLAN. This field is only operable if <i>userDefined</i> is selected in the Protocol ID field.</p>
Port Settings	Allows an individual port to be specified as member of a VLAN.
Tag	Specifies the port as either 802.1Q tagging or 802.1Q untagged. Checking the box will designate the port as Tagged.
None	Allows an individual port to be specified as a non-VLAN member.
Egress	Select this to specify the port as 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.
Forbidden	Select this to specify the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically.

Click **Apply** to implement changes made. Click the [Show All Static VLAN Entries](#) link to return to the **Current 802.1Q Static VLAN Entries** window.

GVRP Settings

In the **Configuration** menu, open the **VLANs** folder and click **GVRP Settings**.

The **GVRP Settings** dialog box, shown below, allows users to determine whether the Switch will share its VLAN configuration information with other GARP VLAN Registration Protocol (GVRP) enabled switches. In addition, **Ingress Checking** can be used to limit traffic by filtering incoming packets whose PVID does not match the PVID of the port. Results can be seen in the table under the configuration settings, as seen below.

GVRP Settings							
Unit	From	To	State	Ingress Check	Acceptable Frame Type	PVID	Apply
1	Port 1	Port 1	Disabled	Enabled	All		Apply

GVRP Table				
Port	PVID	GVRP	Ingress Check	Acceptable Frame Type
1	1	Disabled	Enabled	All Frames
2	1	Disabled	Enabled	All Frames
3	1	Disabled	Enabled	All Frames
4	1	Disabled	Enabled	All Frames
5	1	Disabled	Enabled	All Frames
6	1	Disabled	Enabled	All Frames
7	1	Disabled	Enabled	All Frames
8	1	Disabled	Enabled	All Frames
9	1	Disabled	Enabled	All Frames
10	1	Disabled	Enabled	All Frames
11	1	Disabled	Enabled	All Frames
12	1	Disabled	Enabled	All Frames

Figure 6- 36. GVRP Settings and GVRP Table window

The following fields can be set:

Parameter	Description
Unit	Choose the Switch ID number of the line card in the chassis to be modified.
From/To	These two fields allow users to specify the range of ports that will be included in the Port-based VLAN that you are creating using the GVRP Settings page.
GVRP	The Group VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN. GVRP is <i>Disabled</i> by default.
Ingress Check	This field can be toggled using the space bar between <i>Enabled</i> and <i>Disabled</i> . <i>Enabled</i> 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. <i>Disabled</i> disables ingress filtering. Ingress Checking is <i>Enabled</i> by default.
Acceptable Frame Type	This field denotes the type of frame that will be accepted by the port. The user may choose between <i>Tagged Only</i> , which means only VLAN tagged frames will be accepted, and <i>Admit_All</i> , which means both tagged and untagged frames will be accepted. <i>Admit_All</i> is enabled by default.
PVID	<p>Within the GVRP Settings above, the user may specify the default VLAN ID to be associated with the port being configured for GVRP.</p> <p>The read only field in the GVRP Table shows the current PVID assignment for each port, which may be manually assigned to a VLAN when created in the 802.1Q Port Settings table. The Switch's default is to assign all ports to the default VLAN with a VID of 1. 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 to accept only tagged frames - as tagging, and an untagged packet is 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.</p>

Click **Apply** to implement changes made.

Traffic Control

On a computer network, packets such as Multicast packets and Broadcast packets continually flood the network as normal procedure. At times, this traffic may increase do to a malicious endstation on the network or a malfunctioning device, such as a faulty network card. Thus, switch throughput problems will arise and consequently affect the overall performance of the switch network. To help rectify this packet storm, the Switch will monitor and control the situation.

The packet storm is monitored to determine if too many packets are flooding the network, based on the threshold level provided by the user. Once a packet storm has been detected, the Switch will drop packets coming into the Switch until the storm has subsided. This method can be utilized by selecting the **Drop** option of the **Action** field in the window below.

The Switch will also scan and monitor packets coming into the Switch by monitoring the Switch's chip counter. This method is only viable for Broadcast and Multicast storms because the chip only has counters for these two types of packets. Once a storm has been detected (that is, once the packet threshold set below has been exceeded), the Switch will shutdown the port to all incoming traffic with the exception of STP BPDU packets, for a time period specified using the CountDown field.

If this field times out and the packet storm continues, the port will be placed in a Shutdown Forever mode which will produce a warning message to be sent to the Trap Receiver. Once in Shutdown Forever mode, the only method of recovering this port is to manually recoup it using the **Port Configuration** window in the **Administration** folder and selecting the disabled port and returning it to an Enabled status. To utilize this method of Storm Control, choose the **Shutdown** option of the **Action** field in the window below. To view this window to configure Traffic Control, click **Security > Traffic Control**.

To view the following window to configure Traffic Control, click **Configuration > Traffic Control**.

The screenshot shows the 'Storm Control Recover' window with the following sections:

- Storm Control Recover:** Unit: 1, From: Port 1, To: Port 1, Apply button.
- Storm Trap Configuration:** Storm Trap: None, Apply button.
- Storm Control Settings:**

Unit	From	To	Broadcast	Multicast	DLF	Action	Threshold	CountDown	Interval	Apply
1	Port 1	Port 1	Disabled	Disabled	Disabled	Drop	1024	0	5	Apply
- Storm Control Table:**

Port	Broadcast	Multicast	DLF	Action	Threshold	Count Down	Time Interval	Forever
1	Disabled	Disabled	Disabled	drop	128	0	5	
2	Disabled	Disabled	Disabled	drop	128	0	5	
3	Disabled	Disabled	Disabled	drop	128	0	5	
4	Disabled	Disabled	Disabled	drop	128	0	5	
5	Disabled	Disabled	Disabled	drop	128	0	5	
6	Disabled	Disabled	Disabled	drop	128	0	5	
7	Disabled	Disabled	Disabled	drop	128	0	5	
8	Disabled	Disabled	Disabled	drop	128	0	5	
9	Disabled	Disabled	Disabled	drop	128	0	5	
10	Disabled	Disabled	Disabled	drop	128	0	5	
11	Disabled	Disabled	Disabled	drop	128	0	5	
12	Disabled	Disabled	Disabled	drop	128	0	5	

Figure 6- 37. Traffic Control Settings and Traffic Control Table window

The user may set the following parameters:

Parameter	Description
Storm Control Recover	
Unit	Select the Unit of the line card in the chassis where the Shutdown port resides.
From... To	Select the ports to be manually recovered from the Shutdown state.
Storm Trap Configuration	
Storm Trap	<p>Enable sending of Storm Trap messages when the type of action taken by the Traffic Control function in handling a Traffic Storm is one of the following:</p> <p><i>None</i> – Will send no Storm trap warning messages regardless of action taken by the Traffic Control mechanism.</p> <p><i>Storm Occurred</i> – Will send Storm Trap warning messages upon the occurrence of a Traffic Storm only.</p> <p><i>Storm Cleared</i> – Will send Storm Trap messages when a Traffic Storm has been cleared by the Switch only.</p> <p><i>Both</i> – Will send Storm Trap messages when a Traffic Storm has been both detected and cleared by the Switch.</p> <p>This function cannot be implemented in the Hardware mode. (When Drop is chosen in the Action field.</p>
Storm Control Settings	
Unit	Select the Unit of the line card in the chassis to configure for Storm Control.
From...To	Select the ports of this Switch to configure for Storm Control.
Broadcast	Enables or disable Broadcast Storm Control.
Multicast	Enables or disables Multicast Storm Control.
DLF	Enables or disables Destination Lookup Failure (DLF) storm control. (Not available for Software based Traffic Control { <i>Shutdown</i> }).
Action	<p>Select the method of traffic Control from the pull down menu. The choices are:</p> <p><i>Drop</i> – Utilizes the hardware Traffic Control mechanism, which means the Switch's hardware will determine the Packet Storm based on the Threshold value stated and drop packets until the issue is resolved.</p> <p><i>Shutdown</i> – Utilizes the Switch's software Traffic Control mechanism to determine the Packet Storm occurring. Once detected, the port will deny all incoming traffic to the port except STP BPDU packets, which are essential in keeping the Spanning Tree operational on the Switch. If the Countdown timer has expired and yet the Packet Storm continues, the port will be placed in Shutdown Forever mode and is no longer operational until the user manually resets the port using the Storm Control Recover setting at the top of this window. Choosing this option obligates the user to configure the Interval setting as well, which will provide packet count samplings from the Switch's chip to determine if a Packet Storm is occurring.</p>
Threshold	Specifies the maximum number of packets per second that will trigger the Traffic Control function to commence. This entry should be made in multiples of 128. Other entries will be set internally closest to the multiple of 128. The configurable threshold range is from 0-2047 with a default setting of 1024.
Count Down	The Count Down timer is set to determine the amount of time, in minutes, that the Switch will wait before shutting down the port that is experiencing a traffic storm. This parameter is only useful for ports configured as Shutdown in their Action field and therefore will not operate for Hardware based Traffic Control implementations. The possible time settings for this field are 0, 5-30 minutes. 0 is the default setting for this field and 0 will denote that the port will never shutdown.

Interval	The Interval will set the time between Multicast and Broadcast packet counts sent from the Switch's chip to the Traffic Control function. These packet counts are the determining factor in deciding when incoming packets exceed the Threshold value. The Interval may be set between 5 and 10 seconds with the default setting of 5 seconds.
-----------------	--

Click Apply to implement the settings of each field.



NOTE: Traffic Control cannot be implemented on ports that are set for Link Aggregation (Port Trunking).



NOTE: Ports that are in the Shutdown forever mode will be seen as Discarding in Spanning Tree windows and implementations though these ports will still be forwarding BPDUs to the Switch's CPU.



NOTE: Ports that are in Shutdown Forever mode will be seen as link down in all windows and screens until the user recovers these ports.

Port Security

A given ports' (or a range of ports') dynamic MAC address learning can be locked such that the current source MAC addresses entered into the MAC address forwarding table can not be changed once the port lock is enabled. The port can be locked by using the **Admin State** pull-down menu to *Enabled*, and clicking **Apply**.

Port Security is a security feature that prevents unauthorized computers (with source MAC addresses) unknown to the Switch prior to locking the port (or ports) from connecting to the Switch's locked ports and gaining access to the network. To view the following window, click **Configuration > Port Security**.

Port Security Settings						
Unit	From	To	Admin State	Max.Addr(0-64)	Mode	Apply
1	Port 1	Port 1	Disabled	0	Permanent	Apply

Port Security Table			
Port	Admin State	Max.Learning Addr	Lock Address Mode
1	Disabled	1	DeleteOnReset
2	Disabled	1	DeleteOnReset
3	Disabled	1	DeleteOnReset
4	Disabled	1	DeleteOnReset
5	Disabled	1	DeleteOnReset
6	Disabled	1	DeleteOnReset
7	Disabled	1	DeleteOnReset
8	Disabled	1	DeleteOnReset
9	Disabled	1	DeleteOnReset
10	Disabled	1	DeleteOnReset
11	Disabled	1	DeleteOnReset
12	Disabled	1	DeleteOnReset

Figure 6- 38. Port Security Settings and Table window

The following parameters can be set:

Parameter	Description
Unit	Choose the Switch ID number of the line card in the chassis to be modified.
From/To	A consecutive group of ports may be configured starting with the selected port.
Admin State	This pull-down menu allows you to enable or disable Port Security (locked MAC address table for the selected ports).
Max. Addr (0-64)	The number of MAC addresses that will be in the MAC address forwarding table for the selected switch and group of ports.
Mode	This pull-down menu allows users to select how the MAC address table locking will be implemented on the Switch, for the selected group of ports. The options are: <ul style="list-style-type: none"> • <i>Permanent</i> – The locked addresses will not age out after the aging timer expires. • <i>DeleteOnTimeout</i> – The locked addresses will age out after the aging timer expires. • <i>DeleteOnReset</i> – The locked addresses will not age out until the Switch has been reset.

Click **Apply** to implement changes made.

Port Lock Entries

The **Port Lock Entry Delete** window is used to remove an entry from the port security entries learned by the Switch and entered into the forwarding database. To view the following window, click **Configuration > Port Lock Entries**:

Port Lock Entries Table						
VID	VLAN Name	MAC Address	Unit	Port	Type	Delete
1	default	00-00-80-c8-09-89	1	11	Secured_Permanent	<input type="checkbox"/>
1	default	00-01-30-10-00-0b	1	11	Secured_Permanent	<input type="checkbox"/>
1	default	00-02-06-12-34-56	1	11	Secured_Permanent	<input type="checkbox"/>
1	default	00-02-a5-9a-f5-61	1	11	Secured_Permanent	<input type="checkbox"/>
1	default	00-03-09-18-10-01	1	11	Secured_Permanent	<input type="checkbox"/>
1	default	00-04-13-04-03-01	1	11	Secured_Permanent	<input type="checkbox"/>
1	default	00-05-5d-ed-84-ea	1	11	Secured_Permanent	<input type="checkbox"/>
1	default	00-06-01-01-01-00	1	11	Secured_Permanent	<input type="checkbox"/>
1	default	00-08-02-54-0e-9d	1	11	Secured_Permanent	<input type="checkbox"/>
1	default	00-08-02-54-0f-ce	1	11	Secured_Permanent	<input type="checkbox"/>
1	default	00-0c-6e-12-e1-1a	1	11	Secured_Permanent	<input type="checkbox"/>
1	default	00-0c-6e-1f-9c-aa	1	11	Secured_Permanent	<input type="checkbox"/>
1	default	00-0c-6e-35-90-ee	1	11	Secured_Permanent	<input type="checkbox"/>
1	default	00-0c-6e-d5-5b-f0	1	11	Secured_Permanent	<input type="checkbox"/>
1	default	00-0c-f8-20-90-01	1	11	Secured_Permanent	<input type="checkbox"/>
1	default	00-0c-f8-3e-e0-0d	1	11	Secured_Permanent	<input type="checkbox"/>
1	default	00-0c-f8-42-c0-01	1	11	Secured_Permanent	<input type="checkbox"/>
1	default	00-0c-f8-44-10-01	1	11	Secured_Permanent	<input type="checkbox"/>
1	default	00-0e-a6-01-d5-6c	1	11	Secured_Permanent	<input type="checkbox"/>
1	default	00-0e-a6-11-7c-5f	1	11	Secured_Permanent	<input type="checkbox"/>

Figure 6- 39. Port Lock Entries Table

This function is only operable if the **Mode** in the **Port Security** window is selected as **Permanent** or **DeleteOnReset**, or in other words, only addresses that are permanently learned by the Switch can be deleted. Once the entry has been defined by entering the correct information into the window above, click the under the **Delete** heading of the corresponding MAC address to be deleted. Click the **Next** button to view the next page of entries listed in this table. This window displays the following information:

Parameter	Description
VID	The VLAN ID of the entry in the forwarding database table that has been permanently learned by the Switch.
VLAN NAME	The VLAN Name of the entry in the forwarding database table that has been permanently learned by the Switch.
MAC Address	The MAC address of the entry in the forwarding database table that has been permanently learned by the Switch.
Unit	The ID number of the line card in the chassis that has permanently learned the MAC address.
Port	The ID number of the port that has permanently learned the MAC address.
Type	The type of MAC address in the forwarding database table. Only entries marked Secured Permanent can be deleted.
Delete	Click the <input type="checkbox"/> in this field to delete the corresponding MAC address that was permanently learned by the Switch.

QoS

The xStack[®] DES-6500 chassis switch supports 802.1p priority queuing Quality of Service. The following section discusses the implementation of QoS (Quality of Service) and the benefits of using 802.1p priority queuing.

The Advantages of QoS

QoS is an implementation of the IEEE 802.1p standard that allows network administrators a method of reserving bandwidth for important functions that require a large bandwidth or have a high priority, such as VoIP (voice-over Internet Protocol), web browsing applications, file server applications or video conferencing. Not only can a larger bandwidth be created, but other less critical traffic can be limited, so excessive bandwidth can be saved. The Switch has separate hardware queues on every physical port to which packets from various applications can be mapped to, and, in turn prioritized. View the following map to see how the xStack[®] DES-6500 chassis switch implements basic 802.1P priority queuing.

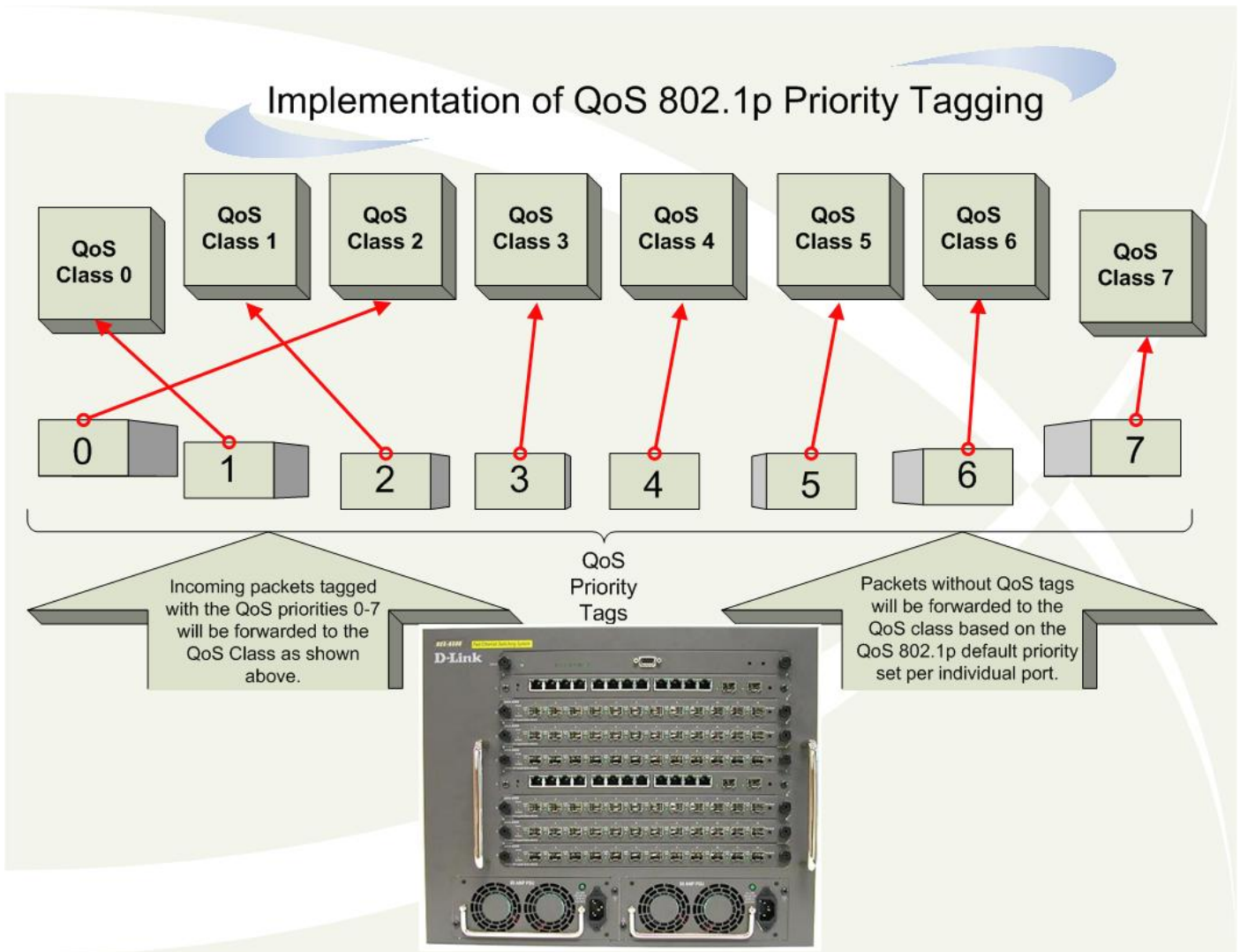


Figure 6- 40. An Example of the Default QoS Mapping on the Switch

The picture above shows the default priority setting for the Switch. Class-6 has the highest priority of the seven priority classes of service on the Switch. In order to implement QoS, the user is required to instruct the Switch to examine the header of a packet to see if it has the proper identifying tag. Then the user may forward these tagged packets to designated classes of service on the Switch where they will be emptied, based on priority.

For example, lets say a user wishes to have a video conference between two remotely set computers. The administrator can add priority tags to the video packets being sent out, utilizing the Access Profile commands. Then, on the receiving end, the administrator instructs the Switch to examine packets for this tag, acquires the tagged packets and maps them to a class queue on the Switch. Then in turn, the administrator will set a priority for this queue so that will be emptied before any other packet is forwarded. This results in the end user receiving all packets sent as quickly as possible, thus prioritizing the queue and allowing for an uninterrupted stream of packets, which optimizes the use of bandwidth available for the video conference.

Understanding QoS

The Switch has eight priority classes of service, one of which is internal and not configurable. These priority classes of service are labeled as 6, the high class to 0, the lowest class. The eight priority tags, specified in IEEE 802.1p are mapped to the Switch's priority classes of service as follows:

- Priority 0 is assigned to the Switch's Q2 class.
- Priority 1 is assigned to the Switch's Q0 class.
- Priority 2 is assigned to the Switch's Q1 class.
- Priority 3 is assigned to the Switch's Q3 class.
- Priority 4 is assigned to the Switch's Q4 class.
- Priority 5 is assigned to the Switch's Q5 class.
- Priority 6 is assigned to the Switch's Q6 class.
- Priority 7 is assigned to the Switch's Q6 class.

For strict priority-based scheduling, any packets residing in the higher priority classes of service are transmitted first. Multiple strict priority classes of service are emptied based on their priority tags. Only when these classes are empty, are packets of lower priority transmitted.

For weighted round-robin queuing, the number of packets sent from each priority queue depends upon the assigned weight. For a configuration of 8 CoS queues, A~H with their respective weight value: 8~1, the packets are sent in the following sequence: A1, B1, C1, D1, E1, F1, G1, H1, A2, B2, C2, D2, E2, F2, G2, A3, B3, C3, D3, E3, F3, A4, B4, C4, D4, E4, A5, B5, C5, D5, A6, B6, C6, A7, B7, A8, A1, B1, C1, D1, E1, F1, G1, H1.

For weighted round-robin queuing, if each CoS queue has the same weight value, then each CoS queue has an equal opportunity to send packets just like round-robin queuing.

For weighted round-robin queuing, if the weight for a CoS is set to 0, then it will continue processing the packets from this CoS until there are no more packets for this CoS. The other CoS queues that have been given a nonzero value, and depending upon the weight, will follow a common weighted round-robin scheme.

Remember that the xStack[®] DES-6500 chassis switch has 7 configurable priority queues (and seven Classes of Service) for each port on the Switch.



NOTICE: The Switch contains eight classes of service for each port on the Switch. One of these classes is reserved for internal use on the Switch and is therefore not configurable. All references in the following section regarding classes of service will refer to only the seven classes of service that may be used and configured by the Switch's Administrator.

Bandwidth Control

The bandwidth control settings are used to place a ceiling on the transmitting and receiving data rates for any selected port. In the **Configuration** folder, click **QoS > Bandwidth Control**, to view the screen shown below.

Bandwidth Settings						
Unit	From	To	Type	No_Limit	Rate	Apply
1	Port 1	Port 1	Both	Disabled	1	Apply

Port Bandwidth Table		
Port	Rx Rate (Mbit/sec)	Tx Rate (Mbit/sec)
1	No_Limit	No_Limit
2	No_Limit	No_Limit
3	No_Limit	No_Limit
4	No_Limit	No_Limit
5	No_Limit	No_Limit
6	No_Limit	No_Limit
7	No_Limit	No_Limit
8	No_Limit	No_Limit
9	No_Limit	No_Limit
10	No_Limit	No_Limit
11	No_Limit	No_Limit
12	No_Limit	No_Limit

Figure 6- 41. Bandwidth Settings and Port Bandwidth Table window

The following parameters can be set or are displayed:

Parameter	Description
Unit	Choose the Switch ID number of the line card in the chassis to be modified.
From/To	A consecutive group of ports may be configured starting with the selected port.
Type	This drop-down menu allows a selection between <i>RX</i> (receive,) <i>TX</i> (transmit,) and <i>Both</i> . This setting will determine whether the bandwidth ceiling is applied to receiving, transmitting, or both receiving and transmitting packets.
No Limit	This drop-down menu allows users to specify that the selected port will have no bandwidth limit. <i>Enabled</i> disables the limit.
Rate	This field allows you to enter the data rate, in Mbit/s, that will be the limit for the selected port. The user may choose a rate between 1 and 9999 Mbit/s.

Click **Apply** to set the bandwidth control for the selected ports. Results of configured **Bandwidth Settings** will be displayed in the **Port Bandwidth Table**.

QoS Scheduling Mechanism

This drop-down menu allows a selection between a **Weight Fair** and a **Strict** mechanism for emptying the priority classes. In the **Configuration** menu open the **QoS** folder and click **QoS Scheduling Mechanism**, to view the screen shown below.

QoS Scheduling Mechanism	
Scheduling Mechanism	Strict <input type="button" value="Apply"/>
QoS Scheduling Mechanism Table	
Class ID	Mechanism
Class-0	Strict
Class-1	Strict
Class-2	Strict
Class-3	Strict
Class-4	Strict
Class-5	Strict
Class-6	Strict

Figure 6- 42. QoS Scheduling Mechanism and QoS Scheduling Mechanism Table window

The **Scheduling Mechanism** has the following parameters.

Parameter	Description
Strict	The highest class of service is the first to process traffic. That is, the highest class of service will finish before other queues empty.
Weight fair	Use the weighted round-robin (<i>WRR</i>) algorithm to handle packets in an even distribution in priority classes of service.

Click **Apply** to allow changes to take effect.

QoS Output Scheduling

QoS can be customized by changing the output scheduling used for the hardware classes of service in the Switch. As with any changes to QoS implementation, careful consideration should be given to how network traffic in lower priority classes of service is affected. Changes in scheduling may result in unacceptable levels of packet loss or significant transmission delay. If choosing to customize this setting, it is important to monitor network performance, especially during peak demand, as bottlenecks can quickly develop if the QoS settings are not suitable. In the **Configuration** folder open the **QoS** folder and click **QoS Output Scheduling**, to view the screen shown below.

QoS Output Scheduling Configuration	
	Max. Packets
Class-0	<input type="text" value="1"/>
Class-1	<input type="text" value="2"/>
Class-2	<input type="text" value="3"/>
Class-3	<input type="text" value="4"/>
Class-4	<input type="text" value="5"/>
Class-5	<input type="text" value="6"/>
Class-6	<input type="text" value="7"/>
<input type="button" value="Apply"/>	

Figure 6- 43. QoS Output Scheduling Configuration window

The following values may be assigned to the QoS classes to set the scheduling.

Parameter	Description
Max. Packets	Specifies the maximum number of packets the above specified hardware priority class of service will be allowed to transmit before allowing the next lowest priority queue to transmit its packets. A value between 0 and 15 can be specified.

Click **Apply** to implement changes made.



NOTE: Entering a 0 for the **Max Packets** field in the **QoS Output Scheduling Configuration** window above will create a Combination Queue. For more information on implementation of this feature, see the next section, **Configuring the Combination Queue**.

Configuring the Combination Queue

Utilizing the **QoS Output Scheduling Configuration** window shown above, the xStack® DES-6500 chassis switch can implement a combination queue for forwarding packets. This combination queue allows for a combination of strict and weight-fair (weighted round-robin “**WRR**”) scheduling for emptying given classes of service. To set the combination queue, enter a 0 for the Max Packets entry of the corresponding priority classes of service listed in the window above. Priority classes of service that have a 0 in the **Max Packet** field will forward packets with strict priority scheduling. The remaining classes of service, that do not have a 0 in their **Max Packet** field, will follow a weighted round-robin (**WRR**) method of forwarding packets — as long as the priority classes of service with a 0 in their **Max Packet** field are empty. When a packet arrives in a priority class with a 0 in its **Max Packet** field, this class of service will automatically begin forwarding packets until it is empty. Once a priority class of service with a 0 in its **Max Packet** field is empty, the remaining priority classes of service will reset the weighted round-robin (**WRR**) cycle of forwarding packets, starting with the highest available priority class of service. Priority classes of service with an equal level of priority and equal entries in their **Max Packet** field will empty their fields based on hardware priority scheduling. The **Max Packet** parameter allows you to specify the maximum number of packets a given priority class of service can transmit per weighted round-robin (**WRR**) scheduling cycle. This provides for a controllable CoS behavior while allowing other classes to empty as well. A value between 0 and 15 packets can be specified per priority class of service to create the combination queue.

The example window below displays an example of the combination queue where Class-1 will have a strict priority for emptying its class, while the other classes will follow a weight fair scheduling.

QoS Output Scheduling Configuration	
	Max. Packets
Class-0	<input type="text" value="1"/>
Class-1	<input type="text" value="0"/>
Class-2	<input type="text" value="3"/>
Class-3	<input type="text" value="4"/>
Class-4	<input type="text" value="5"/>
Class-5	<input type="text" value="6"/>
Class-6	<input type="text" value="7"/>

Figure 6- 44. QoS Output Scheduling window – Combination queue example

802.1p Default Priority

The Switch allows the assignment of a default 802.1p priority to each port on the Switch. In the **Configuration** folder open the **QoS** folder and click **802.1p Default Priority**, to view the screen shown below.

The screenshot shows a window titled "Port Default Priority Assignment". At the top, there are four fields: "Unit" (set to 1), "From" (set to Port 1), "To" (set to Port 1), and "Priority(0~7)" (set to 0). An "Apply" button is located to the right of the Priority field. Below this is a table titled "The Port Priority Table" with two columns: "Port" and "Priority". The table lists ports 1 through 12, all with a priority of 0.

Unit	From	To	Priority(0~7)	Apply
1	Port 1	Port 1	0	Apply

Port	Priority
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0

Figure 6- 45. Port Default Priority assignment and The Port Priority Table window

This page allows assignment of a default 802.1p priority to any given port on the Switch. The priority tags are numbered from 0, the lowest priority, to 7, the highest priority. To implement a new default priority, choose the Switch of the Switch stack to be configured by using the **Unit** pull-down menu, choose a port range by using the **From** and **To** pull-down menus and then insert a priority value, from 0-7 in the **Priority** field. Click **Apply** to implement new settings.

802.1p User Priority

The xStack[®] DES-6500 chassis switch allows the assignment of a class of service to each of the 802.1p priorities. In the **Configuration** folder open the **QoS** folder and click **802.1p User Priority**, to view the screen shown below.

The screenshot shows a window titled "User Priority Configuration". It contains a list of priorities from 0 to 7, each with a corresponding class selection dropdown menu. The classes are: Class-2 for Priority-0, Class-0 for Priority-1, Class-1 for Priority-2, Class-3 for Priority-3, Class-4 for Priority-4, Class-5 for Priority-5, Class-6 for Priority-6, and Class-6 for Priority-7. An "Apply" button is located at the bottom right.

Priority	Class
Priority-0	Class-2
Priority-1	Class-0
Priority-2	Class-1
Priority-3	Class-3
Priority-4	Class-4
Priority-5	Class-5
Priority-6	Class-6
Priority-7	Class-6

Figure 6- 46. User Priority Configuration window

Once you have assigned a priority to the port groups on the Switch, users can then assign this Class to each of the eight levels of 802.1p priorities. Click **Apply** to set changes made.

Traffic Segmentation

Traffic segmentation is used to limit traffic flow from a single port to a group of ports on either a single Switch (in standalone mode) or a group of ports on another switch in a switch stack. This method of segmenting the flow of traffic is similar to using VLANs to limit traffic, but is more restrictive. It provides a method of directing traffic that does not increase the overhead of the Master switch CPU.

In the **Configuration** folder open the **QoS** folder and click **Traffic Segmentation**, to view the screen shown below.

Unit	Port	Configuration	Setup
1	Port 1	View	Setup

Current Traffic Segmentation Table	
Unit	Port Map
1	1-12
2	1-8
3	1-16
4	1-24
5	
6	
7	
8	

Figure 6- 47. Current Traffic Segmentation Table

Click on the **Setup** button to open the **Setup Forwarding ports** page, as shown below.

Unit	Port	Apply
1	Port 1	Apply

Setup Forwarding ports	
Unit	1
Forward Port	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 7 <input checked="" type="checkbox"/> 8 <input checked="" type="checkbox"/> 9 <input checked="" type="checkbox"/> 10 <input checked="" type="checkbox"/> 11 <input checked="" type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24

[View Settings of Unit 1 Port 1](#)

Figure 6- 48. Setup Forwarding Ports window

This page allows users to determine which port on a given line card in the switch chassis will be allowed to forward packets to other ports on another line card within the chassis.

Configuring traffic segmentation on the xStack® DES-6500 chassis switch is accomplished in two parts. First, specify a line card from the chassis by using the **Unit** pull-down menu, and then a port on that line card, using the **Port** pull-down menu. Then specify a second line card from the chassis, and then select which ports (or different ports on the same line card,) on that line card are to be able to receive packets from the line card and port specified in the first part.

Clicking the **Apply** button will enter the combination of transmitting port and allowed receiving ports into the Switch’s **Traffic Segmentation** table.

The **Unit** drop-down menu at the top of the page allows users to select a line card from a switch stack using that line card’s Unit ID. The **Port** drop-down menu allows users to select a port from that line card. This is the port that will be transmitting packets.

The **Unit** drop-down menu under the Setup Forwarding ports heading allows users to select a line card from the chassis using that line card's Unit ID. The **Forward Port** click boxes allow users to select which of the ports on the selected line card will be able to forward packets. These ports will be allowed to receive packets from the port specified above.

Click **Apply** to enter the settings into the Switch's **Traffic Segmentation** table.

Clicking the **Apply** button will enter the combination of transmitting port and allowed receiving ports into the Switch's **Traffic Segmentation Table**.

System Log Server

The Switch can send Syslog messages to up to four designated servers using the **System Log Host** window. In the **Configuration** folder, click **System Log Server**, to view the screen shown below.

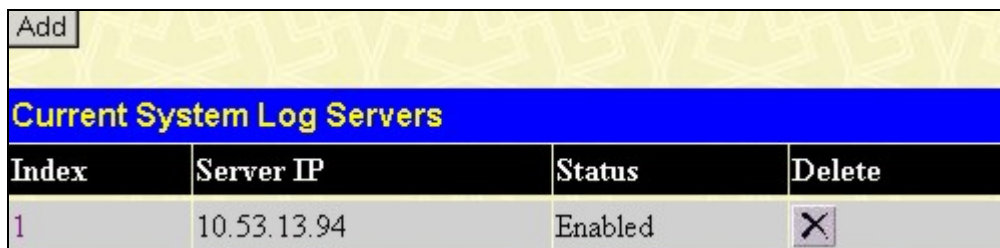


Figure 6- 49. System Log Host window

The parameters configured for adding and editing **System Log Server** settings are the same. To add a new Syslog Server, click the **Add** button. To modify a current entry, click the hyperlinked number of the server in the **Index** field. Both actions will result in the same screen to configure. See the table below for a description of the parameters in the following window.



Figure 6- 50. Configure System Log Server - Edit

The following parameters can be set:

Parameter	Description
Index	Syslog server settings index (1-4).
Server IP	The IP address of the Syslog server.
Severity	This drop-down menu allows you to select the level of messages that will be sent. The options are <i>Warning</i> , <i>Informational</i> , and <i>All</i> .
Facility	Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following. Bold font denotes the facility values that the Switch currently implements. Numerical Facility Code 0 kernel messages 1 user-level messages 2 mail system 3 system daemons 4 security/authorization messages 5 messages generated internally by syslog line printer subsystem 7 network news subsystem

	8 UUCP subsystem 9 clock daemon 10 security/authorization messages 11 FTP daemon 12 NTP subsystem 13 log audit 14 log alert 15 clock daemon 16 local use 0 (local0) 17 local use 1 (local1) 18 local use 2 (local2) 19 local use 3 (local3) 20 local use 4 (local4) 21 local use 5 (local5) 22 local use 6 (local6) 23 local use 7 (local7)
UDP Port (514 or 6000-65535)	Enter the UDP port number used for sending Syslog messages. The default is 514.
Status	Choose <i>Enabled</i> or <i>Disabled</i> to activate or deactivate.

To set the System Log Server configuration, click **Apply**. To delete an entry from the **Current System Log Server** window, click the corresponding under the **Delete** heading of the entry to delete. To return to the **Current System Log Servers** window, click the [Show All System Log Servers](#) link.

System Severity Log

The **System Severity Log** allows users to configure where and when events occurring on the Switch will be recorded. These events are classified by the Switch into the following three categories:

- **Information** – Events classified as information are basic events occurring on the Switch that are not deemed as problematic, such as enabling or disabling various functions on the Switch. This is the lowest severity level.
- **Warning** - Events classified as warning are problematic events that are not critical to the overall function of the Switch but do require attention, such as unsuccessful downloads or uploads and failed logins. This level is regarded as a mid-level warning.
- **Critical** – Events classified as critical are fatal exceptions occurring on the Switch, such as hardware failures or spoofing attacks. This level is regarded as the highest severity level.

When an event occurs, the Switch classifies it into one of these three categories. If the severity of the event is higher than the level configured, the Switch will send a message to the SNMP trap, the Switch’s log or both, depending on user configuration. If the event classified as lower than the configured severity level, the message is regarded as unimportant and will be discarded.

To configure the system severity levels, open the following window by clicking **Configuration > System Severity Log** in the main menu.

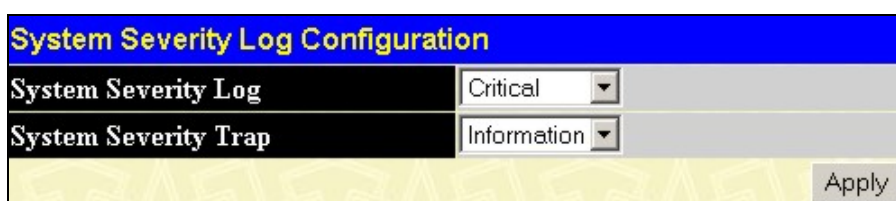


Figure 6- 51. System Severity Log Configurations window

The user may set the following parameters to configure the **System Severity**. Configurations will be displayed in the **System Severity Table**. Click **Apply** to implement changes made.

Parameter	Description
System Severity Log	<p>Choose one of the following to identify what type of severity warnings are to be sent to the switch log file.</p> <ul style="list-style-type: none"> • <i>critical</i> – Entering this parameter along with the proper destination, stated above, will instruct the Switch to send only critical events to the Switch’s log or SNMP agent. • <i>warning</i> – Entering this parameter along with the proper destination, stated above, will instruct the Switch to send critical and warning events to the Switch’s log and/or SNMP agent. • <i>information</i> – Entering this parameter along with the proper destination, stated above, will instruct the Switch to send informational, warning and critical events to the Switch’s log and/or SNMP agent.
System Severity Trap	<p>Choose one of the following to identify what type of severity warnings are to be sent to the SNMP trap.</p> <ul style="list-style-type: none"> • <i>critical</i> – Entering this parameter along with the proper destination, stated above, will instruct the Switch to send only critical events to the Switch’s log or SNMP agent. • <i>warning</i> – Entering this parameter along with the proper destination, stated above, will instruct the Switch to send critical and warning events to the Switch’s log and/or SNMP agent. • <i>information</i> – Entering this parameter along with the proper destination, stated above, will instruct the Switch to send informational, warning and critical events to the Switch’s log and/or SNMP agent.

SNTP Settings

Time Settings

To configure the time settings for the Switch, open the **Configuration** folder, then the **SNTP** folder and click on the **Time Settings** link, revealing the following screen for the user to configure.

Current Time: Status	
System Boot Time	19 Apr 2005 09:15:27
Time Source	System Clock
Current Time: SNTP Settings	
SNTP State	Disabled ▾
SNTP Primary Server	0.0.0.0
SNTP Secondary Server	0.0.0.0
SNTP Poll Interval in Seconds	720
Current Time: Set Current Time	
Year	2005 ▾
Month	April ▾
Day	19 ▾
Time in HH MM SS	16 ▾ 43 ▾ 58 ▾
Apply	

Figure 6- 52. Current Time Settings window

The following parameters can be set or are displayed:

Parameter	Description
Time Settings - Current Time	
System Boot Time	Displays the time when the Switch was initially started for this session.
Current Time	Displays the current time.
Time Source	Displays the source of the time settings viewed here.
SNTP Settings	
SNTP State	Use this pull-down menu to Enable or Disable SNTP.
SNTP Primary Server	The IP address of the primary server from which the SNTP information will be taken.
SNTP Secondary Server	The IP address of the secondary server from which the SNTP information will be taken.
SNTP Poll Interval in Seconds	The interval, in seconds, between requests for updated SNTP information.
Time Settings - Set Current Time	
Year	Enter the current year, if updating the system clock.
Month	Enter the current month, if updating the system clock.
Day	Enter the current day, if updating the system clock.
Time in HH MM SS	Enter the current time in hours, minutes and seconds, if updating the system clock.

Click **Apply** to implement your changes.

Time Zone and DST

The following are screens used to configure time zones and Daylight Savings time settings for SNTP. Open the **Configuration** folder, then the **SNTP** folder and click on the **Time Zone and DST** link, revealing the following screen.

Time Zone and DST Settings

Daylight Saving Time State: Disabled

Daylight Saving Time Offset in Minutes: 60

Time Zone Offset from GMT in +/-HH:MM: + 00 00

DST Repeating Settings

From: Which Day: First

From: Day of Week: Sunday

From: Month: April

From: time in HH MM: 00 00

To: Which Day: Last

To: Day of Week: Sunday

To: Month: October

To: time in HH MM: 00 00

DST Annual Settings

From: Month: April

From: Day: 29

From: time in HH MM: 00 00

To: Month: October

To: Day: 12

To: Time in HH MM: 00 00

Apply

Figure 6- 53. Time Zone and DST Settings page

The following parameters can be set:

Parameter	Description
Time Zone and DST	
Daylight Saving Time State	Use this pull-down menu to Enable or Disable the DST Settings.
Daylight Saving Time Offset in Minutes	Use this pull-down menu to specify the amount of time that will constitute your local DST offset - 30, 60, 90, or 120 minutes.
Time Zone Offset from GMT in +/-HH:MM	Use these pull-down menus to specify your local time zone's offset from Greenwich Mean Time (GMT.)
DST Repeating Settings	
Using repeating mode will enable DST seasonal time adjustment. Repeating mode requires that the DST beginning and ending date be specified using a formula. For example, specify to begin DST on Saturday during the second week of April and end DST on Sunday during the last week of October.	
From: Which Day	Enter the week of the month that DST will start.
From: Day of Week	Enter the day of the week that DST will start on.

From: Month	Enter the month DST will start on.
From: Time in HH:MM	Enter the time of day that DST will start on.
To: Which Day	Enter the week of the month the DST will end.
To: Day of Week	Enter the day of the week that DST will end.
To: Month	Enter the month that DST will end.
To: time in HH:MM	Enter the time DST will end.
DST Annual Settings	
Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14.	
From: Month	Enter the month DST will start on, each year.
From: Day	Enter the day of the month DST will start on, each year.
From: Time in HH:MM	Enter the time of day DST will start on, each year.
To: Month	Enter the month DST will end on, each year.
To: Day	Enter the day of the month DST will end on, each year.
To: Time in HH:MM	Enter the time of day that DST will end on, each year.

Click **Apply** to implement changes made to the **Time Zone and DST** window.

Access Profile Table

Access profiles allow users to establish criteria to determine whether the Switch will forward packets based on the information contained in each packet's header. These criteria can be specified on a basis of VLAN, MAC address, IP address or IPv6 address.

Due to a chipset limitation, the Switch supports a maximum of 8 access profiles. The rules used to define the access profiles are limited to a total of 9600 rules for the Switch, depending on line cards installed.

There is an additional limitation on how the rules are distributed among line cards inserted into the chassis. For Fast Ethernet line cards (DES-6504, DES-6506, DES-6508, DES-6510), ports are divided into ACL Groups, consisting of ports 1-8, ports 9-16 and ports 17-24, except the DES-6504 which has two groups, 1-8 and 9-12. These groups support 240 rules maximum each, which leads to a total of 720 rules maximum per 24-port line card. Since the Switch can hold up to 8 line cards, the maximum number of ACL rules will be 5760 ($240 * 3 * 8 = 5760$).

For Gigabit Ethernet line cards (DES-6505, DES-6507, DES-6509) and the 10-Gigabit DES-6512, all ports can support 100 rules each, which means that the maximum number of ACL rules using the maximum number of inserted 12-port line cards will be 9600 ($12 * 100 * 8 = 9600$). For a better understanding of ACL rules pertaining to DES-6500 line cards, see the following table:

Line Card	Ports / Groups	Maximum Supported Rules Per Unit	Maximum Supported Rules Per Line Card	Maximum Supported Rules Per Full Chassis
DES-6504	2 Groups (ports 1-8 and 9-12)	240 Rules Maximum per group	480 Total Rules	3840 Rules Maximum
DES-6508	2 Groups (ports 1-8 and 9-16)	240 Rules Maximum per group	480 Total Rules	3840 Rules Maximum
DES-6506/DES-6510	3 Groups (ports 1-8, 9-16 and 17-24)	240 Rules Maximum per group	720 Total Rules	5670 Rules Maximum
DES-6505	8 Ports	100 Rules Maximum Per Port	800 Total Rules	6400 Rules Maximum
DES-6507	12 Ports	100 Rules Maximum Per Port	1200 Total Rules	9600 Rules Maximum
DES-6509	12 Ports	100 Rules Maximum Per Port	1200 Total Rules	9600 Rules Maximum
DES-6512	2 Ports	100 Rules Maximum Per Port	200 Total Rules	1600 Rules Maximum

It is important to keep this in mind when setting up VLANs as well. Access rules applied to a VLAN require that a rule be created for each port in the VLAN. For example, let's say VLAN10 contains ports 2, 11 and 12. If you create an access profile specifically for VLAN10, you must create a separate rule for each port. Now take into account the rule limit. The rule limit applies to both port groups 1-8 and 9-16 since VLAN10 spans these groups. One less rule is available for port group 1-8. Two less rules are available for port group 9-16. In addition, a total of three rules apply to the 9600 rule Switch limit.

It must be noted that there are specific circumstances under which the ACL cannot filter a packet even when there is a condition match that should deny forwarding. This is a limitation that may arise if:

- the destination MAC is the same as the Switch (system) MAC
- a packet is directed to the system IP interface such as multicast IP packets or if the hardware IP routing table is full and Switch software routes the packet according to routing protocol.

The DES-6500 has four ways of creating access profile entries on the Switch which include **Ethernet** (MAC Address), **IP**, **Packet Content** and **IPv6**.

Creating an access profile is divided into two basic parts. The first is to specify which part or parts of a frame the Switch will examine, such as the MAC source address or the IP destination address. The second part is entering the criteria the Switch will use to determine what to do with the frame. The entire process is described below.



Due to a backward compatibility issue, when a user upgrades to R3 firmware (3.00.B33), all settings previously configured for any ACL function (CPU ACL included) on the Switch will be lost. We recommend that the user save a configuration file of current settings before upgrading to R3 firmware.

Configuring the Access Profile Table

To display the currently configured Access Profiles on the Switch, open the **Configuration** folder and click on the **Access Profile Table** link. This will open the **Access Profile Table** page, as shown below.

Access Profile Table			
Profile ID	Type	Access Rule	Delete
1	Ethernet	Modify	X
2	IP	Modify	X
3	Packet Content	Modify	X
4	IPv6	Modify	X

Figure 6- 54. Access Profile Table

To add an entry to the **Access Profile Table**, click the **Add** button. This will open the **Access Profile Configuration** page, as shown below. There are four **Access Profile Configuration** pages; one for **Ethernet** (or MAC address-based) profile configuration, one for **IP** address-based profile configuration, one for the **Packet Content Mask** and one for **IPv6**. You can switch between the three **Access Profile Configuration** pages by using the **Type** drop-down menu. The page shown below is the **Ethernet Access Profile Configuration** page.

Figure 6- 55. Access Profile Configuration (Ethernet)

The following parameters can be set, for the **Ethernet** type:

Parameter	Description
Profile ID (1-8)	Type in a unique identifier number for this profile set. This value can be set from 1 - 8.
Type	Select profile based on Ethernet (MAC Address), IP address, Packet Content Mask or IPv6. This will change the menu according to the requirements for the type of profile.

	<ul style="list-style-type: none"> • Select <i>Ethernet</i> to instruct the Switch to examine the layer 2 part of each packet header. • Select <i>IP</i> to instruct the Switch to examine the IP address in each frame's header. • Select <i>Packet Content Mask</i> to specify a mask to hide the content of the packet header. • Select <i>IPv6</i> to instruct the Switch to examine the IPv6 part of each packet header.
VLAN	Selecting this option instructs the Switch to examine the VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
Source MAC	Source MAC Mask - Enter a MAC address mask for the source MAC address.
Destination MAC	Destination MAC Mask - Enter a MAC address mask for the destination MAC address.
802.1p	Selecting this option instructs the Switch to examine the 802.1p priority value of each packet header and use this as the criterion, or part of the criterion for forwarding.
Ethernet type	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.

The page shown below is the **IP Access Profile Configuration** page.

Figure 6- 56. Access Profile Configuration (IP)

The following parameters can be set, for **IP**:

Parameter	Description
Profile ID (1-8)	Type in a unique identifier number for this profile set. This value can be set from 1 - 8.
Type	<p>Select profile based on Ethernet (MAC Address), IP address, Packet Content Mask or IPv6. This will change the menu according to the requirements for the type of profile.</p> <ul style="list-style-type: none"> • Select <i>Ethernet</i> to instruct the Switch to examine the layer 2 part of each packet header. • Select <i>IP</i> to instruct the Switch to examine the IP address in each frame's header. • Select <i>Packet Content Mask</i> to specify a mask to hide the content of the packet header.

	<ul style="list-style-type: none"> Select <i>IPv6</i> to instruct the Switch to examine the IPv6 part of each packet header.
VLAN	Selecting this option instructs the Switch to examine the VLAN part of each packet header and use this as the, or part of the criterion for forwarding.
Source IP Mask	Enter an IP address mask for the source IP address.
Destination IP Mask	Enter an IP address mask for the destination IP address.
DSCP	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding.
Protocol	<p>Selecting this option instructs the Switch to examine the protocol type value in each frame's header. You must then specify what protocol(s) to include according to the following guidelines:</p> <p>Select ICMP to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header.</p> <ul style="list-style-type: none"> Select Type to further specify that the access profile will apply an ICMP type value, or specify Code to further specify that the access profile will apply an ICMP code value. <p>Select IGMP to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header.</p> <ul style="list-style-type: none"> Select Type to further specify that the access profile will apply an IGMP type value <p>Select TCP to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP requires specification of a source port mask and/or a destination port mask. The user may also identify which flag bits to filter. Flag bits are parts of a packet that determine what to do with the packet. The user may filter packets by filtering certain flag bits within the packets, by checking the boxes corresponding to the flag bits of the TCP field. The user may choose between urg (urgent), ack (acknowledgement), psh (push), rst (reset), syn (synchronize), fin (finish).</p> <ul style="list-style-type: none"> src port mask - Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to filter. dest port mask - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) which you wish to filter. <p>Select UDP to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires specification of a source port mask and/or a destination port mask.</p> <ul style="list-style-type: none"> src port mask - Specify a UDP port mask for the source port in hex form (hex 0x0-0xffff). dest port mask - Specify a UDP port mask for the destination port in hex form (hex 0x0-0xffff). <p>protocol id - Enter a value defining the protocol ID in the packet header to mask. Specify the protocol ID mask in hex form (hex 0x0-0xffffffff).</p>

The page shown below is the **Packet Content Mask** configuration window.

Figure 6- 57. Access Profile Configuration window (Packet Content Mask)

This screen will aid the user in configuring the Switch to mask packet headers beginning with the offset value specified. The following fields are used to configure the **Packet Content Mask**:

Parameter	Description
Profile ID (1-8)	Type in a unique identifier number for this profile set. This value can be set from 1 - 8.
Type	Select profile based on Ethernet (MAC Address), IP address, Packet Content Mask or IPv6. This menu will change according to the requirements for the type of profile. <ul style="list-style-type: none"> Select <i>Ethernet</i> to instruct the Switch to examine the layer 2 part of each packet header. Select <i>IP</i> to instruct the Switch to examine the IP address in each frame's header. Select <i>Packet Content Mask</i> to specify a mask to hide the content of the packet header. Select <i>IPv6</i> to instruct the Switch to examine the IPv6 part of each packet header.
Offset	This field will instruct the Switch to mask the packet header beginning with the offset value specified: <ul style="list-style-type: none"> <i>value (0-15)</i> - Enter a value in hex form to mask the packet from the beginning of the packet to the 15th byte. <i>value (16-31)</i> – Enter a value in hex form to mask the packet from byte 16 to byte 31. <i>value (32-47)</i> – Enter a value in hex form to mask the packet from byte 32 to byte 47. <i>value (48-63)</i> – Enter a value in hex form to mask the packet from byte 48 to byte 63. <i>value (64-79)</i> – Enter a value in hex form to mask the packet from byte 64 to byte 79.

Click **Apply** to implement changes made.

The page shown below is the **IPv6** configuration window.

Figure 6- 58. Access Profile Configuration window (IPv6)

The following parameters can be set, for IP:

Parameter	Description
Profile ID (1-8)	Type in a unique identifier number for this profile set. This value can be set from 1 - 8.
Type	Select profile based on Ethernet (MAC Address), IP address, Packet Content Mask or IPv6. This will change the menu according to the requirements for the type of profile. <ul style="list-style-type: none"> Select <i>Ethernet</i> to instruct the Switch to examine the layer 2 part of each packet header. Select <i>IP</i> to instruct the Switch to examine the IP address in each frame's header. Select <i>Packet Content Mask</i> to specify a mask to hide the content of the packet header. Select <i>IPv6</i> to instruct the Switch to examine the IPv6 part of each packet header.
Class	Checking this field will instruct the Switch to examine the <i>class</i> field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4.
Flowlabel	Checking this field will instruct the Switch to examine the <i>flow label</i> field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
Source IPv6 Mask	The user may specify an IP address mask for the source IPv6 address by checking the corresponding box and entering the IP address mask.
Destination IPv6 Mask	The user may specify an IP address mask for the destination IPv6 address by checking the corresponding box and entering the IP address mask.

Click **Apply** to implement changes made.

To establish the rule for a previously created Access Profile:

To configure the **Access Rule for Ethernet**, open the **Access Profile Table** and click **Modify** for an Ethernet entry. This will open the following screen:

Access Rule Table					
Profile ID	Mode	Type	Access ID	Display	Delete
1	Permit	Ethernet	1	View	<input type="button" value="X"/>

[Show All Access Profile Entries](#)

Figure 6- 59. Access Rule Table

To remove a previously created rule, select it and click the button. To add a new Access Rule, click the **Add** button:

Access Rule Configuration	
Profile ID	1
Mode	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Access ID(1-65535)	<input type="text" value="1"/>
Type	Ethernet
Priority(0-7)	<input type="checkbox"/> <input type="text" value="0"/> <input type="checkbox"/> Replace Priority
Replace Dscp(0-63)	<input type="checkbox"/> <input type="text" value="0"/>
VLAN Name	<input type="text"/>
Source MAC	<input type="text" value="00-00-00-00-00-00"/>
Destination MAC	<input type="text" value="00-00-00-00-00-00"/>
802.1p(0-7)	<input type="text" value="0"/>
Ethernet Type	<input type="text" value="0000"/>
Port (UnitID:PortNum)	<input type="text"/>

[Show All Access Rule Entries](#)

Figure 6- 60. Access Rule Configuration window - Ethernet.

To set the Access Rule for Ethernet, adjust the following parameters and click **Apply**.

Parameters	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify that packets that match the access profile are not forwarded by the Switch and will be filtered.
Access ID	Type in a unique identifier number for this access. This value can be set from 1 - 65535.
Type	Selected profile based on Ethernet (MAC Address), IP address, Packet Content Mask or IPv6. <ul style="list-style-type: none"> <i>Ethernet</i> instructs the Switch to examine the layer 2 part of each packet header. <i>IP</i> instructs the Switch to examine the IP address in each frame's header. <i>Packet Content Mask</i> instructs the Switch to examine the packet header. <i>IPv6</i> to instructs the Switch to examine the IPv6 part of each packet header.
Priority (0-7)	This parameter can be specified to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the

	<p>CoS queue specified previously by the user.</p> <p><i>replace priority</i> – Click the corresponding box to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.</p> <p>For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.</p>
VLAN Name	Allows the entry of a name for a previously configured VLAN.
Source MAC	Source MAC Address - Enter a MAC Address for the source MAC address.
Destination MAC	Destination MAC Address - Enter a MAC Address mask for the destination MAC address.
802.1p (0-7)	Enter a value from 0-7 to specify that the access profile will apply only to packets with this 802.1p priority value.
Ethernet Type	Specifies that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value (hex 0x0-0xffff) in the packet header. The Ethernet type value may be set in the form: hex 0x0-0xffff, which means the user may choose any combination of letters and numbers ranging from a-f and from 0-9999.
Port	The Access Rule may be configured on a per-port basis by entering the port number of the line card in the chassis into this field. The port list is specified by listing the lowest line card number and the beginning port number on that line card, separated by a colon. Then the highest line card number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies line card number 1, port 3. 2:4 specifies line card number 2, port 4. 1:3 - 2:4 specifies all of the ports between line card 1, port 3 and line card 2, port 4 – in numerical order. Entering <i>all</i> will denote all ports on the Switch.

To view the settings of a previously correctly configured rule, click [View](#) in the **Access Rule Table** to view the following screen:

Access Rule Display	
Profile ID	1
Access ID	1
Mode	Permit
Type	Ethernet
Priority	-----
Replace Dscp	-----
VLAN Name	default
Source MAC	-----
Destination MAC	-----
802.1p	-----
Ethernet Type	-----
Port	1:4

[Show All Access Rule Entries](#)

Figure 6- 61. Access Rule Display window (Ethernet)

In the **Configuration** folder, click the **Access Profile Table** link opening the **Access Profile Table**. Under the heading **Access Rule**, clicking **Modify**, will open the following window.

Access Rule Table					
Profile ID	Mode	Type	Access ID	Display	Delete
2	Permit	IP	1	View	<input type="button" value="X"/>

[Show All Access Profile Entries](#)

Figure 6- 62. Access Rule Table window – IP

To create a new rule set for an access profile click the **Add** button. A new window is displayed. To remove a previously created rule, click the corresponding button.

Access Rule Configuration	
Profile ID	2
Mode	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Access ID(1-65535)	1
Type	IP
Priority(0-7)	<input type="checkbox"/> 0 <input type="checkbox"/> Replace Priority
Replace Dscp(0-63)	<input type="checkbox"/> 0
VLAN Name	
Source IP	0.0.0.0
Destination IP	0.0.0.0
Dscp(0-63)	0
Protocol	
Port (UnitID:PortNum)	

[Show All Access Rule Entries](#)

Figure 6- 63. Access Rule Configuration window (IP)

Configure the following **Access Rule Configuration** settings for IP:

Parameter	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify that packets that match the access profile are not forwarded by the Switch and will be filtered.
Access ID	Type in a unique identifier number for this access. This value can be set from 1 - 65535.
Type	Selected profile based on Ethernet (MAC Address), IP address, Packet Content Mask or IPv6. <ul style="list-style-type: none"> <i>Ethernet</i> instructs the Switch to examine the layer 2 part of each packet header. <i>IP</i> instructs the Switch to examine the IP address in each frame's header. <i>Packet Content Mask</i> instructs the Switch to examine the packet header. <i>IPv6</i> instructs the Switch to examine the IPv6 part of each packet header.
Priority (0-7)	This parameter is specified to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS

	<p>queue specified previously by the user.</p> <p><i>Replace priority with</i> – Click the corresponding box to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.</p> <p>For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.</p>
Replace Dscp (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
VLAN Name	Allows the entry of a name for a previously configured VLAN.
Source IP	Source IP Address - Enter an IP Address mask for the source IP address.
Destination IP	Destination IP Address- Enter an IP Address mask for the destination IP address.
Dscp (0-63)	This field allows the user to enter a DSCP value in the space provided, which will instruct the Switch to examine the DiffServ Code part of each packet header and use this as the criterion, or part of the criterion for forwarding. The user may choose a value between 0 and 63.
Protocol	This field allows the user to modify the protocol used to configure the Access Rule Table ; depending on which protocol the user has chosen in the Access Profile Table .
Port	The Access Rule may be configured on a per-port basis by entering the port number of the line card in the chassis into this field. The port list is specified by listing the lowest line card number and the beginning port number on that line card, separated by a colon. Then the highest line card number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies line card number 1, port 3. 2:4 specifies line card number 2, port 4. 1:3 - 2:4 specifies all of the ports between line card 1, port 3 and line card 2, port 4 – in numerical order. Entering <i>all</i> will denote all ports on the Switch.

To view the settings of a previously correctly configured rule, click [View](#) in the **Access Rule Table** to view the following screen:

Access Rule Display	
Profile ID	2
Access ID	1
Mode	Permit
Type	IP
Priority	-----
Replace Dscp	-----
VLAN Name	default
Source IP	-----
Destination IP	-----
Dscp	-----
Protocol	-----
Port	1:4
Show All Access Rule Entries	

Figure 6- 64. Access Rule Display window (IP)

To configure the Access Rule for **Packet Content Mask**, open the **Access Profile Table** and click **Modify** for a **Packet Content Mask** entry. This will open the following screen:

Access Rule Table					
Profile ID	Mode	Type	Access ID	Display	Delete
4	Permit	Packet Content	1	View	<input type="button" value="X"/>

[Show All Access Profile Entries](#)

Figure 6- 65. Access Rule Table (Packet Content Mask)

To remove a previously created rule, select it and click the button. To add a new Access Rule, click the **Add** button:

Access Rule Configuration	
Profile ID	3
Mode	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Access ID(1-65535)	<input type="text" value="1"/>
Type	Packet Content
Priority(0-7)	<input type="checkbox"/> <input type="text" value="0"/> <input type="checkbox"/> Replace Priority
Replace Dscp(0-63)	<input type="checkbox"/> <input type="text" value="0"/>
Offset 0-15	<input type="checkbox"/> <input type="text" value="00000000"/> <input type="text" value="00000000"/> <input type="text" value="00000000"/> <input type="text" value="00000000"/>
Offset 16-31	<input type="checkbox"/> <input type="text" value="00000000"/> <input type="text" value="00000000"/> <input type="text" value="00000000"/> <input type="text" value="00000000"/>
Offset 32-47	<input type="checkbox"/> <input type="text" value="00000000"/> <input type="text" value="00000000"/> <input type="text" value="00000000"/> <input type="text" value="00000000"/>
Offset 48-63	<input type="checkbox"/> <input type="text" value="00000000"/> <input type="text" value="00000000"/> <input type="text" value="00000000"/> <input type="text" value="00000000"/>
Offset 64-79	<input type="checkbox"/> <input type="text" value="00000000"/> <input type="text" value="00000000"/> <input type="text" value="00000000"/> <input type="text" value="00000000"/>
Port (UnitID:PortNum)	<input type="text"/>
<input type="button" value="Apply"/>	

[Show All Access Rule Entries](#)

Figure 6- 66. Access Rule Configuration - Packet Content Mask

To set the Access Rule for the **Packet Content Mask**, adjust the following parameters and click **Apply**.

Parameter	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify that packets that match the access profile are not forwarded by the Switch and will be filtered.
Access ID	Type in a unique identifier number for this access. This value can be set from 1 - 65535.
Type	Selected profile based on Ethernet (MAC Address), IP address, Packet Content Mask or IPv6. <ul style="list-style-type: none"> • <i>Ethernet</i> instructs the Switch to examine the layer 2 part of each packet header. • <i>IP</i> instructs the Switch to examine the IP address in each frame's header. • <i>Packet Content Mask</i> instructs the Switch to examine the packet header. • <i>IPv6</i> instructs the Switch to examine the IPv6 part of each packet header.

Priority	<p>This parameter can be specified to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user.</p> <p><i>replace priority</i> – Click the corresponding box to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.</p> <p>For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.</p>
Replace Dscp (0-63)	<p>Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.</p>
Offset	<p>This field will instruct the Switch to mask the packet header beginning with the offset value specified:</p> <ul style="list-style-type: none"> • <i>value (0-15)</i> - Enter a value in hex form to mask the packet from the beginning of the packet to the 15th byte. • <i>value (16-31)</i> - Enter a value in hex form to mask the packet from byte 16 to byte 31. • <i>value (32-47)</i> - Enter a value in hex form to mask the packet from byte 32 to byte 47. • <i>value (48-63)</i> - Enter a value in hex form to mask the packet from byte 48 to byte 63. • <i>value (64-79)</i> - Enter a value in hex form to mask the packet from byte 64 to byte 79.
Port	<p>The Access Rule may be configured on a per-port basis by entering the port number of the line card in the chassis into this field. The port list is specified by listing the lowest line card number and the beginning port number on that line card, separated by a colon. Then the highest line card number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies line card number 1, port 3. 2:4 specifies line card number 2, port 4. 1:3 - 2:4 specifies all of the ports between line card 1, port 3 and line card 2, port 4 – in numerical order. Entering <i>all</i> will denote all ports on the Switch.</p>

To view the settings of a previously correctly configured rule, click [View](#) in the **Access Rule Table** to view the following screen:

Access Rule Display	
Profile ID	3
Access ID	1
Mode	Permit
Type	Packet Content
Priority	-----
Replace Dscp	-----
Offset 0-15	0x00000000 0x00000000 0x00000000 0x00000000
Offset 16-31	-----
Offset 32-47	-----
Offset 48-63	-----
Offset 64-79	-----
Port	1:4
Show All Access Rule Entries	

Figure 6- 67. Access Rule Display window (Packet Content Mask)

To configure the Access Rule for IPv6, open the **Access Profile Table** and click **Modify** for an IPv6 entry. This will open the following screen:

Access Rule Table					
Profile ID	Mode	Type	Access ID	Display	Delete
4	Permit	IPv6	1	View	

[Add](#)

[Show All Access Profile Entries](#)

Figure 6- 68. Access Rule Table

Click **Add** to open the next screen to configure the IPv6 entry for an access rule.

Access Rule Configuration	
Profile ID	4
Mode	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Access ID (1-65535)	<input type="text" value="1"/>
Type	IPv6
Priority (0-7)	<input type="checkbox"/> <input type="text"/> <input type="checkbox"/> Replace Priority
Replace Dscp(0-63)	<input type="checkbox"/> <input type="text"/>
Class (0-255)	<input type="text"/>
Flowlabel (0-FFFFFF)	<input type="text" value="00000"/>
Source IPv6 Address	<input type="text" value="0000:0000:0000:0000:00"/>
Destination IPv6 Address	<input type="text" value="0000:0000:0000:0000:00"/>
Port (UnitID:PortNum)	<input type="text"/>

[Show All Access Rule Entries](#) [Apply](#)

Figure 6- 69. Access Rule Configuration – IPv6

To set the Access Rule for the **Packet Content Mask**, adjust the following parameters and click **Apply**.

Parameter	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify that packets that match the access profile are not forwarded by the Switch and will be filtered.
Access ID	Type in a unique identifier number for this access rule. This value can be set from 1 - 65535.
Type	Selected profile based on Ethernet (MAC Address), IP address, Packet Content Mask or IPv6. <ul style="list-style-type: none"> • <i>Ethernet</i> instructs the Switch to examine the layer 2 part of each packet header. • <i>IP</i> instructs the Switch to examine the IP address in each frame's header. • <i>Packet Content Mask</i> instructs the Switch to examine the packet header. • <i>IPv6</i> instructs the Switch to examine the IPv6 part of each packet header.

Priority	<p>This parameter is specified to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user.</p> <p><i>Replace priority with</i> – Click the corresponding box to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.</p> <p>For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.</p>
Replace Dscp (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
Class	Entering a value between 0 and 255 will instruct the Switch to examine the class field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field of IPv4.
Flowlabel	Configuring this field, in hex form, will instruct the Switch to examine the flow label field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
Source IPv6 Address	The user may specify an IP address mask for the source IPv6 address by entering the IP address mask, in hex form.
Destination IPv6 Address	The user may specify an IP address mask for the destination IPv6 address by and entering the IP address mask, in hex form.
Port	The Access Rule may be configured on a per-port basis by entering the port number of the line card in the chassis into this field. The port list is specified by listing the lowest line card number and the beginning port number on that line card, separated by a colon. Then the highest line card number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies line card number 1, port 3. 2:4 specifies line card number 2, port 4. 1:3 - 2:4 specifies all of the ports between line card 1, port 3 and switch 2, port 4 – in numerical order. Entering <i>all</i> will denote all ports on the Switch.

To view the settings of a previously correctly configured rule, click [View](#) in the **Access Rule Table** to view the following screen:

Access Rule Display	
Profile ID	4
Access ID	1
Mode	Permit
Type	IPv6
Priority	-----
Replace Dscp	-----
Class	2
Flowlabel	-----
Source IPV6	
Destination IPV6	
Port	1:4
Show All Access Rule Entries	

Figure 6-70. Access Rule Display (IPv6)

CPU Interface Filtering

Due to a chipset limitation and needed extra switch security, the xStack® DES-6500 chassis switch incorporates CPU Interface filtering. This added feature increases the running security of the Switch by enabling the user to create a list of access rules for packets destined for the Switch’s CPU interface. Employed similarly to the Access Profile feature previously mentioned, CPU interface filtering examines Ethernet, IP and Packet Content Mask packet headers destined for the CPU and will either forward them or filter them, based on the user’s implementation. As an added feature for the CPU Filtering, the xStack® DES-6500 chassis switch allows the CPU filtering mechanism to be enabled or disabled globally, permitting the user to create various lists of rules without immediately enabling them.

Creating an access profile for the CPU is divided into two basic parts. The first is to specify which part or parts of a frame the Switch will examine, such as the MAC source address or the IP destination address. The second part is entering the criteria the Switch will use to determine what to do with the frame. The entire process is described below.



Due to a backward compatability issue, when a user upgrades to R3 firmware (3.00.B33), all settings previously configured for any ACL function (CPU ACL included) on the Switch will be lost. We recommend that the user save a configuration file of current settings before upgrading to R3 firmware.

CPU Interface Filtering State Settings

In the following window, the user may globally enable or disable the CPU Interface Filtering mechanism by using the pull-down menu to change the running state. To access this window, click **Configuration > CPU Interface Filtering > CPU Interface Filtering State**. Choose **Enabled** to enable CPU packets to be scrutinized by the Switch and **Disabled** to disallow this scrutiny.



Figure 6- 71. CPU Interface Filtering State Settings window

CPU Interface Filtering Table

The **CPU Interface Filtering Table** displays the CPU Access Profile Table entries created on the Switch. To view the configurations for an entry, click the hyperlinked **Profile ID** number.

CPU Interface Filtering Table			
Profile ID	Type	Access Rule	Delete
1	Ethernet	Modify	X
2	IP	Modify	X
3	Packet Content	Modify	X

Figure 6- 72. CPU Interface Filtering Table

To add an entry to the **CPU Interface Filtering Table**, click the **Add** button. This will open the **CPU Interface Filtering Configuration** page, as shown below. There are three **Access Profile Configuration** pages; one for **Ethernet** (or MAC address-based) profile configuration, one for **IP** address-based profile configuration and one for the **Packet Content Mask**. Users can switch between the three **Access Profile Configuration** pages by using the **Type** drop-down menu. The page shown below is the **Ethernet CPU Interface Filtering Configuration** page.

CPU Interface Filtering Configuration	
Profile ID(1-5)	1
Type	Ethernet
VLAN	<input type="checkbox"/>
Source MAC	<input type="checkbox"/> 00-00-00-00-00-00
Destination MAC	<input type="checkbox"/> 00-00-00-00-00-00
Ethernet type	<input type="checkbox"/>
Apply	
Show All CPU Interface Filtering Table Entries	

Figure 6- 73. CPU Interface Filtering Configuration window – Ethernet

Parameter	Description
Profile ID (1-5)	Type in a unique identifier number for this profile set. This value can be set from 1 - 5.
Type	Select profile based on Ethernet (MAC Address), IP address or Packet Content Mask. This will change the menu according to the requirements for the type of profile. <ul style="list-style-type: none"> • Select <i>Ethernet</i> to instruct the Switch to examine the layer 2 part of each packet header. • Select <i>IP</i> to instruct the Switch to examine the IP address in each frame's header. • Select <i>Packet Content Mask</i> to specify a mask to hide the content of the packet header.
VLAN	Selecting this option instructs the Switch to examine the VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
Source MAC	Source MAC Mask - Enter a MAC address mask for the source MAC address.
Destination MAC	Destination MAC Mask - Enter a MAC address mask for the destination MAC address.
Ethernet type	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.

Click **Apply** to set this entry in the Switch's memory.

The page shown below is the **IP Access Profile Configuration** page.

CPU Interface Filtering Configuration	
Profile ID(1-5)	1
Type	IP
VLAN	<input type="checkbox"/>
Source IP Mask	<input type="checkbox"/> 0.0.0.0
Destination IP Mask	<input type="checkbox"/> 0.0.0.0
Dscp	<input type="checkbox"/>
Protocol	<input type="checkbox"/> ICMP <input type="checkbox"/> type <input type="checkbox"/> code <input type="checkbox"/> IGMP <input type="checkbox"/> type <input type="checkbox"/> TCP <input type="checkbox"/> src port mask 0000 <input type="checkbox"/> dest port mask 0000 <input type="checkbox"/> flag mask bit <input type="checkbox"/> urg <input type="checkbox"/> ack <input type="checkbox"/> psh <input type="checkbox"/> rst <input type="checkbox"/> syn <input type="checkbox"/> fin <input type="checkbox"/> UDP <input type="checkbox"/> src port mask 0000 <input type="checkbox"/> dest port mask 0000 <input type="checkbox"/> protocol id <input type="checkbox"/> user mask 00000000
Apply	
Show All CPU Interface Filtering Table Entries	

Figure 6- 74. CPU Interface Filtering Configuration window- IP

Parameter	Description
Profile ID (1-5)	Type in a unique identifier number for this profile set. This value can be set from 1 - 5.
Type	<p>Select profile based on Ethernet (MAC Address), IP address or Packet Content Mask. This will change the menu according to the requirements for the type of profile.</p> <ul style="list-style-type: none"> • Select <i>Ethernet</i> to instruct the Switch to examine the layer 2 part of each packet header. • Select <i>IP</i> to instruct the Switch to examine the IP address in each frame's header. • Select <i>Packet Content Mask</i> to specify a mask to hide the content of the packet header.
VLAN	Selecting this option instructs the Switch to examine the VLAN part of each packet header and use this as the, or part of the criterion for forwarding.
Source IP Mask	Enter an IP address mask for the source IP address.
Destination IP Mask	Enter an IP address mask for the destination IP address.
DSCP	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding.
Protocol	<p>Selecting this option instructs the Switch to examine the protocol type value in each frame's header. Users must then specify what protocol(s) to include according to the following guidelines:</p> <p>Select ICMP to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header.</p> <ul style="list-style-type: none"> • Select Type to further specify that the access profile will apply an ICMP type value, or specify Code to further specify that the access profile will apply an ICMP code value. <p>Select IGMP to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header.</p> <ul style="list-style-type: none"> • Select Type to further specify that the access profile will apply an IGMP type value <p>Select TCP to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP requires specification of a source port mask and/or a destination port mask. The user may also identify which flag bits to filter. Flag bits are parts of a packet that determine what to do with the packet. The user may filter packets by filtering certain flag bits within the packets, by checking the boxes corresponding to the flag bits of the TCP field. The user may choose between urg (urgent), ack (acknowledgement), psh (push), rst (reset), syn (synchronize), fin (finish).</p> <ul style="list-style-type: none"> • src port mask - Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to filter. • dest port mask - Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) which you wish to filter. <p>Select UDP to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires specification of a source port mask and/or a destination port mask.</p> <ul style="list-style-type: none"> • src port mask - Specify a UDP port mask for the source port in hex form (hex 0x0-0xffff). • dest port mask - Specify a UDP port mask for the destination port in hex form (hex 0x0-0xffff). <p>protocol id - Enter a value defining the protocol ID in the packet header to mask. Specify the protocol ID mask in hex form (hex 0x0-0xffffffff).</p>

Click **Apply** to set this entry in the Switch's memory.

The page shown below is the **Packet Content Mask** configuration window.

Figure 6- 75. CPU Interface Filtering Configuration window- Packet Content

This screen will aid the user in configuring the Switch to mask packet headers beginning with the offset value specified. The following fields are used to configure the **Packet Content Mask**:

Parameter	Description
Profile ID (1-5)	Type in a unique identifier number for this profile set. This value can be set from 1 - 5.
Type	Select profile based on Ethernet (MAC Address), IP address or Packet Content Mask. This will change the menu according to the requirements for the type of profile. <ul style="list-style-type: none"> • Select <i>Ethernet</i> to instruct the Switch to examine the layer 2 part of each packet header. • Select <i>IP</i> to instruct the Switch to examine the IP address in each frame's header. • Select <i>Packet Content Mask</i> to specify a mask to hide the content of the packet header.
Offset	This field will instruct the Switch to mask the packet header beginning with the offset value specified: <ul style="list-style-type: none"> • <i>value (0-15)</i> - Enter a value in hex form to mask the packet from the beginning of the packet to the 15th byte. • <i>value (16-31)</i> – Enter a value in hex form to mask the packet from byte 16 to byte 31. • <i>value (32-47)</i> – Enter a value in hex form to mask the packet from byte 32 to byte 47. • <i>value (48-63)</i> – Enter a value in hex form to mask the packet from byte 48 to byte 63. • <i>value (64-79)</i> – Enter a value in hex form to mask the packet from byte 64 to byte 79.

Click **Apply** to implement changes made.

To establish the rule for a previously created CPU Access Profile:

In the **Configuration** folder, click the **CPU Interface Filtering > CPU Interface Filtering State** to open the **CPU Interface Filtering Table**.

Profile ID	Type	Access Rule	Delete
1	Ethernet	Modify	X
2	IP	Modify	X
3	Packet Content	Modify	X

Figure 6- 76. CPU Interface Filtering Table

In this window, the user may add a rule to a previously created CPU access profile by clicking the corresponding Modify button of the entry to configure, **Ethernet**, **IP** or **Packet Content**. Each entry will open a new and unique window, as shown in the examples below.

Profile ID	Mode	Type	Access ID	Display	Delete
1	Permit	Ethernet	1	View	X

[Show All CPU Interface Filtering Entries](#)

Figure 6- 77. CPU Interface Filtering Table – Ethernet

To create a new rule set for an access profile click the **Add** button. A new window is displayed. To remove a previously created rule, click the corresponding **X** button. The following window is used for the Ethernet Rule configuration.

CPU Interface Filtering Rule Configuration

Profile ID: 1

Mode: Permit Deny

Access ID(1-100): 1

Type: Ethernet

VLAN Name:

Source MAC: 00-00-00-00-00-00

Destination MAC: 00-00-00-00-00-00

Ethernet Type: 0000

Port(UniID:PortNum):

[Show All CPU Interface Filtering Rule Entries](#)

Apply

Figure 6- 78. CPU Interface Filtering Rule Configuration – Ethernet

To set the Access Rule for Ethernet, adjust the following parameters and click **Apply**.

Parameters	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify that packets that match the access profile are not forwarded by the Switch and will be filtered.
Access ID	Type in a unique identifier number for this access and priority. This value can be set from 1 - 100.
Type	Selected profile based on Ethernet (MAC Address), IP address or Packet Content. <ul style="list-style-type: none"> • <i>Ethernet</i> instructs the Switch to examine the layer 2 part of each packet header. • <i>IP</i> instructs the Switch to examine the IP address in each frame's header. • <i>Packet Content Mask</i> instructs the Switch to examine the packet header.
VLAN Name	Allows the entry of a name for a previously configured VLAN.
Source MAC	Source MAC Address - Enter a MAC Address for the source MAC address.
Destination MAC	Destination MAC Address - Enter a MAC Address mask for the destination MAC address.
Ethernet Type	Specifies that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value (hex 0x0-0xffff) in the packet header. The Ethernet type value may be set in the form: hex 0x0-0xffff, which means the user may choose any combination of letters and numbers ranging from a-f and from 0-9999.
Port	The Access Rule may be configured on a per-port basis by entering the port number of the line card in the chassis into this field. The port list is specified by listing the lowest line card number and the beginning port number on that line card, separated by a colon. Then the highest line card number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies line card number 1, port 3. 2:4 specifies line card number 2, port 4. 1:3 - 2:4 specifies all of the ports between line card 1, port 3 and switch 2, port 4 – in numerical order. Entering <i>all</i> will denote all ports on the Switch.

To view the settings of a previously correctly configured rule, click [View](#) in the **Access Rule Table** to view the following screen:

CPU Interface Filtering Rule Display	
Profile ID	1
Access ID	1
Mode	Permit
Type	Ethernet
VLAN Name	default
Source Mac	-----
Destination Mac	-----
Ethernet Type	-----
Port	1:1-1:12,3:1-3:16,4:1-4:12,6:1-6:12,7:1-7:12,8:1-8:12
Show All CPU Interface Filtering Rule Entries	

Figure 6- 79. CPU Interface Filtering Rule Display – Ethernet

The following window is the **CPU Interface Filtering Rule Table** for IP.

CPU Interface Filtering Rule Table					
Profile ID	Mode	Type	Access ID	Display	Delete
2	Permit	IP	1	View	

[Add](#)

[Show All CPU Interface Filtering Entries](#)

Figure 6- 80. CPU Interface Filtering Rule Table – IP

To create a new rule set for an access profile click the **Add** button. A new window is displayed. To remove a previously created rule, click the corresponding button. The following window is used for the IP Rule configuration.

CPU Interface Filtering Rule Configuration	
Profile ID	2
Mode	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Access ID(1-100)	1
Type	IP
VLAN Name	
Source IP	0.0.0.0
Destination IP	0.0.0.0
Dscp(0-63)	0
Port(UniID:PortNum)	

[Show All CPU Interface Filtering Rule Entries](#)

[Apply](#)

Figure 6- 81. CPU Interface Filtering Rule Configuration – IP

Configure the following **Access Rule Configuration** settings for IP:

Parameter	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select <i>Permit</i> to specify that packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify that packets that match the access profile are not forwarded by the Switch and will be filtered.
Access ID	Type in a unique identifier number for this access. This value can be set from 1 - 100.
Type	Selected profile based on Ethernet (MAC Address), IP address or Packet Content. <ul style="list-style-type: none"> <i>Ethernet</i> instructs the Switch to examine the layer 2 part of each packet header. <i>IP</i> instructs the Switch to examine the IP address in each frame's header. <i>Packet Content Mask</i> instructs the Switch to examine the packet header.

VLAN Name	Allows the entry of a name for a previously configured VLAN.
Source IP	Source IP Address - Enter an IP Address mask for the source IP address.
Destination IP	Destination IP Address- Enter an IP Address mask for the destination IP address.
Port	The Access Rule may be configured on a per-port basis by entering the port number of the line card in the chassis into this field. The port list is specified by listing the lowest line card number and the beginning port number on that line card, separated by a colon. Then the highest line card number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies line card number 1, port 3. 2:4 specifies line card number 2, port 4. 1:3 - 2:4 specifies all of the ports between line card 1, port 3 and line card 2, port 4 – in numerical order. Entering <i>all</i> will denote all ports on the Switch.

To view the settings of a previously correctly configured rule, click [View](#) in the **Access Rule Table** to view the following screen:

CPU Interface Filtering Rule Display	
Profile ID	2
Access ID	1
Mode	Permit
Type	IP
VLAN Name	default
Source IP	-----
Destination IP	-----
Dscp	-----
Protocol	-----
Port	1:1-1:12,3:1-3:16,4:1-4:12,6:1-6:12,7:1-7:12,8:1-8:12

[Show All CPU Interface Filtering Rule Entries](#)

Figure 6- 82. CPU Interface Filtering Rule Display - IP

The following window is the **CPU Interface Filtering Rule Table** for Packet Content.

CPU Interface Filtering Rule Table					
Profile ID	Mode	Type	Access ID	Display	Delete
3	Permit	Packet Content	1	View	<input type="button" value="X"/>

[Show All CPU Interface Filtering Entries](#)

Figure 6- 83. CPU Interface Filtering Rule Table – Packet Content

To remove a previously created rule, select it and click the button. To add a new Access Rule, click the **Add** button:

CPU Interface Filtering Rule Configuration				
Profile ID	3			
Mode	<input checked="" type="radio"/> Permit <input type="radio"/> Deny			
Access ID(1-100)	1			
Type	Packet Content			
Offset_0-15	<input type="checkbox"/>	<input type="text" value="00000000"/>	<input type="text" value="00000000"/>	<input type="text" value="00000000"/>
Offset_16-31	<input type="checkbox"/>	<input type="text" value="00000000"/>	<input type="text" value="00000000"/>	<input type="text" value="00000000"/>
Offset_32-47	<input type="checkbox"/>	<input type="text" value="00000000"/>	<input type="text" value="00000000"/>	<input type="text" value="00000000"/>
Offset_48-63	<input type="checkbox"/>	<input type="text" value="00000000"/>	<input type="text" value="00000000"/>	<input type="text" value="00000000"/>
Offset_64-79	<input type="checkbox"/>	<input type="text" value="00000000"/>	<input type="text" value="00000000"/>	<input type="text" value="00000000"/>
Port(UniID:PortNum)	<input type="text"/>			
				<input type="button" value="Apply"/>
Show All CPU Interface Filtering Rule Entries				

Figure 6- 84. CPU Interface Filtering Rule Configuration - Packet Content

To set the Access Rule for Ethernet, adjust the following parameters and click **Apply**.

Parameters	Description
Profile ID	This is the identifier number for this profile set.
Mode	<p>Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below).</p> <p>Select <i>Deny</i> to specify that packets that match the access profile are not forwarded by the Switch and will be filtered.</p>
Access ID	Type in a unique identifier number for this access. This value can be set from 1 - 100.
Type	<p>Selected profile based on Ethernet (MAC Address), IP address or Packet Content.</p> <ul style="list-style-type: none"> • <i>Ethernet</i> instructs the Switch to examine the layer 2 part of each packet header. • <i>IP</i> instructs the Switch to examine the IP address in each frame's header. • <i>Packet Content Mask</i> instructs the Switch to examine the packet header.
Offset	<p>This field will instruct the Switch to mask the packet header beginning with the offset value specified:</p> <ul style="list-style-type: none"> • <i>value (0-15)</i> - Enter a value in hex form to mask the packet from the beginning of the packet to the 15th byte. • <i>value (16-31)</i> - Enter a value in hex form to mask the packet from byte 16 to <i>byte 31</i>. • <i>value (32-47)</i> - Enter a value in hex form to mask the packet from byte 32 to byte 47. • <i>value (48-63)</i> - Enter a value in hex form to mask the packet from byte 48 to byte 63. • <i>value (64-79)</i> - Enter a value in hex form to mask the packet from byte 64 to byte 79.
Port	<p>The Access Rule may be configured on a per-port basis by entering the port number of the line card in the chassis into this field. The port list is specified by listing the lowest line card number and the beginning port number on that line card, separated by a colon. Then the highest line card number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies line card number 1, port 3. 2:4 specifies line card number 2, port 4. 1:3 - 2:4 specifies all of the ports between line card 1, port 3 and line card 2, port 4 – in numerical order. Entering <i>all</i> will denote all ports on the Switch.</p>

To view the settings of a previously correctly configured rule, click  in the **Access Rule Table** to view the following screen:

CPU Interface Filtering Rule Display	
Profile ID	3
Access ID	1
Mode	Permit
Type	Packet Content
VLAN Name	-----
Offset 0-15	0x00000000 0x00000000 0x00000000 0x00000000
Offset 16-31	-----
Offset 32-47	-----
Offset 48-63	-----
Offset 64-79	-----
Port	1:1-1:12,3:1-3:16,4:1-4:12,6:1-6:12,7:1-7:12,8:1-8:12
Show All CPU Interface Filtering Rule Entries	

Figure 6- 85. CPU Interface Filtering Rule Display – Packet Content

Safeguard Engine

Developed by D-Link, the **Safeguard Engine** is a robust and innovative technology which will automatically reduce the negative impact of repeated packet flooding to the Switch's CPU. As a result, D-Link Switches will be better protected from frequent interruptions by malicious viruses or worm attacks.

Periodically, malicious hosts on the network will attack the Switch by utilizing packet flooding (ARP Storm) or other methods. These attacks may increase the CPU utilization beyond its capability. To alleviate this problem, the Safeguard Engine function was added to the Switch's software.

The Safeguard Engine can help the overall operability of the Switch by minimizing the workload of the Switch while the attack is ongoing, thus making it capable to forward essential packets over its network in a limited bandwidth. When the Switch either (a) receives too many packets to process or (b) exerts too much memory, it will enter an **Exhausted** mode. When in this mode, the Switch will perform the following tasks to minimalize the CPU usage:

1. It will limit bandwidth of receiving ARP packets. The user may implement this in two ways, by using the Mode pull down menu in the screen below:
 - a. When **Strict** is chosen, the Switch will stop receiving ARP packets not destined for the Switch. This will eliminate all unnecessary ARP packets while allowing the essential ARP packets to pass through to the Switch's CPU.
 - b. When **Fuzzy** is chosen, the Switch will minimize the ARP packet bandwidth received by the Switch by adjusting the bandwidth for all ARP packets, whether destined for the Switch or not. The Switch uses an internal algorithm to filter ARP packets through, with a higher percentage set aside for ARP packets destined for the Switch.
2. It will limit the bandwidth of IP packets received by the Switch. The user may implement this in two ways, by using the Mode pull down menu in the screen below:
 - a. When **Strict** is chosen, the Switch will stop receiving all unnecessary broadcast IP packets, even if the high CPU utilization is not caused by the high receival rate of broadcast IP packets.
 - b. When **Fuzzy** is chosen, the Switch will minimize the IP packet bandwidth received by the Switch by adjusting the bandwidth for all IP packets, by setting a acceptable bandwidth for both unicast and broadcast IP packets. The Switch uses an internal algorithm to filter IP packets through while adjusting the bandwidth dynamically.

IP packets may also be limited by the Switch by configuring only certain IP addresses to be accepted. This method can be accomplished through the CPU Interface Filtering mechanism explained in the previous section. Once the user configures these acceptable IP addresses, other packets containing different IP addresses will be dropped by the Switch, thus limiting the bandwidth of IP packets. To keep the process moving fast, be sure not to add many conditions on which to accept these acceptable IP addresses and their packets, this limiting the CPU utilization.

Once in Exhausted mode, the packet flow will decrease by half of the level that caused the Switch to enter Exhausted mode. After the packet flow has stabilized, the rate will initially increase by 25% and then return to a normal packet flow.



NOTICE: When the Safeguard Engine is enabled, the Switch will allot bandwidth to various traffic flows (ARP, IP) using the FFP (Fast Filter Processor) metering table to control the CPU utilization and limit traffic. This may limit the speed of routing traffic over the network.

To configure the Safeguard Engine for the Switch, click **Configuration > Safeguard Engine > Safeguard Engine Settings**, which will open the following window.

Safeguard Engine Settings	
State	Disabled ▾
Trap / Log	Disabled ▾
Mode	Fuzzy ▾
CPU Utilization Settings	
Rising Threshold (20-100)	30
Falling Threshold (20-100)	20
Safeguard Engine Current Status	normal mode
Apply	

Developed by D-Link, the [Safeguard Engine](#) is a robust and innovative technology which will automatically reduce the negative impact of repeated packet flooding to the Switch's CPU. As a result, D-Link Switches will be better protected from frequent interruptions by malicious viruses or worm attacks.

Figure 6- 86. Safeguard Engine Settings window

To configure, set the following parameters and click Apply.

Parameter	Description
Safeguard Engine Settings	
State	Use the pull-down menu to globally enable or disable the Safeguard Engine settings for the Switch.
Trap / Log	Use the pull-down menu to enable or disable the sending of messages to the device's SNMP agent and switch log once the Safeguard Engine has been activated by a high CPU utilization rate.
Mode	Used to select the type of Safeguard Engine to be activated by the Switch when the CPU utilization reaches a high rate. The user may select: <i>Fuzzy</i> – If selected, this function will instruct the Switch to minimize the IP and ARP traffic flow to the CPU by dynamically allotting an even bandwidth to all traffic flows. <i>Strict</i> – If selected, this function will stop accepting all ARP packets not intended for the Switch, and will stop receiving all unnecessary broadcast IP packets, until the storm has subsided. (For line cards DES-6505, DES-6507, DES-6509 and DES-6512, the Safeguard Engine will always be Strict mode regardless of configuration, due to a chipset limitation.) The default setting is Fuzzy mode.
CPU Utilization	
Rising Threshold	Used to configure the acceptable level of CPU utilization before the Safeguard Engine mechanism is enabled. Once the CPU utilization reaches this percentage level, the Switch will move into the Safeguard Engine state, based on the parameters provided in this window.
Falling Threshold	Used to configure the acceptable level of CPU utilization as a percentage, where the Switch leaves the Safeguard Engine state and returns to normal mode.
Safeguard Engine Status	This is a read-only field that will state the current Safeguard Engine mode of the Switch. This field may read "normal mode" or "exhausted mode".

Click **Apply** to implement changes made to this window.

Port Access Entity (802.1X)

802.1x Port-Based and MAC-Based Access Control

The IEEE 802.1x standard is a security measure for authorizing and authenticating users to gain access to various wired or wireless devices on a specified Local Area Network by using a Client and Server based access control model. This is accomplished by using a RADIUS server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the Client and the Server. The following figure represents a basic EAPOL packet:

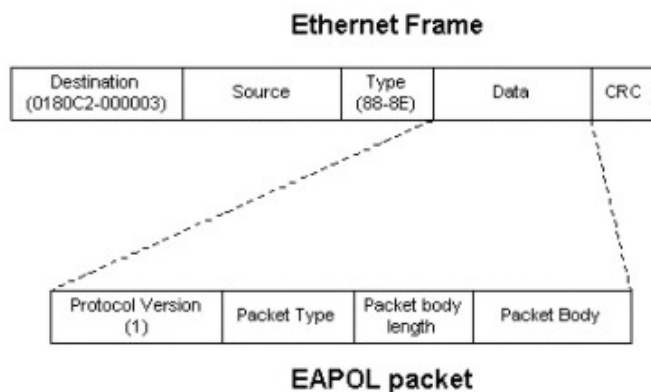


Figure 6- 87. The EAPOL Packet

Utilizing this method, unauthorized devices are restricted from connecting to a LAN through a port to which the user is connected. EAPOL packets are the only traffic that can be transmitted through the specific port until authorization is granted. The 802.1x Access Control method holds three roles, each of which are vital to creating and upkeeping a stable and working Access Control security method.

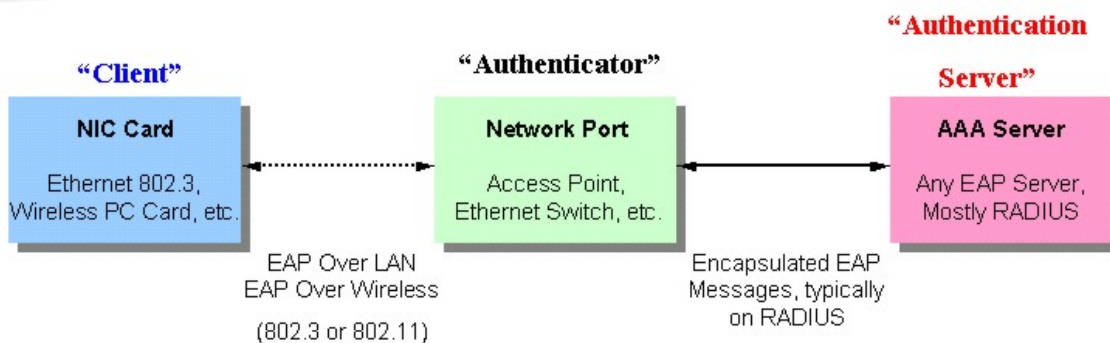


Figure 6- 88. The three roles of 802.1x

The following section will explain the three roles of Client, Authenticator and Authentication Server in greater detail.

Authentication Server

The Authentication Server is a remote device that is connected to the same network as the Client and Authenticator, must be running a RADIUS Server program and must be configured properly on the Authenticator (Switch). Clients connected to a port on the Switch must be authenticated by the Authentication Server (RADIUS) before attaining any services offered by the Switch on the LAN. The role of the Authentication Server is to certify the identity of the Client attempting to access the network by exchanging secure information between the RADIUS server and the Client through EAPOL packets and, in turn, informs the Switch whether or not the Client is granted access to the LAN and/or switches services.

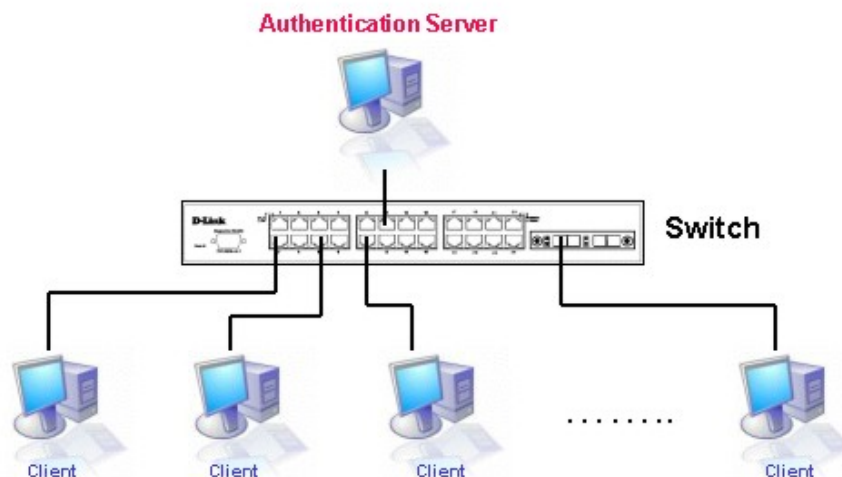


Figure 6- 89. The Authentication Server

Authenticator

The Authenticator (the Switch) is an intermediary between the Authentication Server and the Client. The Authenticator serves two purposes when utilizing 802.1x. The first purpose is to request certification information from the Client through EAPOL packets, which is the only information allowed to pass through the Authenticator before access is granted to the Client. The second purpose of the Authenticator is to verify the information gathered from the Client with the Authentication Server, and to then relay that information back to the Client.

Three steps must be implemented on the Switch to properly configure the Authenticator.

1. The 802.1x State must be *Enabled*. (**Configuration / Port Access Entity / 802.1X Auth Mode Settings**)
2. The 802.1x settings must be implemented by port (**Configuration / Port Access Entity / 802.1X Authenticator Settings**)
3. A RADIUS server must be configured on the Switch. (**Configuration / Port Access Entity / RADIUS Server**)

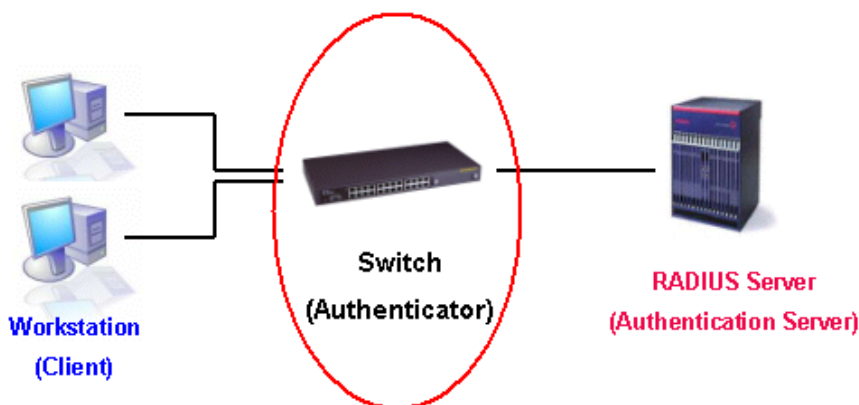


Figure 6- 90. The Authenticator

Client

The Client is simply the endstation that wishes to gain access to the LAN or switch services. All endstations must be running software that is compliant with the 802.1x protocol. For users running Windows XP, that software is included within the operating system. All other users are required to attain 802.1x client software from an outside source. The Client will request access to the LAN and or Switch through EAPOL packets and, in turn will respond to requests from the Switch.

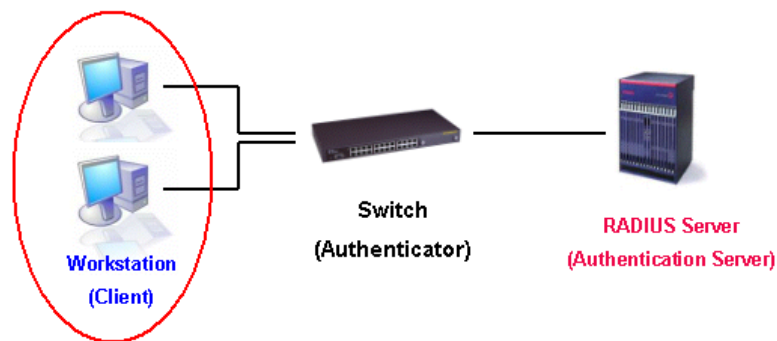


Figure 6- 91. The Client

Authentication Process

Utilizing the three roles stated above, the 802.1x protocol provides a stable and secure way of authorizing and authenticating users attempting to access the network. Only EAPOL traffic is allowed to pass through the specified port before a successful authentication is made. This port is “locked” until the point when a Client with the correct username and password (and MAC address if 802.1x is enabled by MAC address) is granted access and therefore successfully “unlocks” the port. Once unlocked, normal traffic is allowed to pass through the port. The following figure displays a more detailed explanation of how the authentication process is completed between the three roles stated above.

802.1X Authentication process

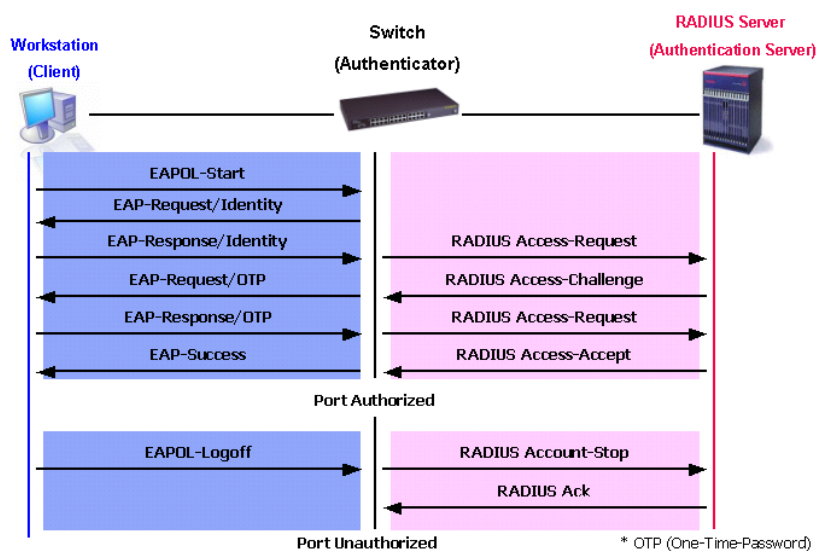


Figure 6- 92. The 802.1x Authentication Process

The D-Link implementation of 802.1x allows network administrators to choose between two types of Access Control used on the Switch, which are:

1. Port-Based Access Control – This method requires only one user to be authenticated per port by a remote RADIUS server to allow the remaining users on the same port access to the network.
2. MAC-Based Access Control – Using this method, the Switch will automatically learn up to sixteen MAC addresses by port and set them in a list. Each MAC address must be authenticated by the Switch using a remote RADIUS server before being allowed access to the Network.

Understanding 802.1x Port-based and MAC-based Network Access Control

The original intent behind the development of 802.1X was to leverage the characteristics of point-to-point in LANs. As any single LAN segment in such infrastructures has no more than two devices attached to it, one of which is a Bridge Port. The Bridge Port detects events that indicate the attachment of an active device at the remote end of the link, or an active device becoming inactive. These events can be used to control the authorization state of the Port and initiate the process of authenticating the attached device if the Port is unauthorized. This is the Port-Based Network Access Control.

Port-Based Network Access Control

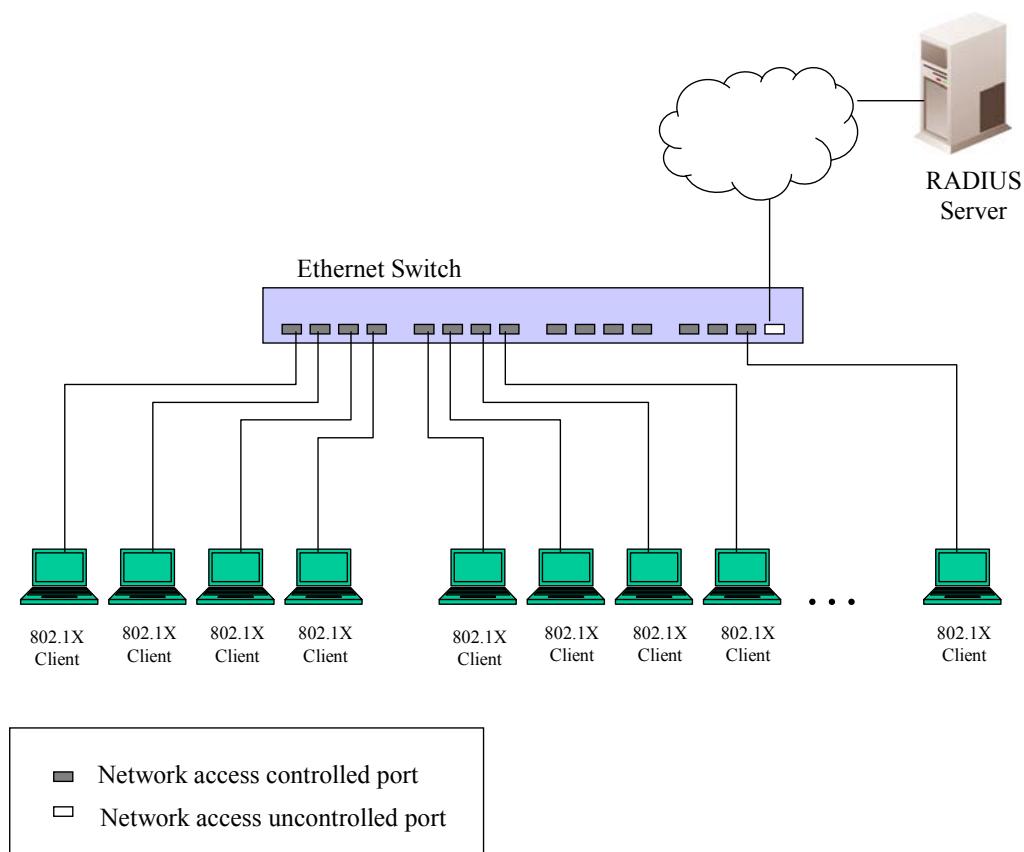


Figure 6- 93. Example of Typical Port-Based Configuration

Once the connected device has successfully been authenticated, the Port then becomes Authorized, and all subsequent traffic on the Port is not subject to access control restriction until an event occurs that causes the Port to become Unauthorized. Hence, if the Port is actually connected to a shared media LAN segment with more than one attached device, successfully authenticating one of the attached devices effectively provides access to the LAN for all devices on the shared segment. Clearly, the security offered in this situation is open to attack.

MAC-Based Network Access Control

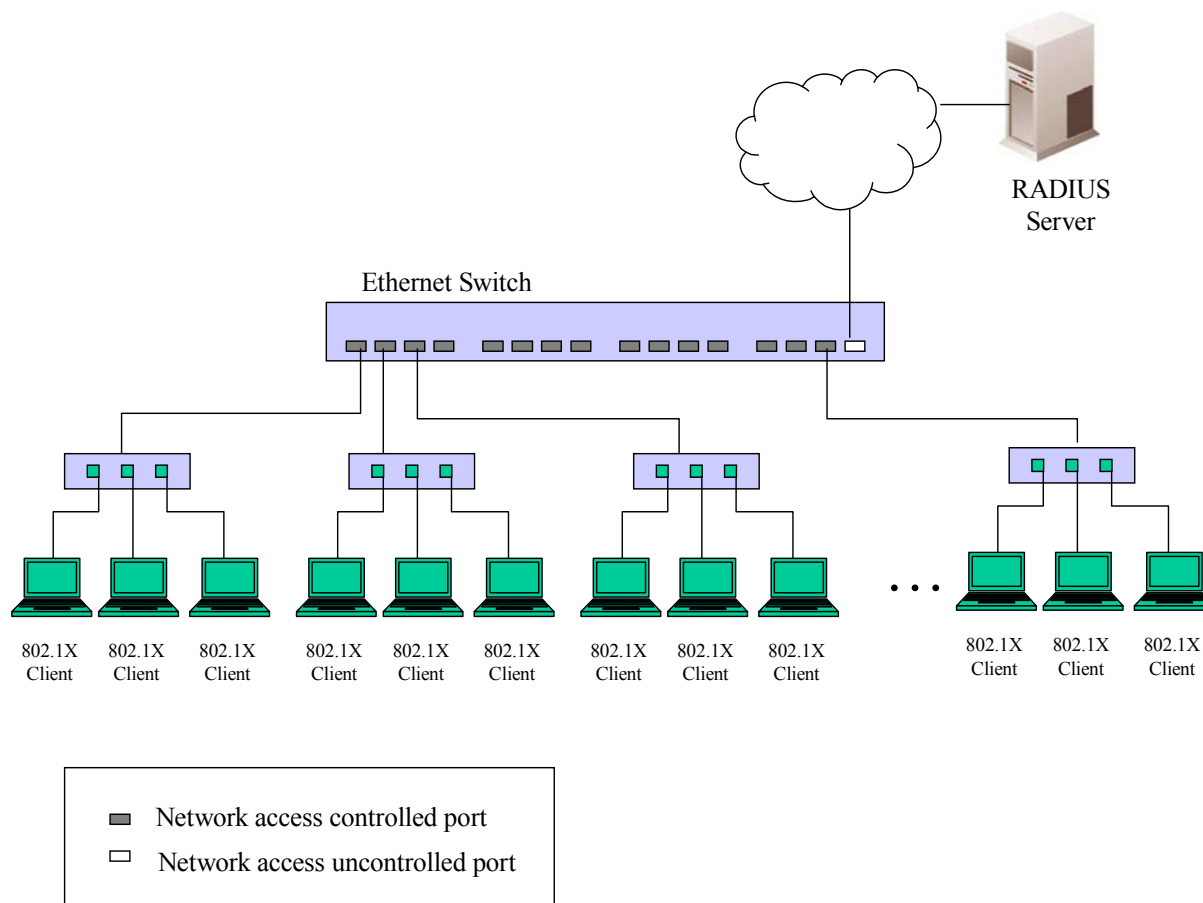


Figure 6- 94. Example of Typical MAC-Based Configuration

In order to successfully make use of 802.1X in a shared media LAN segment, it would be necessary to create “logical” Ports, one for each attached device that required access to the LAN. The Switch would regard the single physical Port connecting it to the shared media segment as consisting of a number of distinct logical Ports, each logical Port being independently controlled from the point of view of EAPOL exchanges and authorization state. The Switch learns each attached devices’ individual MAC addresses, and effectively creates a logical Port that the attached device can then use to communicate with the LAN via the Switch.

802.1x Auth Mode Settings

The following window is used to set the type of authentication mode used in employing the 802.1X security settings. Simply use the pull down menu to select **Port-based** or **MAC-based 802.1X** and click the **Apply** button.



Figure 6- 95. 802.1X Auth Mode Settings window

802.1X Authenticator Settings

To configure the 802.1X authenticator settings, click **Configuration > Port Access Entity > 802.1x Authenticator Settings**:

Unit: 1

802.1X Authenticator Settings

Port	AdmDir	Ctrl Stat	TxPeriod	Quiet Period	Supp-Timeout	Server-Timeout	MaxReq	ReAuth Period	ReAuth Enabled
1	both	auto	30	60	30	30	2	3600	no
2	both	auto	30	60	30	30	2	3600	no
3	both	auto	30	60	30	30	2	3600	no
4	both	auto	30	60	30	30	2	3600	no
5	both	auto	30	60	30	30	2	3600	no
6	both	auto	30	60	30	30	2	3600	no
7	both	auto	30	60	30	30	2	3600	no
8	both	auto	30	60	30	30	2	3600	no
9	both	auto	30	60	30	30	2	3600	no
10	both	auto	30	60	30	30	2	3600	no
11	both	auto	30	60	30	30	2	3600	no
12	both	auto	30	60	30	30	2	3600	no

Figure 6- 96. Configure 802.1X Authenticator Parameter window

To view the 802.1X authenticator settings on a different line card in the chassis, use the **Unit** pull-down menu to select that line card by its ID number in the chassis. To configure the settings by port, click on the hyperlinked port number under the **Port** heading, which will display the following table to configure:

802.1X Authenticator Settings-Unit 1	
Unit	1
From	Port 1
To	Port 1
AdmDir	both
PortControl	auto
TxPeriod	30
QuietPeriod	60
Supp Timeout	30
ServerTimeout	30
MaxReq	2
ReAuthPeriod	3600
ReAuth	Disabled
Show Authenticators Setting for Unit 1 Apply	

Figure 6- 97. 802.1X Authenticator Settings – Modify window

This screen allows you to set the following features:

Parameter	Description
Unit	Choose the Switch ID number of the line card in the chassis to be modified.
From [] To []	Enter the port or ports to be set.
AdmCtrlDir	<p>Sets the administrative-controlled direction to either <i>in</i> or <i>both</i>.</p> <p>If <i>in</i> is selected, control is only exerted over incoming traffic through the port you selected in the first field.</p> <p>If <i>both</i> is selected, control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field.</p>
PortControl	<p>This allows you to control the port authorization state.</p> <p>Select <i>forceAuthorized</i> to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client.</p> <p>If <i>forceUnauthorized</i> is selected, the port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. The Switch cannot provide authentication services to the client through the interface.</p> <p>If <i>Auto</i> is selected, it will enable 802.1X and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server.</p> <p>The default setting is <i>Auto</i>.</p>
TxPeriod	This sets the TxPeriod of time for the authenticator PAE state machine. This value determines the period of an EAP Request/Identity packet transmitted to the client. The default setting is 30 seconds.

QuietPeriod	This allows the user to set the number of seconds that the Switch remains in the quiet state following a failed authentication exchange with the client. The default setting is 60 seconds.
SuppTimeout	This value determines timeout conditions in the exchanges between the Authenticator and the client. The default setting is 30 seconds.
ServerTimeout	This value determines timeout conditions in the exchanges between the Authenticator and the authentication server. The default setting is 30 seconds.
MaxReq	The maximum number of times that the Switch will retransmit an EAP Request to the client before it times out of the authentication sessions. The default setting is 2.
ReAuthPeriod	A constant that defines a nonzero number of seconds between periodic reauthentication of the client. The default setting is 3600 seconds.
ReAuth	Determines whether regular reauthentication will take place on this port. The default setting is <i>Disabled</i> .

Click **Apply** to implement configuration changes. To view configurations for the **802.1X Authenticator Settings** on a port-by-port basis, see the **802.1X Authenticator Settings** table.

Local Users

In the **Configuration** folder, open the **Port Access Entity** folder and click **Local Users** to open the **802.1x Local User Table Configuration** window. This window will allow the user to set different local users on the Switch.

802.1x Local User Table Configuration		
User Name	Password	Confirm Password
<input type="text"/>	<input type="text"/>	<input type="text"/>
		Apply
Total Entries: 1		
802.1x Local User Table		
User Name	Password	Delete
Darren	1	X

Figure 6- 98. 802.1x User and 802.1x User Table window

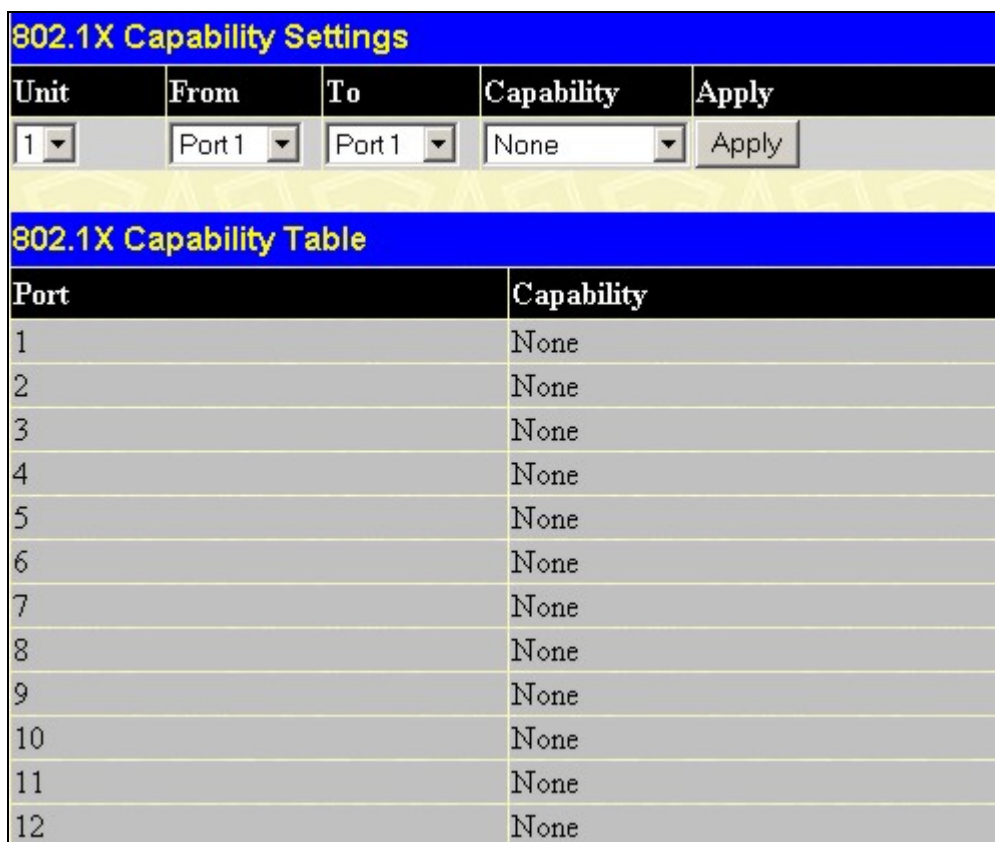
Enter a **User Name**, **Password** and confirmation of that password. Properly configured local users will be displayed in the **802.1x Local User Table** in the same window.

PAE System Control

Existing 802.1x port and MAC settings are displayed and can be configured using the windows below.

Port Capability

Click **Port Access Entity > PAE System Control > 802.1x Capability Settings** to view the following window:



802.1X Capability Settings				
Unit	From	To	Capability	Apply
1	Port 1	Port 1	None	Apply

802.1X Capability Table	
Port	Capability
1	None
2	None
3	None
4	None
5	None
6	None
7	None
8	None
9	None
10	None
11	None
12	None

Figure 6- 99. 802.1x Capability Settings and Table window

To set up the Switch's 802.1x port-based authentication, select the line card in the chassis by using the **Unit** pull-down menu and then select which ports are to be configured in the **From** and **To** fields. Next, enable the ports by selecting *Authenticator* from the drop-down menu under **Capability**. Click **Apply** allow changes to take effect.

Configure the following 802.1x capability settings:

Parameter	Description
Unit	Choose the Switch ID number of the line card in the switch stack to be modified.
From and To	Ports being configured for 802.1x settings.
Capability	Two role choices can be selected: <i>Authenticator</i> - A user must pass the authentication process to gain access to the network. <i>None</i> - The port will not be controlled by the 802.1x functions.

Initializing Ports for Port Based 802.1x

Existing 802.1x port and MAC settings are displayed and can be configured using the window below.

Click **Port Access Entity > PAE System Control > Initialize Port(s)** to open the following window:

Initialize Port			
Unit	From	To	Apply
1	Port 1	Port 1	Apply

Initialize Port Table			
Port	Auth PAE State	Backend_State	Port Status
4	ForceAuth	Success	Authorized
5	ForceAuth	Success	Authorized
6	ForceAuth	Success	Authorized
7	ForceAuth	Success	Authorized
8	ForceAuth	Success	Authorized
9	ForceAuth	Success	Authorized
10	ForceAuth	Success	Authorized
11	ForceAuth	Success	Authorized
12	ForceAuth	Success	Authorized

Figure 6- 100. Initialize Port window

This window allows you to initialize a port or group of ports. The **Initialize Port Table** in the bottom half of the window displays the current status of the port(s).

This window displays the following information:

Parameter	Description
Unit	Choose the Switch ID number of the line card in the chassis to be modified.
From and To	Select ports to be initialized.
Port	A read only field indicating a port on the Switch.
MAC Address	The MAC address of the Switch connected to the corresponding port, if any.
Auth PAE State	The Authenticator PAE State will display one of the following: <i>Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth, and N/A.</i>
Backend State	The Backend Authentication State will display one of the following: <i>Request, Response, Success, Fail, Timeout, Idle, Initialize, and N/A.</i>
Port Status	The status of the controlled port can be <i>Authorized, Unauthorized, or N/A.</i>

Initializing Ports for MAC Based 802.1x

To initialize ports for the MAC side of 802.1x, the user must first enable 802.1x by MAC address in the **Advanced Settings** window. Click **Configuration > Port Access Entity > PAE System Control > Initialize Port(s)** to open the following window:

Figure 6- 101. Initialize Ports (MAC based 802.1x)

To initialize ports, first choose the line card in the chassis by using the **Unit** pull-down menu, then the range of ports in the **From** and **To** field. Then the user must specify the MAC address to be initialized by entering it into the **MAC Address** field and checking the corresponding check box. To begin the initialization, click **Apply**.



NOTE: The user must first globally enable 802.1X in the **802.1X Auth Mode Settings** window before initializing ports. Information in the **Initialize Ports Table** cannot be viewed before enabling 802.1X.

Reauthenticate Port(s) for Port Based 802.1x

This window allows users to reauthenticate a port or group of ports by choosing a port or group of ports by using the pull down menus **From** and **To** and clicking **Apply**. The **Reauthenticate Port Table** displays the current status of the reauthenticated port(s) once **Apply** has been clicked.

Click **Configuration > Port Access Entity > PAE System Control > Reauthenticate Port(s)** to open the **Reauthenticate Port** window:

Port	Auth PAE State	Backend State	Port Status
4	ForceAuth	Success	Authorized
5	ForceAuth	Success	Authorized
6	ForceAuth	Success	Authorized
7	ForceAuth	Success	Authorized
8	ForceAuth	Success	Authorized
9	ForceAuth	Success	Authorized
10	ForceAuth	Success	Authorized
11	ForceAuth	Success	Authorized
12	ForceAuth	Success	Authorized

Figure 6- 102. Reauthenticate Port and Reauthenticate Port Table window

This window displays the following information:

Parameter	Description
Unit	Choose the Switch ID number of the line card in the chassis to be modified.
Port	The port number of the reauthenticated port.
MAC Address	Displays the physical address of the Switch where the port resides.
Auth PAE State	The Authenticator State will display one of the following: <i>Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth, and N/A.</i>
BackendState	The Backend State will display one of the following: <i>Request, Response, Success, Fail, Timeout, Idle, Initialize, and N/A.</i>
PortStatus	The status of the controlled port can be <i>Authorized, Unauthorized, or N/A.</i>



NOTE: The user must first globally enable 802.1X in the **Advanced Settings** window in the **Configuration** folder before reauthenticating ports. Information in the **Reauthenticate Ports Table** cannot be viewed before enabling 802.1X.

Reauthenticate Port(s) for MAC-based 802.1x

To reauthenticate ports for the MAC side of 802.1x, the user must first enable 802.1x by MAC address in the **Advanced Settings** window. Click **Configuration > Port Access Entity > PAE System Control > Reauthenticate Port(s)** to open the following window:

Figure 6- 103. Reauthenticate Ports – MAC based 802.1x

To reauthenticate ports, first choose the line card in the chassis by using the **Unit** pull-down menu, then the range of ports in the **From** and **To** field. Then the user must specify the MAC address to be reauthenticated by entering it into the **MAC Address** field and checking the corresponding check box. To begin the reauthentication, click **Apply**.

RADIUS Server

The RADIUS feature of the Switch allows you to facilitate centralized user administration as well as providing protection against a sniffer, active hacker. The Web Manager offers three windows.

Click **Configuration > Port Access Entity > RADIUS Server > Authentic RADIUS Server** to open the **Authentic RADIUS Server Setting** window shown below:

Authentic RADIUS Server					
Succession	First				
RADIUS Server	0.0.0.1				
Authentic Port	1812				
Accounting Port	1813				
Key					
Confirm Key					
Status	Valid				
Apply					
Current RADIUS Server(s) Settings Table					
Succession	RADIUS Server	Auth UDP Port	Acct UDP Port	Status	Key
First					
Second					
Third					

Figure 6- 104. Authentic RADIUS Server and Current RADIUS Server Settings Table window

This window displays the following information:

Parameter	Description
Succession	Choose the desired RADIUS server to configure: <i>First</i> , <i>Second</i> or <i>Third</i> .
RADIUS Server	Set the RADIUS server IP.
Authentic Port	Set the RADIUS authentic server(s) UDP port. The default port is 1812.
Accounting Port	Set the RADIUS account server(s) UDP port. The default port is 1813.
Key	Set the key the same as that of the RADIUS server.
Confirm Key	Confirm the shared key is the same as that of the RADIUS server.
Status	This allows users to set the RADIUS Server as <i>Valid</i> (Enabled) or <i>Invalid</i> (Disabled).

Click **Apply** to implement changes made.

Layer 3 IP Networking

Layer 3 Global Advanced Settings

The **L3 Global Advanced Settings** window allows the user to enable and disable Layer 3 settings and functions from a single window. The full settings and descriptions for these functions will appear later in this section. To view this window, open the **Configuration** folder and then the **Layer 3 IP Networking** folder and click on the **L3 Global Advanced Settings** link to access the following window.

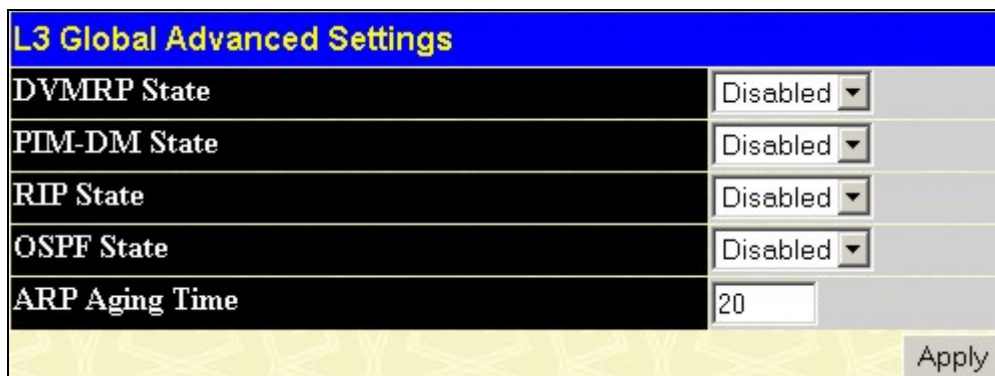


Figure 6- 105. L3 Global Advanced Settings window

The user may set the following:

Parameter	Description
DVMRP State	The user may globally enable or disable the Distance Vector Multicast Routing Protocol (DVMRP) function by using the pull down menu.
PIM State	The user may globally enable or disable the Protocol Independent Multicast (PIM) function by using the pull down menu.
RIP State	The user may globally enable or disable the Routing Information Protocol (RIP) function by using the pull down menu.
OSPF State	The user may globally enable or disable the Open Shortest Path first (OSPF) function by using the pull down menu.
ARP Aging Time	The user may globally set the maximum amount of time, in minutes, that an Address Resolution Protocol (ARP) entry can remain in the Switch's ARP table, without being accessed, before it is dropped from the table. The value may be set in the range of 0-65535 minutes with a default setting of 20 minutes.

IP Multinetting

IP Multinetting is a function that allows multiple IP interfaces to be assigned to the same VLAN. This is beneficial to the administrator when the number of IPs on the original interface is insufficient and the network administrator wishes not to resize the interface. IP Multinetting is capable of assigning another IP interface on the same VLAN without affecting the original stations or settings of the original interface.

Two types of interfaces are configured for IP multinetting, *primary* and *secondary*, and every IP interface must be classified as one of these. A *primary* interface refers to the first interface created on a VLAN, with no exceptions. All other interfaces created will be regarded as *secondary* only, and can only be created once a *primary* interface has been configured. There may be five interfaces per VLAN (one primary, and up to four secondary) and they are, in most cases, independent of each other. *Primary* interfaces cannot be deleted if the VLAN contains a *secondary* interface. Once the user creates multiple interfaces for a specified VLAN (*primary* and *secondary*), that set IP interface cannot be changed to another VLAN.



Application Limitation: A multicast router cannot be connected to IP interfaces that are utilizing the IP Multinetting function.



NOTE: Only the primary IP interface will support the BOOTP relay agent.



NOTE: After IP interfaces are properly configured, VLANs associated with these interfaces can be routed without additional configuration.

IP Multinetting is a valuable tool for network administrators requiring a multitude of IP addresses, but configuring the Switch for IP multinetting may cause troubleshooting and bandwidth problems, and should not be used as a long term solution. Problems may include:

- The Switch may use extra resources to process packets for multiple IP interfaces.
- The amount of broadcast data, such as RIP update packets and PIM hello packets, will be increased.

IP Interface Setup

Each VLAN must be configured prior to setting up the VLAN's corresponding IP interface.

An example is presented below:

VLAN Name	VID	Switch Ports
System (default)	1	5, 6, 7, 8, 21, 22, 23, 24
Engineer	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- 4. VLAN Example - Assigned Ports

In this case, six IP interfaces 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, the above example would give six network addresses and six subnets.

Any IP address from the allowed range of IP addresses for each subnet can be chosen as an IP address for an IP interface on the switch.

For this example, we have chosen the next IP address above the network address for the IP interface's IP Address:

VLAN Name	VID	Network Number	IP Address
System (default)	1	10.32.0.0	10.32.0.1
Engineer	2	10.64.0.0	10.64.0.1
Marketing	3	10.96.0.0	10.96.0.1
Finance	4	10.128.0.0	10.128.0.1
Sales	5	10.160.0.0	10.160.0.1
Backbone	6	10.192.0.0	10.192.0.1

Table 6- 5. VLAN Example - Assigned IP Interfaces

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

changes made.



NOTE: When the IP Interfaces have been configured correctly, each VLAN can be routed without any additional steps.

To setup IP Interfaces on the Switch:

Go to the **Configuration** folder, and click on the **Layer 3 IP Networking** folder, and then click on the **IP Interfaces Table** link to open the following dialog box:

IP Interface Table						
Interface Name	Secondary	IP Address	Subnet Mask	VLAN Name	Active	Delete
System	False	10.53.13.65	255.0.0.0	default	Enabled	X

Total Entries: 1

Figure 6- 106. IP Interface Table

To setup a new IP interface, click the **Add** button. To edit an existing IP Interface entry, click on an entry under the **Interface Name** heading. Both actions will result in the same screen to configure, as shown below.

Figure 6- 107. IP Interface Configuration window

Enter a name for the new interface to be added in the **Interface Name** field (if editing an IP interface, the **Interface Name** will already be in the top field as seen in the window above). Enter the interface’s IP address and subnet mask in the corresponding fields. Pull the **State** pull-down menu to *Enabled* and click **Apply** to enter to make the IP interface effective. To view entries in the **IP Interface Table**, click the [Show All IP Interface Entries](#) hyperlink. Use the **Save Changes** dialog box from the **Maintenance** folder to enter the changes into NV-RAM.

The following fields can be set:

Parameter	Description
Interface Name	This field displays the name for the IP interface. The default IP interface is named “System”. Secondary – Click the check box to set the IP interface as a secondary IP interface. <i>Secondary</i> interfaces can only be configured if a <i>primary</i> interface is first configured.
IP Address	This field allows the entry of an IP address to be assigned to this IP interface.
Subnet Mask	This field allows the entry of a subnet mask to be applied to this IP interface.
VLAN Name	This field allows the entry of the VLAN Name for the VLAN the IP interface belongs to.
State	This field may be altered between <i>Enabled</i> and <i>Disabled</i> using the pull down menu. This entry determines whether the interface will be active or not.
Link Status	This read only field states the current status of the IP Interface on the Switch. <i>Link Up</i> denotes that the IP interface is up and running on the Switch. <i>Link Down</i> will denote that the IP interface is not currently set and/or enabled on the Switch.

Click **Apply** to implement changes made.

MD5 Key Configuration

The **MD5 Key Configuration** menu allows the entry of a sixteen-character Message Digest – version 5 (MD5) key which can be used to authenticate every packet exchanged between OSPF routers. It is used as a security mechanism to limit the exchange of network topology information to the OSPF routing domain.

MD5 Keys created here can be used in the **OSPF** menu below.

To configure an **MD5 Key**, click the **MD5 Key Configuration** link to open the following dialog box:

MD5 Key Configuration		
Key ID	Key	
1		
Add/Modify		
MD5 Key Table		
Key ID	Key	Delete
1	45	✕

Figure 6- 108. MD5 Key Configuration and Table window

The following fields can be set:

Parameter	Description
Key ID	A number from 1 to 255 used to identify the MD5 Key.
Key	An alphanumeric string of between 1 and 16 case-sensitive characters are used to generate the Message Digest which is in turn, used to authenticate OSPF packets within the OSPF routing domain.

Click **Apply** to enter the new Key ID settings. To delete a Key ID entry, click the corresponding ✕ under the **Delete** heading.

Route Redistribution Settings

Route redistribution allows routers on the network, which are running different routing protocols to exchange routing information. This is accomplished by comparing the routes' stored in the various routers routing tables and assigning appropriate metrics. This information is then exchanged among the various routers according to the individual routers' current routing protocol. The Switch can redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. Routing information entered into the **Static Routing Table** on the local xStack® DES-6500 chassis switch is also redistributed.

Routing information source – OSPF and the Static Route table. Routing information will be redistributed to RIP. The following table lists the allowed values for the routing metrics and the types (or forms) of the routing information that will be redistributed.

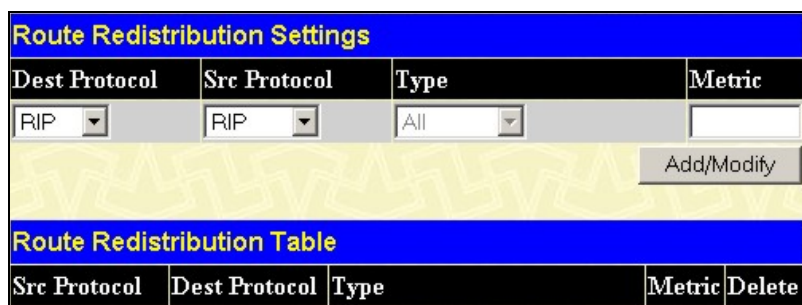
Route Source	Metric	Type
OSPF	0 to 16	All Internal External ExtType1 ExtType2 Inter-E1 Inter-E2
RIP	0 to 16777214	Type 1 Type 2
Static	0 to 16777214	Type 1 Type 2
Local	0 to 16777214	Type 1 Type 2

Table 6- 6. Route Redistribution Source table

Entering the Type combination – Internal, ExtType_1, ExtType_2 is functionally equivalent to All. Entering the combination ExtType_1, ExtType_2 is functionally equivalent to External. Entering the combination Internal, External is functionally equivalent to All.

Entering the metric 0 specifies transparency.

This window will redistribute routing information between the OSPF and RIP routing protocols to all routers on the network that are running OSPF or RIP. To access the **Route Redistribution Settings** window, go to **Configuration > Layer 3 IP Networking > Route Redistribution Settings**:



NOTE: The source protocol (**Src. Protocol**) entry and the destination protocol (**Dst. Protocol**) entry cannot be the same.

Figure 6- 109. Route Redistribution Settings and Table window

The following parameters may be set or viewed:

Parameter	Description
Dst. Protocol	Allows for the selection of the protocol for the destination device. Choose between <i>RIP</i> and <i>OSPF</i> .
Src. Protocol	Allows for the selection of the protocol for the source device. Choose between <i>RIP</i> , <i>OSPF</i> , <i>Static</i> and <i>Local</i> .
Type	Allows for the selection of one of six methods of calculating the metric value. The user may choose between <i>All</i> , <i>Internal</i> , <i>External</i> , <i>ExtType1</i> , <i>ExtType2</i> , <i>Inter-E1</i> , <i>Inter-E2</i> . See the table above for available metric value types for each source protocol.
Metric	Allows the entry of an OSPF interface cost. This is analogous to a Hop Count in the RIP routing protocol. The user may specify a cost between 0 and 16.

Click **Add/Modify** to implement changes made.

Static/Default Route Settings

Entries 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 an IP address into the Switch's **Static IP Routing Table**. To view the following window, click **Configuration > Layer 3 IP Networking > Static/Default Route**.

Static/Default Route Settings						
IP Address	Subnet Mask	Gateway	Hops	Protocol	Backup State	Delete
Total Entries: 0						

Figure 6- 110. Static/Default Route Settings window

This window shows the following values:

Parameter	Description
IP Address	The IP address of the Static/Default Route.
Subnet Mask	The corresponding Subnet Mask of the IP address entered into the table.
Gateway	The corresponding Gateway of the IP address entered into the table.
Hops	Represents the metric value of the IP interface entered into the table. This field may read a number between 1-65535 for an OSPF setting, and 1-16 for a RIP setting.
Protocol	Represents the protocol used for the Routing Table entry of the IP interface. This field may read OSPF, RIP, Static or Local.
Backup State	Represents the Backup state for which this IP interface is configured. This field may read Primary or Backup.
Delete	Click the <input type="checkbox"/> to delete this entry from the Static/Default Route Settings table.

To enter an IP Interface into the Switch's **Static/Default Route Settings** window, click the **Add** button, revealing the following window to configure.

Figure 6- 111. Static/Default Route Settings – Add window

The following fields can be set:

Parameter	Description
Backup State	Allows the user to configure the type of IP route entries on the Switch. <i>Default</i> – Choosing this parameter will allow the user to configure the default gateway for the next hop router only. <i>Static</i> – Choosing this parameter will allow the user to create static destination routes.
IP Address	Allows the entry of an IP address that will be a static entry into the Switch's Routing Table.
Subnet Mask	Allows the entry of a subnet mask corresponding to the IP address above.
Gateway IP	Allows the entry of an IP address of a gateway for the IP address above.
Metric (1-65535)	Allows the entry of a routing protocol metric representing the number of routers between the Switch and the IP address above.
Backup State	The user may choose between <i>Primary</i> and <i>Backup</i> . If the Primary Static/Default Route fails, the Backup Route will support the entry. Please take note that the Primary and Backup entries cannot have the same Gateway.

Click **Apply** to implement changes made.

Static ARP Table

The *Address Resolution Protocol (ARP)* is a TCP/IP protocol that converts IP addresses into physical addresses. This table allows network managers to view, define, modify and delete ARP information for specific devices.

Static entries can be defined in the **ARP Table**. When static entries are defined, a permanent entry is entered and is used to translate IP address to MAC addresses.

To open the **Static ARP Table** open the **Configuration** folder, and then open the **Layer 3 IP Networking** folder and click on the **Static ARP Settings** link.

Static ARP Settings					
Interface Name	IP Address	MAC Address	Type	Modify	Delete
System	10.1.1.2	00-05-5d-19-a5-ab	Static	Modify	X

Total Entries: 1

Figure 6- 112. Static ARP Settings window

To add a new entry, click the **Add** button, revealing the following screen to configure:

Static ARP Table - Add a New Entry

IP Address: 0.0.0.0

MAC Address: 00-00-00-00-00-00

Apply

[Show All Static ARP Entries](#)

Figure 6- 113. Static ARP Settings – Add window

To modify a current entry, click the corresponding **Modify** button of the entry to be modified, revealing the following screen to configure:

Static ARP Table - Modify

IP Address: 10.1.1.2

MAC Address: 00-05-5d-19-a5-ab

Apply

[Show All Static ARP Entries](#)

Figure 6- 114. Static ARP Settings – Edit window

The following fields can be set or viewed:

Parameter	Description
IP Address	The IP address of the ARP entry. This field cannot be edited in the Static ARP Settings – Edit window.
MAC Address	The MAC address of the ARP entry.

After entering the IP Address and MAC Address of the **Static ARP** entry, click **Apply** to implement the new entry. To completely clear the **Static ARP Settings**, click the **Clear All** button.

RIP

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. Both types use the same format.

The Command field specifies an operation according 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

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.

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:

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.

RIP Global Configuration

To setup RIP for the IP interfaces configured on the Switch, the user must first globally enable RIP and then configure RIP settings for the individual IP interfaces. To globally enable RIP on the Switch, open the **Configuration** folder to **Layer 3 Networking** and then open the **RIP** folder and click on the **RIP Global Configuration** link to access the following screen:



Figure 6- 115. RIP Global Settings window

To enable RIP, simply use the pull-down menu, select **Enabled** and click **Apply**.

RIP Settings

RIP settings are configured for each IP interface on the Switch. Click the **RIP Interface Settings** link in the **RIP** folder. The menu appears in table form listing settings for IP interfaces currently on the Switch. To configure RIP settings for an individual interface, click on the hyperlinked **Interface Name**. To view the next page of RIP Interface Settings, click the **Next** button.

RIP Interface Settings					
Interface Name	IP Address	Tx Mode	RX Mode	Auth.	State
System	10.53.13.126	Disabled	Disabled	Disabled	Disabled
					Next

Figure 6- 116. RIP Interface Settings window

Click the hyperlinked name of the interface to set up for RIP, which will give access to the following menu:

RIP Interface Settings-Edit	
Interface Name	System
IP Address	10.53.13.126
Tx Mode	Disabled ▾
RX Mode	Disabled ▾
Authentication	Disabled ▾
Password	<input type="text"/>
State	Disabled ▾
Interface Metric	1
Apply	
Show All RIP Interface Entries	

Figure 6- 117. RIP Interface Settings - Edit window

Refer to the table below for a description of the available parameters for RIP interface settings.

The following RIP settings can be applied to each IP interface:

Parameter	Description
Interface Name	The name of the IP interface on which RIP is to be setup. This interface must be previously configured on the Switch.
IP Address	The IP address corresponding to the Interface Name showing in the field above.
TX Mode	Toggle among <i>Disabled</i> , <i>V1 Only</i> , <i>V1 Compatible</i> , and <i>V2 Only</i> . This entry specifies which version of the RIP protocol will be used to transmit RIP packets. <i>Disabled</i> prevents the transmission of RIP packets.
RX Mode	Toggle among <i>Disabled</i> , <i>V1 Only</i> , <i>V2 Only</i> , and <i>V1 or V2</i> . This entry specifies which version of the RIP protocol will be used to interpret received RIP packets. <i>Disabled</i> prevents the reception of RIP packets.
Authentication	Toggle between <i>Disabled</i> and <i>Enabled</i> to specify that routers on the network should use the Password above to authenticate router table exchanges.
Password	A password to be used to authenticate communication between routers on the network.
State	Toggle between <i>Disabled</i> and <i>Enabled</i> to disable or enable this RIP interface on the switch.
Interface Metric	A read only field that denotes the Metric value of the current IP Interface setting.

Click **Apply** to implement changes made.

OSPF

The Open Shortest Path First (OSPF) routing protocol uses a *link-state* algorithm to determine routes to network destinations. A “link” is an interface on a router and the “state” is a description of that interface and its relationship to neighboring routers. The state contains information such as the IP address, subnet mask, type of network the interface is attached to, other routers attached to the network, etc. The collection of link-states is then collected in a link-state database that is maintained by routers running OSPF.

OSPF specifies how routers will communicate to maintain their link-state database and defines several concepts about the topology of networks that use OSPF.

To limit the extent of link-state update traffic between routers, OSPF defines the concept of *Area*. All routers within an area share the exact same link-state database, and a change to this database on one router triggers an update to the link-state database of all other routers in that area. Routers that have interfaces connected to more than one area are called *Border Routers* and take the responsibility of distributing routing information between areas.

One area is defined as *Area 0* or the *Backbone*. This area is central to the rest of the network in that all other areas have a connection (through a router) to the backbone. Only routers have connections to the backbone and OSPF is structured such that routing information changes in other areas will be introduced into the backbone, and then propagated to the rest of the network.

When constructing a network to use OSPF, it is generally advisable to begin with the backbone (area 0) and work outward

Link-State Algorithm

An OSPF router uses a link-state algorithm to build a shortest path tree to all destinations known to the router. The following is a simplified description of the algorithm’s steps:

- When OSPF is started, or when a change in the routing information changes, the router generates a link-state advertisement. This advertisement is a specially formatted packet that contains information about all the link-states on the router.
- This link-state advertisement is flooded to all router in the area. Each router that receives the link-state advertisement will store the advertisement and then forward a copy to other routers.
- When the link-state database of each router is updated, the individual routers will calculate a Shortest Path Tree to all destinations – with the individual router as the root. The IP routing table will then be made up of the destination address, associated cost, and the address of the next hop to reach each destination.
- Once the link-state databases are updated, Shortest Path Trees calculated, and the IP routing tables written – if there are no subsequent changes in the OSPF network (such as a network link going down) there is very little OSPF traffic.

Shortest Path Algorithm

The Shortest Path to a destination is calculated using the Dijkstra algorithm. Each router is places at the root of a tree and then calculates the shortest path to each destination based on the cumulative cost to reach that destination over multiple possible routes. Each router will then have its own Shortest Path Tree (from the perspective of its location in the network area) even though every router in the area will have and use the exact same link-state database.

The following sections describe the information used to build the Shortest Path Tree.

OSPF Cost

Each OSPF interface has an associated cost (also called “metric”) that is representative of the overhead required to send packets over that interface. This cost is inversely proportional to the bandwidth of the interface (i.e. a higher bandwidth interface has a lower cost). There is then a higher cost (and longer time delays) in sending packets over a 56 Kbps dial-up connection than over a 10 Mbps Ethernet connection. The formula used to calculate the OSPF cost is as follows:

Cost = 100,000,000 / bandwidth in bps

As an example, the cost of a 10 Mbps Ethernet line will be 10 and the cost to cross a 1.544 Mbps T1 line will be 64.

Shortest Path Tree

To build Router A’s shortest path tree for the network diagramed below, Router A is put at the root of the tree and the smallest cost link to each destination network is calculated.

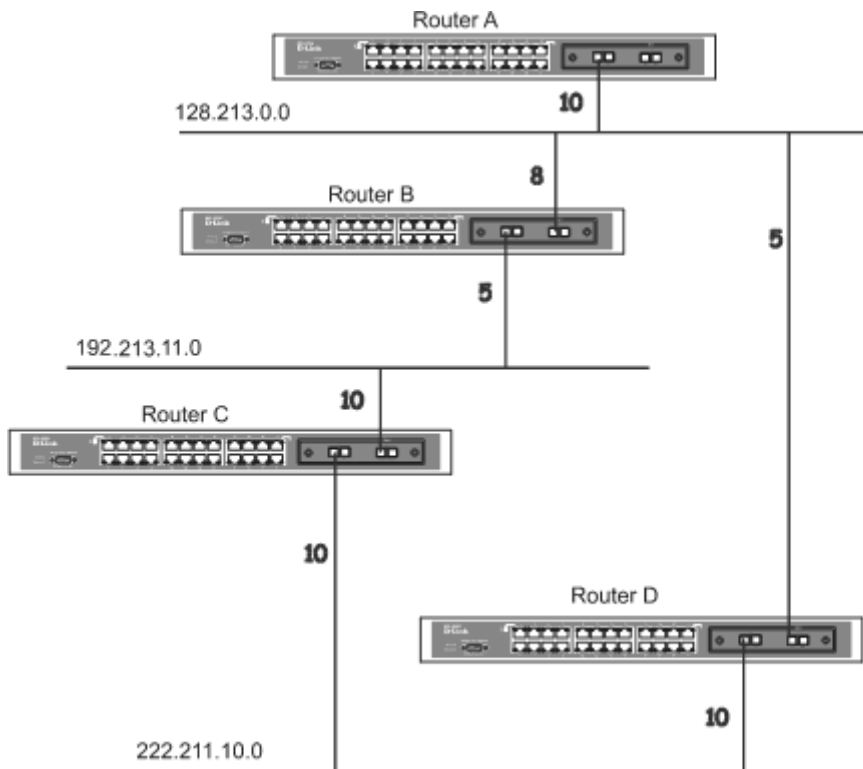


Figure 6- 118. Constructing a Shortest Path Tree

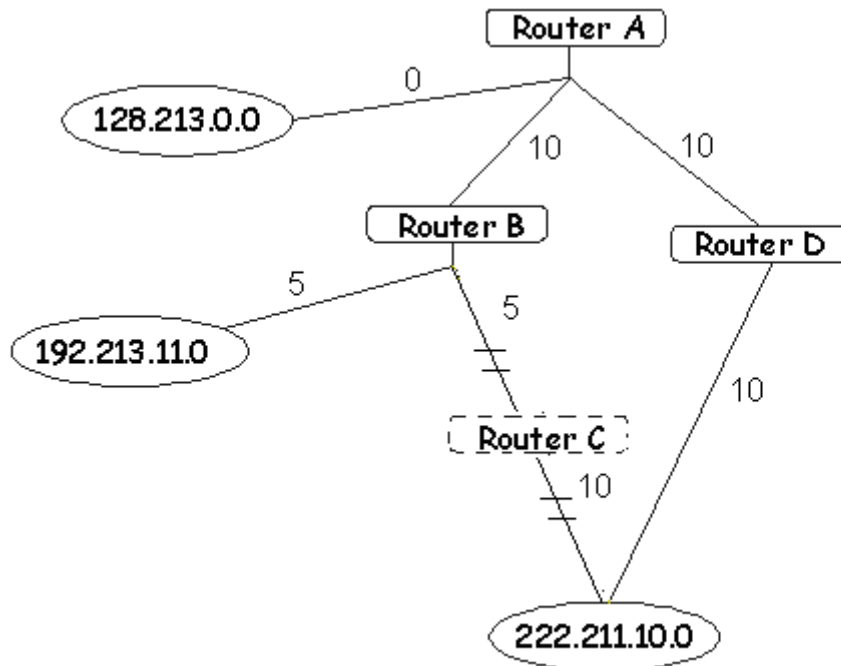


Figure 6- 119. Constructing a Shortest Path Tree

The diagram above shows the network from the viewpoint of Router A. Router A can reach 192.213.11.0 through Router B with a cost of $10 + 5 = 15$. Router A can reach 222.211.10.0 through Router C with a cost of $10 + 10 = 20$. Router A can also reach 222.211.10.0 through Router B and Router D with a cost of $10 + 5 + 10 = 25$, but the cost is higher than the route through Router C. This higher-cost route will not be included in the Router A's shortest path tree. The resulting tree will look like this:

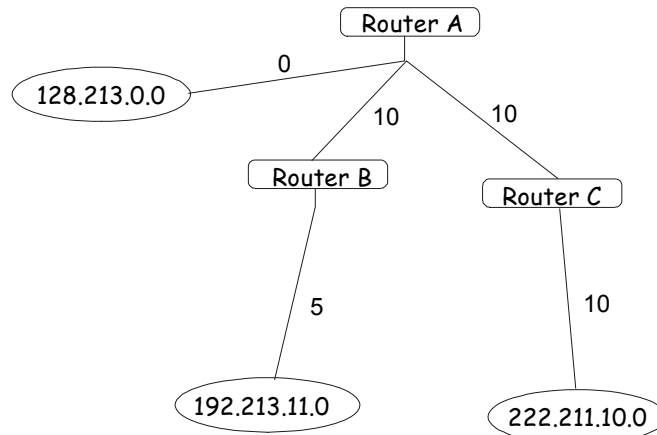


Figure 6- 120. Constructing a Shortest Path Tree - Completed

Note that this shortest path tree is only from the viewpoint of Router A. The cost of the link from Router B to Router A, for instance is not important to constructing Router A's shortest path tree, but is very important when Router B is constructing its shortest path tree.

Note also that directly connected networks are reached at a cost of zero, while other networks are reached at the cost calculated in the shortest path tree.

Router A can now build its routing table using the network addresses and costs calculated in building the above shortest path tree.

Areas and Border Routers

OSPF link-state updates are forwarded to other routers by flooding to all routers on the network. OSPF uses the concept of areas to define where on the network routers that need to receive particular link-state updates are located. This helps ensure that routing updates are not flooded throughout the entire network and to reduce the amount of bandwidth consumed by updating the various router's routing tables.

Areas establish boundaries beyond which link-state updates do not need to be flooded. So the exchange of link-state updates and the calculation of the shortest path tree are limited to the area that the router is connected to.

Routers that have connections to more than one area are called Border Routers (BR). The Border Routers have the responsibility of distributing necessary routing information and changes between areas.

Areas are specific to the router interface. A router that has all of its interfaces in the same area is called an Internal Router. A router that has interfaces in multiple areas is called a Border Router. Routers that act as gateways to other networks (possibly using other routing protocols) are called Autonomous System Border Routers (ASBRs).

Link-State Packets

There are a number of different types of link-state packets, four of which are illustrated below:

- Router Link-State Updates – These describe a router's links to destinations within an area.
- Summary Link-State Updates – Issued by Border Routers and describe links to networks outside the area but within the Autonomous System (AS).
- Network Link-State Updates – Issued by multi-access areas that have more than one attached router. One router is elected as the Designated Router (DR) and this router issues the network link-state updates describing every router on the segment.
- External Link-State Updates – Issued by an Autonomous System Border Router and describes routes to destinations outside the AS or a default route to the outside AS.

The format of these link-state updates is described in more detail below.

Router link-state updates are flooded to all routers in the current area. These updates describe the destinations reachable through all of the router's interfaces.

Summary link-state updates are generated by Border Routers to distribute routing information about other networks within the AS. Normally, all Summary link-state updates are forwarded to the backbone (area 0) and are then forwarded to all other areas in the network. Border Routers also have the responsibility of distributing routing information from the Autonomous System Border Router in order for routers in the network to get and maintain routes to other Autonomous Systems.

Network link-state updates are generated by a router elected as the Designated Router on a multi-access segment (with more than one attached router). These updates describe all of the routers on the segment and their network connections.

External link-state updates carry routing information to networks outside the Autonomous System. The Autonomous System Border Router is responsible for generating and distributing these updates.

OSPF Authentication

OSPF packets can be authenticated as coming from trusted routers by the use of predefined passwords. The default for routers is to use not authentication.

There are two other authentication methods – simple password authentication (key) and Message Digest authentication (MD-5).

Message Digest Authentication (MD-5)

MD-5 authentication is a cryptographic method. A key and a key-ID are configured on each router. The router then uses an algorithm to generate a mathematical “message digest” that is derived from the OSPF packet, the key and the key-ID. This message digest (a number) is then appended to the packet. The key is not exchanged over the wire and a non-decreasing sequence number is included to prevent replay attacks.

Simple Password Authentication

A password (or key) can be configured on a per-area basis. Routers in the same area that participate in the routing domain must be configured with the same key. This method is possibly vulnerable to passive attacks where a link analyzer is used to obtain the password.

Backbone and Area 0

OSPF limits the number of link-state updates required between routers by defining areas within which a given router operates. When more than one area is configured, one area is designated as area 0 – also called the backbone.

The backbone is at the center of all other areas – all areas of the network have a physical (or virtual) connection to the backbone through a router. OSPF allows routing information to be distributed by forwarding it into area 0, from which the information can be forwarded to all other areas (and all other routers) on the network.

In situations where an area is required, but is not possible to provide a physical connection to the backbone, a virtual link can be configured.

Virtual Links

Virtual links accomplish two purposes:

- Linking an area that does not have a physical connection to the backbone.
- Patching the backbone in case there is a discontinuity in area 0.

Areas Not Physically Connected to Area 0

All areas of an OSPF network should have a physical connection to the backbone, but in some cases it is not possible to physically connect a remote area to the backbone. In these cases, a virtual link is configured to connect the remote area to the backbone. A virtual path is a logical path between two border routers that have a common area, with one border router connected to the backbone.

Partitioning the Backbone

OSPF also allows virtual links to be configured to connect the parts of the backbone that are discontinuous. This is the equivalent to linking different area 0s together using a logical path between each area 0. Virtual links can also be added for redundancy to protect against a router failure. A virtual link is configured between two border routers that both have a connection to their respective area 0s.

Neighbors

Routers that are connected to the same area or segment become neighbors in that area. Neighbors are elected via the Hello protocol. IP multicast is used to send out Hello packets to other routers on the segment. Routers become neighbors when they see themselves listed in a Hello packet sent by another router on the same segment. In this way, two-way communication is guaranteed to be possible between any two neighbor routers.

Any two routers must meet the following conditions before the become neighbors:

- **Area ID** – Two routers having a common segment – their interfaces have to belong to the same area on that segment. Of course, the interfaces should belong to the same subnet and have the same subnet mask.

- **Authentication** – OSPF allows for the configuration of a password for a specific area. Two routers on the same segment and belonging to the same area must also have the same OSPF password before they can become neighbors.
- **Hello and Dead Intervals** – The Hello interval specifies the length of time, in seconds, between the hello packets that a router sends on an OSPF interface. The dead interval is the number of seconds that a router's Hello packets have not been seen before its neighbors declare the OSPF router down. OSPF routers exchange Hello packets on each segment in order to acknowledge each other's existence on a segment and to elect a Designated Router on multi-access segments. OSPF requires these intervals to be exactly the same between any two neighbors. If any of these intervals are different, these routers will not become neighbors on a particular segment.
- **Stub Area Flag** – Any two routers also have to have the same stub area flag in their Hello packets in order to become neighbors.

Adjacencies

Adjacent routers go beyond the simple Hello exchange and participate in the link-state database exchange process. OSPF elects one router as the Designated Router (DR) and a second router as the Backup Designated Router (BDR) on each multi-access segment (the BDR is a backup in case of a DR failure). All other routers on the segment will then contact the DR for link-state database updates and exchanges. This limits the bandwidth required for link-state database updates.

Designated Router Election

The election of the DR and BDR is accomplished using the Hello protocol. The router with the highest OSPF priority on a given multi-access segment will become the DR for that segment. In case of a tie, the router with the highest Router ID wins. The default OSPF priority is 1. A priority of zero indicates a router that cannot be elected as the DR.

Building Adjacency

Two routers undergo a multi-step process in building the adjacency relationship. The following is a simplified description of the steps required:

- **Down** – No information has been received from any router on the segment.
- **Attempt** – On non-broadcast multi-access networks (such as Frame Relay or X.25), this state indicates that no recent information has been received from the neighbor. An effort should be made to contact the neighbor by sending Hello packets at the reduced rate set by the Poll Interval.
- **Init** – The interface has detected a Hello packet coming from a neighbor but bi-directional communication has not yet been established.
- **Two-way** – Bi-directional communication with a neighbor has been established. The router has seen its address in the Hello packets coming from a neighbor. At the end of this stage the DR and BDR election would have been done. At the end of the Two-way stage, routers will decide whether to proceed in building an adjacency or not. The decision is based on whether one of the routers is a DR or a BDR or the link is a point-to-point or virtual link.
- **Exstart** – (Exchange Start) Routers establish the initial sequence number that is going to be used in the information exchange packets. The sequence number insures that routers always get the most recent information. One router will become the primary and the other will become secondary. The primary router will poll the secondary for information.
- **Exchange** – Routers will describe their entire link-state database by sending database description packets.
- **Loading** – The routers are finalizing the information exchange. Routers have link-state request list and a link-state retransmission list. Any information that looks incomplete or outdated will be put on the request list. Any update that is sent will be put on the retransmission list until it gets acknowledged.
- **Full** – The adjacency is now complete. The neighboring routers are fully adjacent. Adjacent routers will have the same link-state database.

Adjacencies on Point-to-Point Interfaces

OSPF Routers that are linked using point-to-point interfaces (such as serial links) will always form adjacencies. The concepts of DR and BDR are unnecessary.

OSPF Packet Formats

All OSPF packet types begin with a standard 24-byte header and there are five packet types. The header is described first, and each packet type is described in a subsequent section.

All OSPF packets (except for Hello packets) forward link-state advertisements. Link-State Update packets, for example, flood advertisements throughout the OSPF routing domain.

- OSPF packet header
- Hello packet
- Database Description packet

- Link-State Request packet
- Link-State Update packet
- Link-State Acknowledgment packet

OSPF Packet Header

Every OSPF packet is preceded by a common 24-byte header. This header contains the information necessary for a receiving router to determine if the packet should be accepted for further processing.

The format of the OSPF packet header is shown below:

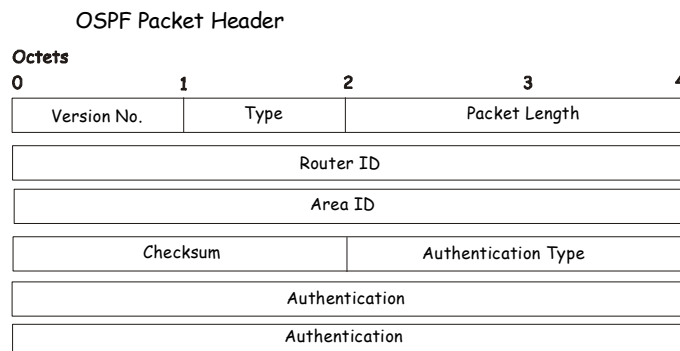


Figure 6- 121. OSPF Packet Header Format

Field	Description
Version No.	The OSPF version number
Type	The OSPF packet type. The OSPF packet types are as follows: Type Description Hello Database Description Link-State Request Link-State Update Link-State Acknowledgment
Packet Length	The length of the packet in bytes. This length includes the 24-byte header.
Router ID	The Router ID of the packet's source.
Area ID	A 32-bit number identifying the area that this packet belongs to. All OSPF packets are associated with a single area. Packets traversing a virtual link are assigned the backbone Area ID of 0.0.0.0
Checksum	A standard IP checksum that includes all of the packet's contents except for the 64-bit authentication field.
Authentication Type	The type of authentication to be used for the packet.
Authentication	A 64-bit field used by the authentication scheme.

Hello Packet

Hello packets are OSPF packet type 1. They are sent periodically on all interfaces, including virtual links, in order to establish and maintain neighbor relationships. In addition, Hello Packets are multicast on those physical networks having a multicast or broadcast capability, enabling dynamic discovery of neighboring routers.

All routers connected to a common network must agree on certain parameters such as the Network Mask, the Hello Interval, and the Router Dead Interval. These parameters are included in the hello packets, so that differences can inhibit the forming of neighbor relationships. A detailed explanation of the receive process for Hello packets is necessary so that differences can inhibit the forming of neighbor relationships.

The format of the Hello packet is shown below:

Hello Packet

Octets	0	1	2	3	4
Version No.	1	Packet Length			
Router ID					
Area ID					
Checksum	Authentication Type				
Authentication					
Authentication					
Network Mask					
Hello Interval	Options		Router Priority		
Router Dead Interval					
Designated Router					
Backup Designated Router					
Neighbor					

Figure 6- 122. Hello Packet

Field	Description
Network Mask	The network mask associated with this interface.
Options	The optional capabilities supported by the router.
Hello Interval	The number of seconds between this router's Hello packets.
Router Priority	This router's Router Priority. The Router Priority is used in the election of the DR and BDR. If this field is set to 0, the router is ineligible to become the DR or the BDR.
Router Dead Interval	The number of seconds that must pass before declaring a silent router as down.
Designated Router	The identity of the DR for this network, in the view of the advertising router. The DR is identified here by its IP interface address on the network.
Backup Designated Router	The identity of the Backup Designated Router (BDR) for this network. The BDR is identified here by its IP interface address on the network. This field is set to 0.0.0.0 if there is no BDR.
Field	Description
Neighbor	The Router IDs of each router from whom valid Hello packets have been seen within the Router Dead Interval on the network.

Database Description Packet

Database Description packets are OSPF packet type 2. These packets are exchanged when an adjacency is being initialized. They describe the contents of the topological database. Multiple packets may be used to describe the database. For this purpose, a poll-response procedure is used. One of the routers is designated to be master, the other a slave. The master sends Database Description packets (polls) that are acknowledged by Database Description packets sent by the slave (responses). The responses are linked to the polls via the packets' DD sequence numbers.

Database Description Packet

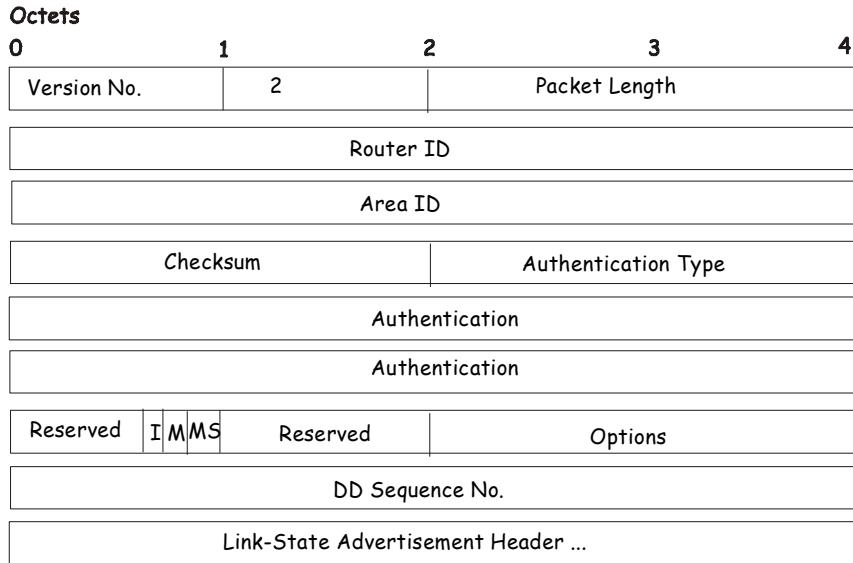


Figure 6- 123. Database Description Packet

Field	Description
Options	The optional capabilities supported by the router.
I - bit	The Initial bit. When set to 1, this packet is the first in the sequence of Database Description packets.
M - bit	The More bit. When set to 1, this indicates that more Database Description packets will follow.
MS - bit	The Master Slave bit. When set to 1, this indicates that the router is the master during the Database Exchange process. A zero indicates the opposite.
DD Sequence Number	User to sequence the collection of Database Description Packets. The initial value (indicated by the Initial bit being set) should be unique. The DD sequence number then increments until the complete database description has been sent.

The rest of the packet consists of a list of the topological database's pieces. Each link state advertisement in the database is described by its link state advertisement header.

Link-State Request Packet

Link-State Request packets are OSPF packet type 3. After exchanging Database Description packets with a neighboring router, a router may find that parts of its topological database are out of date. The Link-State Request packet is used to request the pieces of the neighbor's database that are more up to date. Multiple Link-State Request packets may need to be used. The sending of Link-State Request packets is the last step in bringing up an adjacency.

A router that sends a Link-State Request packet has in mind the precise instance of the database pieces it is requesting, defined by LS sequence number, LS checksum, and LS age, although these fields are not specified in the Link-State Request packet itself. The router may receive even more recent instances in response.

The format of the Link-State Request packet is shown below:

Link-State Request Packet

Octets	
0	4
Version No.	Packet Length
Router ID	
Area ID	
Checksum	Authentication Type
Authentication	
Authentication	
Link-State Type	
Link-State ID	
Advertising Router	

Figure 6- 124. Link-State Request Packet

Each advertisement requested is specified by its Link-State Type, Link-State ID, and Advertising Router. This uniquely identifies the advertisement, but not its instance. Link-State Request packets are understood to be requests for the most recent instance.

Link-State Update Packet

Link-State Update packets are OSPF packet type 4. These packets implement the flooding of link-state advertisements. Each Link-State Update packet carries a collection of link-state advertisements one hop further from its origin. Several link-state advertisements may be included in a single packet.

Link-State Update packets are multicast on those physical networks that support multicast/broadcast. In order to make the flooding procedure reliable, flooded advertisements are acknowledged in Link-State Acknowledgment packets. If retransmission of certain advertisements is necessary, the retransmitted advertisements are always carried by unicast Link-State Update packets.

The format of the Link-State Update packet is shown below:

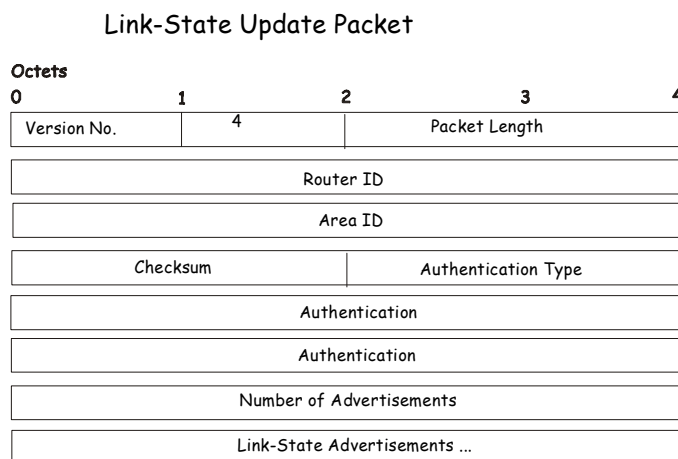


Figure 6- 125. Link-State Update Packet

The body of the Link-State Update packet consists of a list of link-state advertisements. Each advertisement begins with a common 20-byte header, the link-state advertisement header. Otherwise, the format of each of the five types of link-state advertisements is different.

Link-State Acknowledgment Packet

Link-State Acknowledgment packets are OSPF packet type 5. To make the folding of link-state advertisements reliable, flooded advertisements are explicitly acknowledged. This acknowledgment is accomplished through the sending and receiving of Link-State Acknowledgment packets. Multiple link-state advertisements can be acknowledged in a single Link-State Acknowledgment packet.

Depending on the state of the sending interface and the source of the advertisements being acknowledged, a Link-State Acknowledgment packet is sent either to the multicast address AllSPFRouters, to the multicast address AllDRouters, or as a unicast packet.

The format of this packet is similar to that of the Data Description packet. The body of both packets is simply a list of link-state advertisement headers.

The format of the Link-State Acknowledgment packet is shown below:

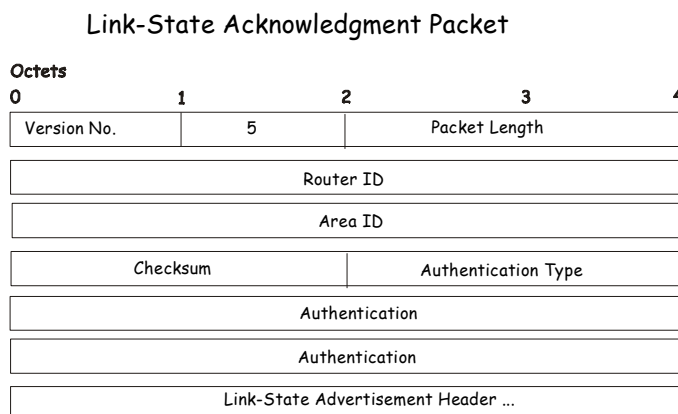


Figure 6- 126. Link State Acknowledge Packet

Each acknowledged link-state advertisement is described by its link-state advertisement header. It contains all the information required to uniquely identify both the advertisement and the advertisement's current instance.

Link-State Advertisement Formats

There are five distinct types of link-state advertisements. Each link-state advertisement begins with a standard 20-byte link-state advertisement header. Succeeding sections then diagram the separate link-state advertisement types.

Each link-state advertisement describes a piece of the OSPF routing domain. Every router originates a router links advertisement. In addition, whenever the router is elected as the Designated Router, it originates a network links advertisement. Other types of link-state advertisements may also be originated. The flooding algorithm is reliable, ensuring that all routers have the same collection of link-state advertisements. The collection of advertisements is called the link-state (or topological) database.

From the link-state database, each router constructs a shortest path tree with itself as root. This yields a routing table.

There are four types of link state advertisements, each using a common link state header. These are:

- Router Links Advertisements
- Network Links Advertisements
- Summary Link Advertisements
- Autonomous System Link Advertisements

Link State Advertisement Header

All link state advertisements begin with a common 20-byte header. This header contains enough information to uniquely identify the advertisements (Link State Type, Link State ID, and Advertising Router). Multiple instances of the link state advertisement may exist in the routing domain at the same time. It is then necessary to determine which instance is more recent. This is accomplished by examining the link state age, link state sequence number and link state checksum fields that are also contained in the link state advertisement header.

The format of the Link State Advertisement Header is shown below:

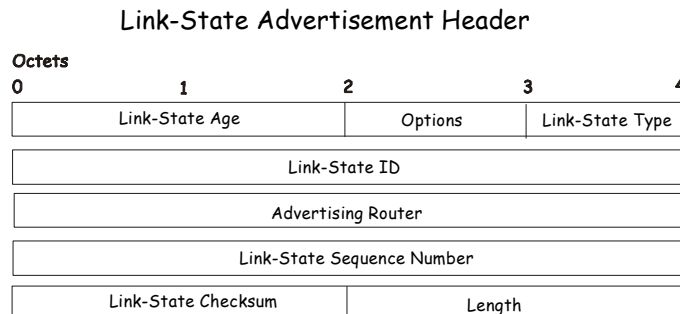


Figure 6- 127. Link State Advertisement Header

Field	Description
Link State Age	The time in seconds since the link state advertisement was originated.
Options	The optional capabilities supported by the described portion of the routing domain.
Link State Type	The type of the link state advertisement. Each link state type has a separate advertisement format. The link state types are as follows: Router Links, Network Links, Summary Link (IP Network), Summary Link (ASBR), AS External Link.
Link State ID	This field identifies the portion of the internet environment that is being described by the advertisement. The contents of this field depend on the advertisement's Link State Type.
Advertising Router	The Router ID of the router that originated the Link State Advertisement. For example, in network links advertisements this field is set to the Router ID of the network's Designated Router.
Link State Sequence Number	Detects old or duplicate link state advertisements. Successive instances of a link state advertisement are given successive Link State Sequence numbers.
Link State Checksum	The Fletcher checksum of the complete contents of the link state advertisement, including the link state advertisement header by accepting the Link State Age field.
Length	The length in bytes of the link state advertisement. This includes the 20-byte link state advertisement header.

Router Links Advertisements

Router links advertisements are type 1 link state advertisements. Each router in an area originates a routers links advertisement. The advertisement describes the state and cost of the router’s links to the area. All of the router’s links to the area must be described in a single router links advertisement.

The format of the Router Links Advertisement is shown below:

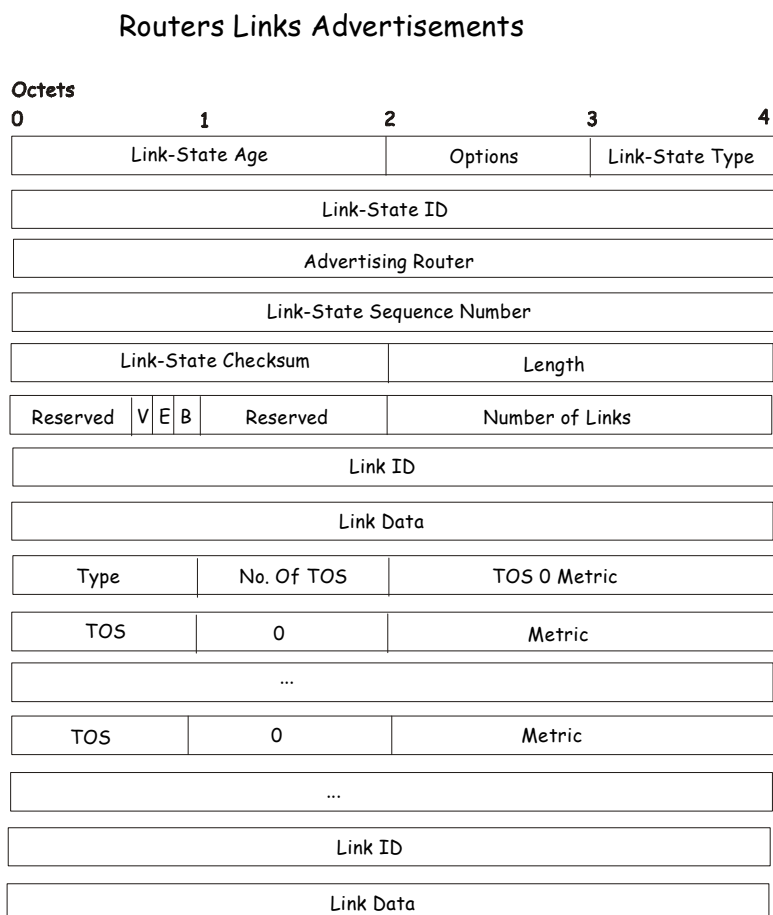


Figure 6- 128. Routers Links Advertisements

In router links advertisements, the Link State ID field is set to the router’s OSPF Router ID. The T - bit is set in the advertisement’s Option field if and only if the router is able to calculate a separate set of routes for each IP Type of Service (TOS). Router links advertisements are flooded throughout a single area only.

Field	Description
V - bit	When set, the router is an endpoint of an active virtual link that is using the described area as a Transit area (V is for Virtual link endpoint).
E - bit	When set, the router is an Autonomous System (AS) boundary router (E is for External).
B - bit	When set, the router is an area border router (B is for Border).
Number of Links	The number of router links described by this advertisement. This must be the total collection of router links to the area.

The following fields are used to describe each router link. Each router link is typed. The Type field indicates the kind of link being described. It may be a link to a transit network, to another router or to a stub network. The values of all the other fields describing a router link depend on the link’s Type. For example, each link has an associated 32-bit data field. For links to stub networks, this field specifies the network’s IP address mask. For other link types, the Link Data specifies the router’s associated IP interface address.

Field	Description
Type	A quick classification of the router link. One of the following: Type Description Point-to-point connection to another router. Connection to a transit network. Connection to a stub network. Virtual link.
Link ID	Identifies the object that this router link connects to. Value depends on the link's Type. When connecting to an object that also originates a link state advertisement (i.e. another router or a transit network) the Link ID is equal to the neighboring advertisement's Link State ID. This provides the key for looking up an advertisement in the link state database. Type Link ID Neighboring router's Router ID. IP address of Designated Router. IP network/subnet number. Neighboring router's Router ID
Link Data	Contents again depend on the link's Type field. For connections to stub networks, it specifies the network's IP address mask. For unnumbered point-to-point connection, it specifies the interface's MIB-II ifIndex value. For other link types it specifies the router's associated IP interface address. This latter piece of information is needed during the routing table build process, when calculating the IP address of the next hop.
No. of TOS	The number of different Type of Service (TOS) metrics given for this link, not counting the required metric for TOS 0. If no additional TOS metrics are given, this field should be set to 0.
TOS 0 Metric	The cost of using this router link for TOS 0.

For each link, separate metrics may be specified for each Type of Service (TOS). The metric for TOS 0 must always be included, and was discussed above. Metrics for non-zero TOS are described below. Note that the cost for non-zero TOS values that are not specified defaults to the TOS 0 cost. Metrics must be listed in order of increasing TOS encoding. For example, the metric for TOS 16 must always follow the metric for TOS 8 when both are specified.

Field	Description
TOS	IP Type of Service that this metric refers to.
Metric	The cost of using this outbound router link, for traffic of the specified TOS.

Network Links Advertisements

Network links advertisements are Type 2 link state advertisements. A network links advertisement is originated for each transit network in the area. A transit network is a multi-access network that has more than one attached router. The network links advertisement is originated by the network's Designated router. The advertisement describes all routers attached to the network, including the Designated Router itself. The advertisement's Link State ID field lists the IP interface address of the Designated Router.

The distance from the network to all attached routers is zero, for all TOS. This is why the TOS and metric fields need not be specified in the network links advertisement.

The format of the Network Links Advertisement is shown below:

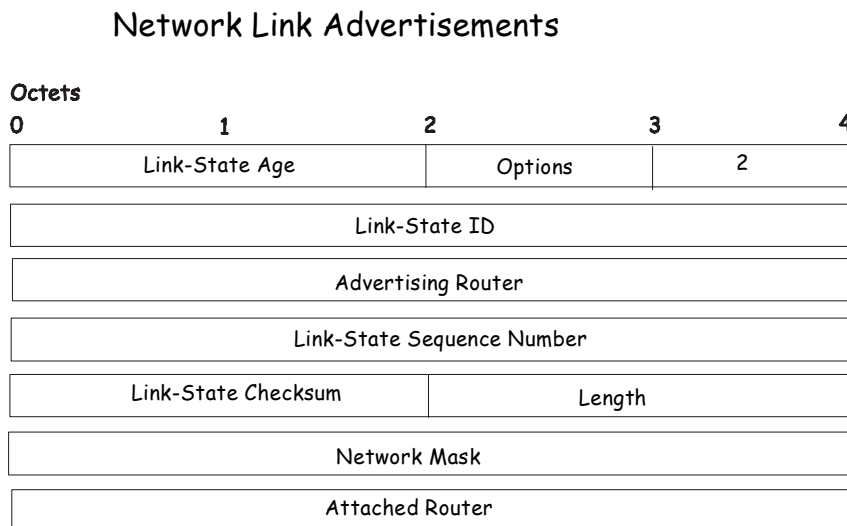


Figure 6- 129. Network Link Advertisements

Field	Description
Network Mask	The IP address mask for the network.
Attached Router	The Router Ids of each of the routers attached to the network. Only those routers that are fully adjacent to the Designated Router (DR) are listed. The DR includes itself in this list.

Summary Link Advertisements

Summary link advertisements are Type 3 and 4 link state advertisements. These advertisements are originated by Area Border routers. A separate summary link advertisement is made for each destination known to the router, that belongs to the Autonomous System (AS), yet is outside the area.

Type 3 link state advertisements are used when the destination is an IP network. In this case, the advertisement's Link State ID field is an IP network number. When the destination is an AS boundary router, a Type 4 advertisement is used, and the Link State ID field is the AS boundary router's OSPF Router ID. Other than the difference in the Link State ID field, the format of Type 3 and 4 link state advertisements is identical.

Summary Link Advertisements

Octets	
0	1
Link-State Age	Options
Link-State ID	
Advertising Router	
Link-State Sequence Number	
Link-State Checksum	Length
Network Mask	
TOS	Metric

Figure 6- 130. Summary Link Advertisements

For stub area, Type 3 summary link advertisements can also be used to describe a default route on a per-area basis. Default summary routes are used in stub area instead of flooding a complete set of external routes. When describing a default summary route, the advertisement's Link State ID is always set to the Default Destination – 0.0.0.0, and the Network Mask is set to 0.0.0.0.

Separate costs may be advertised for each IP Type of Service. Note that the cost for TOS 0 must be included, and is always listed first. If the T-bit is reset in the advertisement's Option field, only a route for TOS 0 is described by the advertisement. Otherwise, routes for the other TOS values are also described. If a cost for a certain TOS is not included, its cost defaults to that specified for TOS 0.

Field	Description
Network Mask	For Type 3 link state advertisements, this indicates the destination network's IP address mask. For example, when advertising the location of a class A network the value 0xff000000
TOS	The Type of Service that the following cost is relevant to.
Metric	The cost of this route. Expressed in the same units as the interface costs in the router links advertisements.

Autonomous Systems External Link Advertisements

Autonomous Systems (AS) link advertisements are Type 5 link state advertisements. These advertisements are originated by AS boundary routers. A separate advertisement is made for each destination known to the router that is external to the AS.

AS external link advertisements usually describe a particular external destination. For these advertisements the Link State ID field specifies an IP network number. AS external link advertisements are also used to describe a default route. Default routes are used when no specific route exists to the destination. When describing a default route, the Link Stat ID is always set the Default Destination address (0.0.0.0) and the Network Mask is set to 0.0.0.0.

The format of the AS External Link Advertisement is shown below:

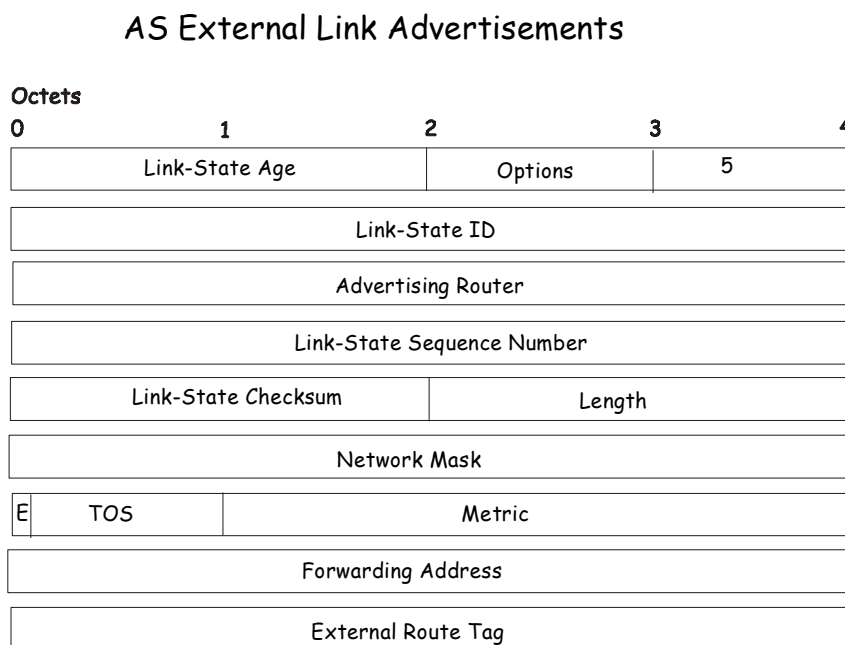


Figure 6- 131. AS External Link Advertisements

Field	Description
Network Mask	The IP address mask for the advertised destination.
E - bit	The type of external metric. If the E - bit is set, the metric specified is a Type 2 external metric. This means the metric is considered larger than any link state path. If the E - bit is zero, the specified metric is a Type 1 external metric. This means that is comparable directly to the link state metric.
Forwarding Address	Data traffic for the advertised destination will be forwarded to this address. If the Forwarding Address is set to 0.0.0.0, data traffic will be forwarded instead to the advertisement's originator.
TOS	The Type of Service that the following cost is relevant to.
Metric	The cost of this route. The interpretation of this metric depends on the external type indication (the E - bit above).
External Route Tag	A 32-bit field attached to each external route. This is not used by the OSPF protocol itself.

OSPF General Settings

The **OSPF General Settings** menu allows OSPF to be enabled or disabled on the Switch – without changing the Switch’s OSPF configuration.

To view the following window, click **Configuration > Layer 3 IP Networking > OSPF > General**. To enable OSPF, first supply an **OSPF Route ID** (see below), select *Enabled* from the **State** drop-down menu and click the **Apply** button.

Figure 6- 132. OSPF General Settings window

The following parameters are used for general OSPF configuration:

Parameter	Description
OSPF Route ID	A 32-bit number (in the same format as an IP address – xxx.xxx.xxx.xxx) that uniquely identifies the Switch in the OSPF domain. It is common to assign the highest IP address assigned to the Switch (router). In this case, it would be 10.53.13.189, but any unique 32-bit number will do. If 0.0.0.0 is entered, the highest IP address assigned to the Switch will become the OSPF Route ID.
Current Route ID	Displays the OSPF Route ID currently in use by the Switch. This Route ID is displayed as a convenience to the user when changing the Switch’s OSPF Route ID.
State	Allows OSPF to be enabled or disabled globally on the Switch without changing the OSPF configuration.

OSPF Area ID Settings

This menu allows the configuration of OSPF Area IDs and to designate these areas as either **Normal** or **Stub**. Normal OSPF areas allow Link-State Database (LSDB) advertisements of routes to networks that are external to the area. Stub areas do not allow the LSDB advertisement of external routes. Stub areas use a default summary external route (0.0.0.0 or Area 0) to reach external destinations.

To set up an OSPF area configuration click **Configuration > Layer 3 IP Networking > OSPF > OSPF Area ID Settings** link to open the following dialog box:

Figure 6- 133. OSPF Area Settings and Table window

To add an OSPF Area to the table, type a unique **Area ID** (see below) select the **Type** from the drop-down menu. For a Stub type, choose *Enabled* or *Disabled* from the **Stub Import Summary LSA** drop-down menu and determine the **Stub Default Cost**. Click the **Add/Modify** button to add the area ID set to the table. To remove an Area ID configuration set, simply click **X** in the **Delete** column for the configuration.

To change an existing set in the list, type the **Area ID** of the set you want to change, make the changes and click the **Add/Modify** button. The modified OSPF area ID will appear in the table.

OSPF Area ID Settings				
Area ID	Type	Stub Import Summary LSA	Stub Default Cost	
0.0.0.0	Stub	Disabled	1	
				Add/Modify
OSPF Area ID Table				
Area ID	Type	Stub Import Summary LSA	Stub Default Cost	Delete
0.0.0.0	Normal	None	None	✕
10.53.13.94	Stub	Disabled	1	✕

Figure 6- 134. OSPF Area Settings example window

See the parameter descriptions below for information on the OSPF Area ID Settings.

The Area ID settings are as follows:

Parameter	Description
Area ID	A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.
Type	This field can be toggled between <i>Normal</i> and <i>Stub</i> using the space bar. When it is toggled to <i>Stub</i> , additional fields appear – Stub Import Summary LSA , and the Stub Default Cost .
Stub Import Summary LSA	Displays whether or not the selected Area will allow Summary Link-State Advertisements (Summary LSAs) to be imported into the area from other areas.
Stub Default Cost	Displays the default cost for the route to the stub of between 0 and 65,535. The default is 1.

OSPF Interface Settings

To set up OSPF interfaces, click **Configuration > Layer 3 IP Networking > OSPF > OSPF Interface Settings** to view OSPF settings for existing IP interfaces. If there are no IP interfaces configured (besides the default System interface), only the System interface settings will appear listed. To change settings for in IP interface, click on the hyperlinked name of the interface to see the configuration menu for that interface.

OSPF Interface Settings					
Interface Name	IP Address	Area ID	Auth. Type	State	Metric
System	10.53.13.121	0.0.0.0	None	Disabled	1
Trinity	12.1.1.1	0.0.0.0	None	Disabled	1

Figure 6- 135. OSPF Interface Settings window

OSPF Interface Settings - Edit	
Interface Name	System
IP Address	10.53.13.144(Link Up)
Network Medium Type	BROADCAST
Area ID	<input type="text" value="0.0.0.0"/>
Router Priority	<input type="text" value="1"/>
Hello Interval	<input type="text" value="10"/>
Dead Interval	<input type="text" value="40"/>
State	Disabled ▾
Auth. Type	None ▾
Auth. Key ID	<input type="text"/>
Metric	<input type="text" value="1"/>
DR State	DOWN
DR Address	0.0.0.0
Backup DR Address	0.0.0.0
Transmit Delay	1
Retransmit Time	5
<input type="button" value="Apply"/>	
Show All OSPF Interface Entries	

Figure 6- 136. OSPF Interface Settings - Edit window

Configure each IP interface individually using the **OSPF Interface Settings - Edit** menu. Click the **Apply** button when settings have been entered. The new configuration appears listed in the **OSPF Interface Settings** table. To return to the **OSPF Interface Settings** table, click the [Show All OSPF Interface Entries](#) link.

OSPF interface settings are described below. Some OSPF interface settings require previously configured OSPF settings. Read the descriptions below for details.

Parameter	Description
Interface Name	Displays the of an IP interface previously configured on the Switch.
IP Address	Displays the IP address of the interface and its current status (Link Up / Link Down)
Network Medium Type	A read only field describing the type of network medium in use. This field will only read Broadcast due to OSPF configurations permanently set in the Switch.
Area ID	Allows the entry of an OSPF Area ID configured above.
Router Priority	Allows the entry of a number between 0 and 255 representing the OSPF priority of the selected area. If a Router Priority of 0 is selected, the Switch cannot be elected as the Designated Router for the network.
Hello Interval	Allows the specification of the interval between the transmission of OSPF Hello packets, in seconds. Between 1 and 65535 seconds can be specified. The Hello Interval , Dead Interval , Authorization Type , and Authorization Key should be the same for all routers on the same network.
Dead Interval	Allows the specification of the length of time between the receipt of Hello packets from a neighbor router before the selected area declares that router down. An interval between 1 and 65535 seconds can be specified. The Dead Interval must be evenly divisible by the Hello Interval .
State	Allows the OSPF interface to be disabled for the selected area without changing the configuration for that area.

Auth Type	<p>This field can be toggled between None, Simple, and MD5 using the space bar. This allows a choice of authorization schemes for OSPF packets that may be exchanged over the OSPF routing domain.</p> <ul style="list-style-type: none"> • None specifies no authorization. • Simple uses a simple password to determine if the packets are from an authorized OSPF router. When Simple is selected, the Auth Key field allows the entry of an 8-character password that must be the same as a password configured on a neighbor OSPF router. • MD5 uses a cryptographic key entered in the MD5 Key Table Configuration menu. When MD5 is selected, the Auth Key ID field allows the specification of the Key ID as defined in the MD5 configuration above. This must be the same MD5 Key as used by the neighboring router.
Auth. Key ID	Enter a Key ID of up to 5 characters to set the Auth. Key ID for either the Simple Auth Type or the MD5 Auth Type, as specified in the previous parameter.
Metric	This field allows the entry of a number between 1 and 65,535 that is representative of the OSPF cost of reaching the selected OSPF interface. The default metric is 1.
DR State	A read only field describing the Designated Router state of the IP interface. This field may read DR if the interface is the designated router, or Backup DR if the interface is the Backup Designated Router. The highest IP address will be the Designated Router and is determined by the OSPF Hello Protocol of the Switch.
DR Address	The IP address of the aforementioned Designated Router.
Backup DR Address	The IP address of the aforementioned Backup Designated Router.
Transmit Delay	A read only field that denotes the estimated time to transmit a Link State Update Packet over this interface, in seconds.
Retransmit Time	A read only field that denotes the time between LSA retransmissions over this interface, in seconds.

OSPF Virtual Interface Settings

Click the **OSPF Virtual Interface Settings** link to view the current **OSPF Virtual Interface Settings**. There are not virtual interface settings configured by default, so the first time this table is viewed there will be not interfaces listed. To add a new OSPF virtual interface configuration set to the table, click the **Add** button. A new menu appears (see below). To change an existing configuration, click on the hyperlinked **Transit Area ID** for the set you want to change. The menu to modify an existing set is the same as the menu used to add a new one. To eliminate an existing configuration, click the **X** in the **Delete** column.

Add									
OSPF Virtual Interface Settings									
Transit Area ID	Neighbor Router ID	Hello Interval	Dead Interval	Auth. Type	Transmit Delay	RetransInterval	Status	Delete	

Figure 6- 137. OSPF Virtual Link Settings

The status of the virtual interface appears (Up or Down) in the **Status** column.

OSPF Virtual Link Settings - Add	
Transit Area ID	<input type="text" value="0.0.0.0"/>
Neighbor Router ID	<input type="text" value="0.0.0.0"/>
Hello Interval(1-65535)	<input type="text" value="10"/>
Dead Interval(1-65535)	<input type="text" value="60"/>
Auth Type	None <input type="button" value="v"/>
Password/Auth. Key ID	<input type="text"/>
Transmit Delay	<input type="text" value="1"/>
Retransmit Interval	<input type="text" value="5"/>
<input type="button" value="Apply"/>	
Show All OSPF Virtual Link Entries	

Figure 6- 138. OSPF Virtual Link Settings – Add

Configure the following parameters to add or change an **OSPF Virtual Interface**:

Parameter	Description
Transit Area ID	Allows the entry of an OSPF Area ID – previously defined on the Switch – that allows a remote area to communicate with the backbone (area 0). A Transit Area cannot be a Stub Area or a Backbone Area.
Neighbor Router	The OSPF router ID for the remote router. This is a 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the remote area’s Area Border Router.
Hello Interval (1-65535)	Specify the interval between the transmission of OSPF Hello packets, in seconds. Enter a value between 1 and 65535 seconds. The Hello Interval , Dead Interval , Authorization Type , and Authorization Key should have identical settings for all routers on the same network.
Dead Interval (1-65535)	Specify the length of time between (receiving) Hello packets from a neighbor router before the selected area declares that router down. Again, all routers on the network should use the same setting.
Auth Type	If using authorization for OSPF routers, select the type being used. MD5 key authorization must be set up in the MD5 Key Settings menu.

Password/Auth. Key ID	Enter a case-sensitive password for simple authorization or enter the MD5 key you set in the MD5 Key settings menu.
Transmit Delay	The number of seconds required to transmit a link state update over this virtual link. Transit delay takes into account transmission and propagation delays. This field is fixed at 1 second.
RetransInterval	The number of seconds between link state advertisement retransmissions for adjacencies belonging to this virtual link. This field is fixed at 5 seconds.

Click **Apply** to implement changes made.



NOTE: For OSPF to function properly some settings should be identical on all participating OSPF devices. These settings include the Hello Interval and Dead Interval. For networks using authorization for OSPF devices, the Authorization Type and Password or Key used must likewise be identical.

OSPF Area Aggregation Settings

Area Aggregation allows all of the routing information that may be contained within an area to be aggregated into a summary LSDB advertisement of just the network address and subnet mask. This allows for a reduction in the volume of LSDB advertisement traffic as well as a reduction in the memory overhead in the Switch used to maintain routing tables.

Click **Configuration > Layer 3 IP Networking > OSPF > OSPF Area Aggregation Settings** link to view the current settings. There are no aggregation settings configured by default, so there will not be any listed the first accessing the menu. To add a new **OSPF Area Aggregation** setting, click the **Add** button. A new menu (pictured below) appears. To change an existing configuration, click on the hyperlinked Area ID for the set you want to change. The menu to modify an existing configuration is the same as the menu used to add a new one. To eliminate an existing configuration, click the **X** in the **Delete** column for the configuration being removed.

OSPF Area Aggregation Settings					
Area ID	Network Number	Network Mask	LSDB Type	Advertisement	Delete
255.255.255.255	201.0.0.0	255.254.0.0	Summary	Enabled	X
255.255.255.255	201.2.0.0	255.254.0.0	Summary	Enabled	X

Figure 6- 139. OSPF Area Aggregation Settings table

Use the menu below to change settings or add a new **OSPF Area Aggregation** setting.

OSPF Area Aggregation Configuration - Add	
Area ID	<input type="text" value="0.0.0.0"/>
Network Number	<input type="text" value="0.0.0.0"/>
Network Mask	<input type="text" value="0.0.0.0"/>
LSDB Type	<input type="text" value="Summary"/>
Advertisement	<input type="text" value="Enabled"/>
<input type="button" value="Apply"/>	
Show All OSPF Aggregation Entries	

Figure 6- 140. OSPF Area Aggregation Settings – Add window

Specify the OSPF aggregation settings and click the **Apply** button to add or change the settings. The new settings will appear listed in the **OSPF Area Aggregation Settings** table. To view the table, click the [Show All OSPF Aggregation Entries](#) link to return to the previous window.

Use the following parameters to configure the following settings for **OSPF Area Aggregation**:

Parameter	Description
Area ID	Allows the entry the OSPF Area ID for which the routing information will be aggregated. This Area ID must be previously defined on the Switch.
Network Number	Sometimes called the Network Address. The 32-bit number in the form of an IP address that uniquely identifies the network that corresponds to the OSPF Area above.
Network Mask	The corresponding network mask for the Network Number specified above.
LSDB Type	Specifies the type of address aggregation, which is set at <i>Summary</i> .
Advertisement	Select <i>Enabled</i> or <i>Disabled</i> to determine whether the selected OSPF Area will advertise it's summary LSDB (Network-Number and Network-Mask).

Click **Apply** to implement changes made.

OSPF Host Route Settings

OSPF host routes work in a way analogous to RIP, only this is used to share OSPF information with other OSPF routers. This is used to work around problems that might prevent OSPF information sharing between routers.

To configure OSPF host routes, click the **OSPF Host Route Settings** link. To add a new OSPF Route, click the **Add** button. Configure the setting in the menu that appears. The **Add** and **Modify** menus for OSPF host route setting are nearly identical. The only difference being that if users are changing an existing configuration, the **Host Address** will not be accessible to change. To change an existing configuration, click on the hyperlinked **Host Address** in the list for the configuration to change and proceed to change the metric or area ID. To eliminate an existing configuration, click the **X** in the **Delete** column for the configuration being removed.

OSPF Host Route Settings			
Host Address	Metric	Area ID	Delete
11.1.1.1	10	255.255.255.255	X
11.1.1.2	10	255.255.255.255	X
11.1.1.3	10	255.255.255.255	X

Figure 6- 141. OSPF Host Route Settings table

Use the menu below to set up OSPF host routes.

OSPF Host Route Setting - Add	
Host Address	<input type="text" value="0.0.0.0"/>
Metric	<input type="text" value="0"/>
Area ID	<input type="text" value="0.0.0.0"/>
<input type="button" value="Apply"/>	
Show All OSPF Host Route Entries	

Figure 6- 142. OSPF Host Route Settings – Add window

Specify the host route settings and click the **Apply** button to add or change the settings. The new settings will appear listed in the **OSPF Host Route Settings** list. To view the previous window, click the [Show All OSPF Host Route Entries](#) link to return to the previous window.

The following fields are configured for OSPF host route:

Parameter	Description
Host Address	The IP address of the OSPF host.
Metric	A value between 1 and 65535 that will be advertised for the route.
Area ID	A 32-bit number in the form of an IP address (xxx.xxx.xxx.xxx) that uniquely identifies the OSPF area in the OSPF domain.

IP Multicast Routing Protocol

The functions supporting IP multicasting are added under the **IP Multicast Routing Protocol** folder, from the **Layer 3 IP Networking** folder.

IGMP, **DVMRP**, and **PIM** can be enabled or disabled on the Switch without changing the individual protocol's configuration.

IGMP

Computers and network devices that want to receive multicast transmissions need to inform nearby routers that they will become members of a multicast group. The **Internet Group Management Protocol (IGMP)** is used to communicate this information. IGMP is also used to periodically check the multicast group for members that are no longer active.

In the case where there is more than one multicast router on a subnetwork, one router is elected as the 'querier'. This router then keeps track of the membership of the multicast groups that have active members. The information received from IGMP is then used to determine if multicast packets should be forwarded to a given subnetwork or not. The router can check, using IGMP, to see if there is at least one member of a multicast group on a given subnetwork. If there are no members on a subnetwork, packets will not be forwarded to that subnetwork.

IGMP Versions 1 and 2

Multicast groups allow members to join or leave at any time. IGMP provides the method for members and multicast routers to communicate when joining or leaving a multicast group.

IGMP version 1 is defined in RFC 1112. It has a fixed packet size and no optional data.

The format of an IGMP packet is shown below:

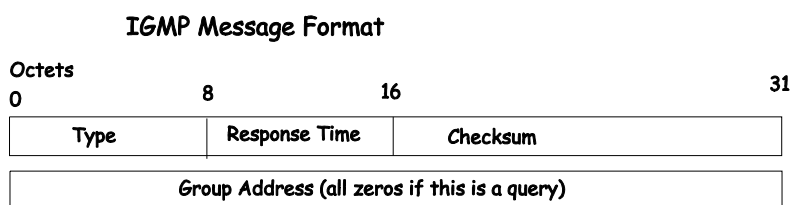


Figure 6- 143. IGMP Message Format

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 6- 7. IGMP Type Codes

IGMP packets enable multicast routers to keep track of the membership of multicast groups, on their respective subnetworks. The following outlines what is communicated between a multicast router and a multicast group member using IGMP.

A host sends an IGMP "report" to join a group

A host will never send a report when it wants to leave a group (for version 1).

A host will send a "leave" report when it wants to leave a group (for 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.

The Time-to-Live (TTL) field of query messages is set to 1 so that the queries will not be forwarded to other subnetworks.

IGMP version 2 introduces some enhancements such as a method to elect a multicast querier for each LAN, an explicit leave message, and query messages that are specific to a given group.

The states a computer will go through to join or to leave a multicast group are shown below:

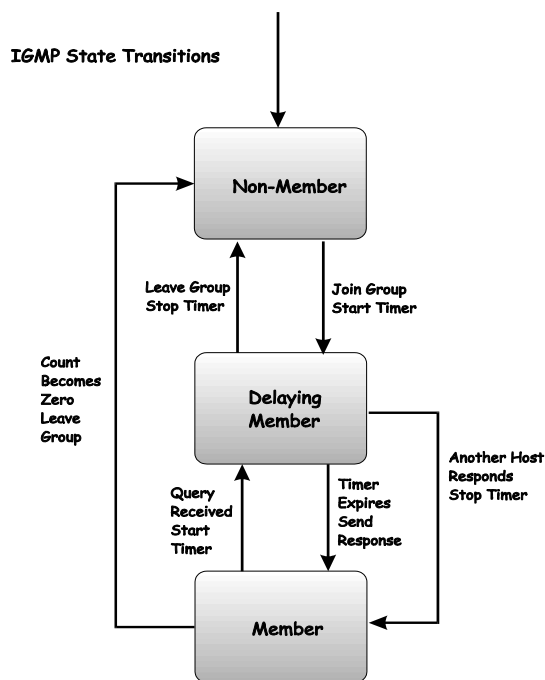


Figure 6- 144. IGMP State Transitions

IGMP Version 3

The current release of the xStack[®] DES-6500 switch series now implements IGMPv3. Improvements of IGMPv3 over version 2 include:

- The introduction of the *SSM* or *Source Specific Multicast*. In previous versions of IGMP, the host would receive all packets sent to the multicast group. Now, a host will receive packets only from a specific source or sources. This is done through the implementation of *include* and *exclude* filters used to accept or deny traffic from these specific sources.
- In IGMP v2, Membership reports could contain only one multicast group whereas in v3, these reports can contain multiple multicast groups and multiple sources within the multicast group.
- Leaving a multicast group could only be accomplished using a specific leave message in v2. In v3, leaving a multicast group is done through a Membership report which includes a block message in the group report packet.
- For version 2, the host could respond to a group query but in version 3, the host is now capable to answer queries specific to the group and the source.

IGMP v3 is backwards compatible with other versions of IGMP.

The IGMPv3 Type supported codes are shown below:

Type	Meaning
0x11	Membership Query
0x12	Version 1 Membership Report
0x16	Version 2 Membership Report
0x17	Version 2 Leave Group
0x22	IGMPv3 Membership Report

Timers

As previously mentioned, IGMPv3 incorporates filters to include or exclude sources. These filters are kept updated using timers. IGMPv3 utilizes two types of timers, one for the group and one for the source. The purpose of the filter mode is to reduce the reception state of a multicast group so that all members of the multicast group are satisfied. This filter mode is dependant on membership reports and timers of the multicast group. These filters are used to maintain a list of multicast sources and groups of multicast receivers that more accurately reflect the actual sources and receiving groups at any one time on the network.

Source timers are used to keep sources present and active within a multicast group on the Switch. These source timers are refreshed if a group report packet is received by the Switch, which holds information pertaining to the active source group record

part of a report packet. If the filter mode is exclude, traffic is being denied from at least one specific source, yet other hosts may be accepting traffic from the multicast group. If the group timer expires for the multicast group, the filter mode is changed to include and other hosts can receive traffic from the source. If no group report packet is received and the filter mode is include, the Switch presumes that traffic from the source is no longer wanted on the attached network and the source record list is then deleted after all source timers expire. If there is no source list record in the multicast group, the multicast group will be deleted from the Switch.

Timers are also used for IGMP version 1 and 2 members, which are a part of a multicast group when the Switch is running IGMPv3. This timer is based on a host within the multicast group that is running IGMPv1 or v2. Receiving a group report from an IGMPv1 or v2 host within the multicast group will refresh the timer and keep the v1 and/or v2 membership alive in v3.



NOTE: The length of time for all timers utilized in IGMPv3 can be determined using IGMP configurations to perform the following calculation:

(Group Membership Interval x Robustness Variable) + One Query Response Interval

IGMP Interface Configuration

The Internet Group Multicasting Protocol (IGMP) can be configured on the Switch on a per-IP interface basis. To view the **IGMP Interface Table**, open the **IP Multicast Routing Protocol** folder under **Configuration** and click **IGMP Interface Settings**. Each IP interface configured on the Switch is displayed in the below **IGMP Interface Table** dialog box. To configure IGMP for a particular interface, click the corresponding hyperlink for that IP interface. This will open another **IGMP Interface Configuration** window:

Total Entries : 1							
IGMP Interface Table							
Interface Name	IP Address	Version	Query	Max Response Time	Robustness Value	Last Member Query Interval	State
System	10.53.13.65	2	125	10	2	1	Disabled

Figure 6- 145. IGMP Interface Settings window

IGMP Interface Configuration	
Interface Name	System
IP Address	10.53.13.100
Version	3 ▾
Query Interval(1-31744)	125
Max Response Time(1-25)	10
Robustness Variable(1-255)	2
Last Member Query Interval(1-25)	1
State	Disabled ▾
<input type="button" value="Apply"/>	
Show All IGMP Interface Entries	

Figure 6- 146. IGMP Interface Settings - Edit window

This window allows the configuration of IGMP for each IP interface configured on the Switch. IGMP can be configured as Version 1, 2 or 3 by toggling the **Version** field using the pull-down menu. The length of time between queries can be varied by entering a value between 1 and 31,744 seconds in the **Query Interval** field. The maximum length of time between the receipt of a query and the sending of an IGMP response report can be varied by entering a value in the **Max Response Time** field.

The **Robustness Variable** field allows IGMP to be ‘tuned’ for sub-networks that are expected to lose many packets. A high value (max. 255) for the robustness variable will help compensate for ‘lossy’ sub-networks. A low value (min. 2) should be used for less ‘lossy’ sub-networks.

The following fields can be set:

Parameter	Description
Interface Name	Displays the name of the IP interface that is to be configured for IGMP. This must be a previously configured IP interface.
IP Address	Displays the IP address corresponding to the IP interface name above.
Version	Enter the IGMP version (1, 2 or 3) that will be used to interpret IGMP queries on the interface.
Query Interval	Allows the entry of a value between 1 and 31744 seconds, with a default of 125 seconds. This specifies the length of time between sending IGMP queries.

Max Response Time	Sets the maximum amount of time allowed before sending an IGMP response report. A value between 1 and 25 seconds can be entered, with a default of 10 seconds.
Robustness Variable	A tuning variable to allow for subnetworks that are expected to lose a large number of packets. A value between 2 and 255 can be entered, with larger values being specified for subnetworks that are expected to lose larger numbers of packets.
Last Member Query Interval	Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave group messages. A value between 1 and 25. The default is 1 second.
State	This field can be toggled between <i>Enabled</i> and <i>Disabled</i> and enables or disables IGMP for the IP interface. The default is <i>Disabled</i> .

Click **Apply** to implement changes made.

DVMRP Interface Configuration

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.

DVMRP resembles the Routing Information Protocol (RIP), but is extended for multicast delivery. DVMRP builds a routing table to calculate ‘shortest paths’ back to the source of a multicast message, but defines a ‘route cost’ (similar to the hop count in RIP) as a relative number that represents the real cost of using this route in the construction of a multicast delivery tree to be ‘pruned’ - once the delivery tree has been 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.

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.

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.

DVMRP Configuration

To enable DVMRP globally on the Switch, click **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > Configuration**. This will give the user access to the following screen:



Figure 6- 147. DVMRP Global Settings window

Use the pull down menu, choose *Enabled*, and click **Apply** to implement the DVMRP function on the Switch.

DVMRP Interface Settings

To view the **DVMRP Interface Table**, click **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > DVMRP Interface Settings**. This menu allows the **Distance-Vector Multicast Routing Protocol (DVMRP)** to be configured for each IP interface defined on the Switch. Each IP interface configured on the Switch is displayed in the below **DVMRP Interface Configuration** dialog box. To configure DVMRP for a particular interface, click the corresponding hyperlink for that IP interface. This will open the **DVMRP Interface Settings** window:

DVMRP Interface Settings					
Interface Name	IP Address	Neighbor Timeout	Probe	Metric	State
System	10.53.13.121	35	10	1	Disabled
Trinity	12.1.1.1	35	10	1	Disabled

Figure 6- 148. DVMRP Interface Settings window

DVMRP Interface Settings	
Interface Name	System
IP Address	10.53.13.65
Neighbor Timeout Interval(1-65535 sec)	<input type="text" value="35"/>
Probe Interval(1-65535 sec)	<input type="text" value="10"/>
Metric(1-31)	<input type="text" value="1"/>
State	Disabled ▾
<input type="button" value="Apply"/>	
Show All DVMRP Interface Entries	

Figure 6- 149. DVMRP Interface Settings – Edit window

The following fields can be set:

Parameter	Description
Interface Name	Displays the name of the IP interface for which DVMRP is to be configured. This must be a previously defined IP interface.
IP Address	Displays the IP address corresponding to the IP Interface name entered above.
Neighbor Timeout Interval (1-65535)	This field allows an entry between 1 and 65,535 seconds and defines the time period DVMRP will hold Neighbor Router reports before issuing poison route messages. The default is 35 seconds.
Probe Interval (1-65535)	This field allows an entry between 1 and 65,535 seconds and defines the interval between 'probes'. The default is 10.
Metric (1-31)	This field allows an entry between 1 and 31 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.
State	This field can be toggled between <i>Enabled</i> and <i>Disabled</i> and enables or disables DVMRP for the IP interface. The default is <i>Disabled</i> .

Click **Apply** to implement changes made. Click [Show All DVMRP Interface Entries](#) to return to the **DVMRP Interface Settings** window.

PIM Protocol

PIM or *Protocol Independent Multicast* is a method of forwarding traffic to multicast groups over the network using any pre-existing unicast routing protocol, such as RIP or OSPF, set on routers within a multicast network. The xStack® DES-6500 Series supports two types of PIM, Dense Mode (PIM-DM) and Sparse Mode (PIM-SM).

PIM-SM

PIM-SM or *Protocol Independent Multicast – Sparse Mode* is a method of forwarding multicast traffic over the network only to multicast routers who actually request this information. Unlike most multicast routing protocols which flood the network with multicast packets, PIM-SM will forward traffic to routers who are explicitly a part of the multicast group through the use of a Rendezvous Point (RP). This RP will take all requests from PIM-SM enabled routers, analyze the information and then returns multicast information it receives from the source, to requesting routers within its configured network. Through this method, a distribution tree is created, with the RP as the root. This distribution tree holds all PIM-SM enabled routers within which information collected from these router is stored by the RP.

Two other types of routers also exist with the PIM-SM configuration. When many routers are a part of a multiple access network, a Designated Router (DR) will be elected. The DR's primary function is to send Join/Prune messages to the RP. The router with the highest priority on the LAN will be selected as the DR. If there is a tie for the highest priority, the router with the higher IP address will be chosen.

The third type of router created in the PIM-SM configuration is the Boot Strap Router (BSR). The goal of the Boot Strap Router is to collect and relay RP information to PIM-SM enabled routers on the LAN. Although the RP can be statically set, the BSR mechanism can also determine the RP. Multiple Candidate BSRs (C-BSR) can be set on the network but only one BSR will be elected to process RP information. If it is not explicitly apparent which C-BSR is to be the BSR, all C-BSRs will emit Boot Strap Messages (BSM) out on the PIM-SM enabled network to determine which C-BSR has the higher priority and once determined, will be elected as the BSR. Once determined, the BSR will collect RP data emanating from candidate RPs on the PIM-SM network, compile it and then send it out on the land using periodic Boot Strap Messages (BSM). All PIM-SM Routers will get the RP information from the Boot Strap Mechanism and then store it in their database.

Discovering and Joining the Multicast Group

Although Hello packets discover PIM-SM routers, these routers can only join or be “pruned” from a multicast group through the use of Join/Prune Messages exchanged between the DR and RP. Join/Prune Messages are packets relayed between routers that effectively state which interfaces are, or are not to be receiving multicast data. These messages can be configured for their frequency to be sent out on the network and are only valid to routers if a Hello packet has first been received. A Hello packet will simply state that the router is present and ready to become a part of the RP's distribution tree. Once a router has accepted a member of the IGMP group and it is PIM-SM enabled, the interested router will then send an explicit Join/Prune message to the RP, which will in turn route multicast data from the source to the interested router, resulting in a unidirectional distribution tree for the group. Multicast packets are then sent out to all nodes on this tree. Once a prune message has been received for a router that is a member of the RP's distribution tree, the router will drop the interface from its distribution tree.

Distribution Trees

Two types of distribution trees can exist within the PIM-SM protocol, a Rendezvous-Point Tree (RPT) and a Shortest Path Tree (SPT). The RP will send out specific multicast data that it receives from the source to all outgoing interfaces enabled to receive multicast data. Yet, once a router has determined the location of its source, an SPT can be created, eliminating hops between the source and the destination, such as the RP. This can be configured by the switch administrator by setting the multicast data rate threshold. Once the threshold has been passed, the data path will switch to the SPT. Therefore, a closer link can be created between the source and destination, eliminating hops previously used and shortening the time a multicast packet is sent from the source to its final destination.

Register and Register Suppression Messages

Multicast sources do not always join the intended receiver group. The first hop router (DR) can send multicast data without being the member of a group or having a designated source, which essentially means it has no information about how to relay this information to the RP distribution tree. This problem is alleviated through Register and Register-Stop messages. The first multicast packet received by the DR is encapsulated and sent on to the RP which in turn removes the encapsulation and sends the packet on down the RP distribution tree. When the route has been established, a SPT can be created to directly connect routers to the source, or the multicast traffic flow can begin, traveling from the DR to the RP. When the latter occurs, the same packet may be sent twice, one type encapsulated, one not. The RP will detect this flaw and then return a Register Suppression message to the DR requesting it to discontinue sending encapsulated packets.

Assert Messages

At times on the PIM-SM enabled network, parallel paths are created from source to receiver, meaning some receivers will receive the same multicast packets twice. To improve this situation, Assert messages are sent from the receiving device to both multicast sources to determine which single router will send the receiver the necessary multicast data. The source with the shortest metric (hop count) will be elected as the primary multicast source. This metric value is included within the Assert message.

PIM-DM Interface Configuration

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 PIM-DM multicast routing protocol 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**.

PIM Global Settings

To enable PIM globally on the Switch, go to **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > PIM Protocol > PIM Global Settings**. This will give the user access to the following screen:



Figure 6- 150. PIM Global Settings window

Use the pull-down menu, choose *Enabled*, and click **Apply** to set the PIM function on the Switch.

PIM Interface Settings

To configure the settings for the PIM Protocol per IP interface, go to **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > PIM Protocol > PIM Interface Settings**. This will give the user access to the following screen:

PIM Interface Settings							
Interface Name	IP Address	Designated Router	Hello Interval	Join/Prune Interval	Mode	State	DR priority
System	10.53.13.30	10.53.13.30	30	60	DM	Disabled	1
Trinity	11.1.1.1	11.1.1.1	30	60	DM	Disabled	1

Figure 6- 151. PIM Interface Settings window

To configure an IP interface for PIM, click its corresponding link which will lead you to the following screen:

PIM Interface Settings - Edit	
Interface Name	System
IP Address	10.53.13.30
Designated Router	10.53.13.30
Hello Interval (1-18724 sec)	<input type="text" value="30"/>
Join/Prune Interval (1-18724 sec)	<input type="text" value="60"/>
Mode	<input type="text" value="DM"/>
State	<input type="text" value="Disabled"/>
DR priority (0-4294967294)	<input type="text" value="1"/>
<input type="button" value="Apply"/>	
Show All PIM Interface Entries	

Figure 6- 152. PIM Interface Settings – Edit window

The following fields can be set:

Parameter	Description
Interface Name	This read-only field denotes the IP interface selected to be configured for PIM.
IP Address	This read-only field denotes the IP address of the IP interface selected to be configured for PIM.
Designated Router	This read-only field denotes the IP address of the Designated Router of the distribution tree to which this IP address belongs.
Hello Interval	This field will set the interval time between the sending of Hello Packets from this IP interface to neighboring routers one hop away. These Hello packets are used to discover other PIM enabled routers and state their priority as the Designated Router (DR) on the PIM enabled network. The user may state an interval time between 1 – 18724 seconds with a default interval time of 30 seconds.
Join/Prune Interval	This field will set the interval time between the sending of Join/Prune packets stating which multicast groups are to join the PIM enabled network and which are to be removed or “pruned” from that group. The user may state an interval time between 1 – 18724 seconds with a default interval time of 60 seconds.
Mode	Use the pull-down menu to select the type of PIM protocol to use, Sparse Mode (SM) or Dense Mode (DM). The default setting is DM.
State	Use the pull-down menu to enable or disable PIM for this IP interface. The default is Disabled.
DR priority	Enter the priority of this IP interface to become the Designated Router for the multiple access network. The user may enter a DR priority between 0 and 4,294,967,294 with a default setting of 1.

Click **Apply** to implement changes made.

PIM Candidate BSR Settings

The following windows are used to configure the Candidate Boot Strap Router (C-BSR) settings for the switch and the priority of the selected IP interface to become the Boot Strap Router (BSR) for the PIM enabled network. The Boot Strap Router holds the information which determines which router on the network is to be elected as the RP for the multicast group and then to gather and distribute RP information to other PIM-SM enabled routers. To view the Candidate BSR window, click **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > PIM Protocol > PIM Candidate BSR Settings**.

Figure 6- 153. PIM Candidate BSR Global Settings window

The following fields can be set:

Parameter	Description
Hash Mask Len	Enter a hash mask length, which will be used with the IP address of the candidate RP and the multicast group address, to calculate the hash algorithm used by the router to determine which C-RP on the PIM-SM enabled network will be the RP. The user may select a length between 0 – 32 with a default setting of 30.
Bootstrap Period	Enter a time period between 1-255 to determine the interval the Switch will send out Boot Strap Messages (BSM) to the PIM enabled network. The default setting is 60 seconds.
Interface Name	To find an IP interface on the Switch, enter the interface name into the space provided and click Find . If found, the Interface Name will appear alone in the PIM Candidate BSR Settings window below.

To view the CBSR settings for an IP interface and set its BSR priority, click its hyperlinked name, which will lead to the following window.

Figure 6- 154. PIM Candidate BSR Settings – Edit

The following fields can be viewed or set:

Parameter	Description
Interface Name	This read-only field denotes the IP Interface Name to be edited for its C-BSR priority.
IP Address	Denotes the IP Address of the IP Interface Name to be edited for its C-BSR priority.
Priority	Used to state the Priority of this IP Interface to become the BSR. The user may select a priority between -1 to 255. An entry of -1 states that the interface will be disabled to be the BSR.

Click **Apply** to set the priority for this IP Interface.

PIM Parameter Settings

The following window will configure the parameter settings for the PIM distribution tree. To view this window, click **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > PIM Protocol > PIM Parameter Settings**.

PIM Parameter Settings	
Last Hop SPT Threshold (0-65535 Packets/Second) [infinity]	0
RP SPT Threshold (0-65535 Packets/Second) [infinity]	0
Register Probe Time (1-127 sec.)	5
Register Suppression Time (3-255 sec.)	60

Apply

Figure 6- 155. PIM Parameter Settings window

The following fields can be viewed or set:

Parameter	Description
Last Hop SPT Threshold	This field is to be configured for the last hop router in the RP tree. When the amount of multicast packets per second reaches the configured threshold, the last hop router will change its distribution tree to a (Shortest Path Tree) SPT. The user may enter a value between 0-65535 packets per second. 0 will denote that the last hop router will immediately enter the SPT once a multicast packet has been received. An entry of <i>infinity</i> will disable the last hop router from entering the SPT. The default setting is 0.
RP SPT Threshold	This field is to be configured for the RP of the distribution tree. When the amount of register packets per second reaches the configured threshold, it will trigger the RP to switch to an SPT, between the RP and the first hop router. The user may enter a value between 0-65535 packets per second. 0 will denote that the RP will immediately enter the SPT once a register packet has been received. An entry of <i>infinity</i> will disable the RP from entering an SPT. The default setting is 0.
Register Probe Time	This command is used to set a time to send a probe message from the DR to the RP before the Register Suppression time expires. If a Register Stop message is received by the DR, the Register Suppression Time will be restarted. If no Register Stop message is received within the probe time, Register Packets will be resent to the RP. The user may configure a time between 1-127 seconds with a default setting of 5 seconds.
Register Suppression Time	This field is to be configured for the first hop router from the source. After this router sends out a Register message to the RP, and the RP replies with a Register stop message, it will wait for the time configured here to send out another register message to the RP. The user may set a time between 3-255 with a default setting of 60 seconds.

Click **Apply** to implement changes made.



NOTE: The Probe time value must be less than half of the Register Suppression Time value. If not, the administrator will be presented with an error message after clicking Apply.

PIM Candidate RP Global Settings

The following window is used to set the Parameters for this Switch to become the RP of its distribution tree. To view this window, click **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > PIM Protocol > PIM Candidate RP Global Settings**.

Figure 6- 156. PIM Candidate RP Global Settings

The following fields can be viewed or set:

Parameter	Description
Hold Time	This field is used to set the time Candidate RP (CRP) advertisements are valid on the PIM-SM enabled network. If CRP advertisements are not received by the BSR within this time frame, the CRP is removed from the list of candidates. The user may set a time between 0-255 seconds with a default setting of 150 seconds. An entry of 0 will send out one advertisement that states to the BSR that it should be immediately removed from CRP status on the PIM-SM network.
Priority	Enter a priority value to determine which CRP will become the RP for the distribution tree. This priority value will be included in the router's CRP advertisements. A lower value means a higher priority, yet, if there is a tie for the highest priority, the router having the higher IP address will become the RP. The user may set a priority between 0–255 with a default setting of 0.
Wildcard Prefix Count	The user may set the Prefix Count value of the wildcard group address here by choosing a value between 0 and 1 with a default setting of 0.

Click **Apply** to implement changes made.

PIM Candidate RP Settings

The following window will display the parameters for the switch to become a CRP. To view this window, click **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > PIM Protocol > PIM Candidate RP Settings**.

Figure 6- 157. PIM Candidate RP Settings window

To configure the settings for this window, click the Add button, which will reveal the following window for the administrator to configure.

Figure 6- 158. PIM Candidate RP Settings – Add window

The following fields can be viewed or set:

Parameter	Description
Group Address	Enter the multicast group address for this CRP. This address must be a class D address.
Group Mask	Enter the mask for the multicast group address stated above.
Interface Name	Enter the name of the PIM-SM enabled interface the switch administrator wishes to become the CRP for this group.

Click **Apply** to implement changes made.

PIM Register Checksum Settings

This window is used to set a first hop router to create checksums to be included with the data in Registered packets. To view this window, click **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > PIM Protocol > PIM Register Checksum Settings**.

Figure 6- 159. PIM Register Checksum Include Data RP List Settings window

To configure the settings for this window, click the **Add** button, which will reveal the following window for the administrator to configure.

Figure 6- 160. PIM Register Checksum Include Data RP List Settings - Add window

The following fields can be set:

Parameter	Description
RP Address	Enter the IP address of the RP that will verify checksums included with Registered packets.

Click **Apply** to set the RP as a checksum enabled router.

PIM Static RP Settings

This window is used to view the Static RP settings for this router. To view this window, click **Configuration > Layer 3 IP Networking > IP Multicast Routing Protocol > PIM Protocol > PIM Static RP Settings**.

Figure 6- 161. PIM Static RP Settings window

To configure the settings for this window and set this router as the Static RP, click the **Add** button, which will reveal the following window for the administrator to configure.

Figure 6- 162. PIM Static RP Settings – Add window

The following fields can be set:

Parameter	Description
Group Address	Enter the multicast group IP address to identify who is the RP. This address must be a class D address.
Group Mask	Enter the mask for the Group address stated above.
RP Address	Enter the RP's IP address to be set for the Group Address stated above.

Click **Apply** to set the static RP.

DNS Relay

Computer users usually prefer to use text names for computers for which they may want to open a connection. 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 Switch 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 Domain Name System (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 sub domain. 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 DHCP or BOOTP server, or can be entered manually and configured into the operating system at startup.

DNS Relay Information

To configure the DNS function on the Switch, click **Configuration > Layer 3 IP Networking > DNS Relay > DNS Relay Information**, which will open the **DNS Relay Information** window, as seen below:

DNS Relay Information	
DNS Relay Status	Disabled
Primary Name Server	0.0.0.0
Secondary Name Server	0.0.0.0
DNSR Cache Status	Disabled
DNSR Static Table Status	Disabled
Apply	

Figure 6- 163. DNS Relay Global Settings window

The following fields can be set:

Parameter	Description
DNS Relay Status	This field can be toggled between <i>Disabled</i> and <i>Enabled</i> using the pull-down menu, and is used to enable or disable the DNS Relay service on the Switch.
Primary Name Server	Allows the entry of the IP address of a primary domain name server (DNS).
Secondary Name Server	Allows the entry of the IP address of a secondary domain name server (DNS).

DNSR Cache Status	This can be toggled between <i>Disabled</i> and <i>Enabled</i> . This determines if a DNS cache will be enabled on the Switch.
DNSR Static Table State	This field can be toggled using the pull-down menu between <i>Disabled</i> and <i>Enabled</i> . This determines if the static DNS table will be used or not.

Click **Apply** to implement changes made.

DNS Relay Static Settings

To view the **DNS Relay Static Settings**, click **Configuration > Layer 3 IP Networking > DNS Relay > DNS Relay Static Settings**, which will open the **DNS Relay Static Settings** window, as seen below:

DNS Relay Static Settings		
Domain Name	IP Address	Apply
<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="button" value="Add"/>
DNS Relay Static Table		
Domain Name	IP Address	Delete
System	10.53.13.94	<input type="button" value="X"/>

Figure 6- 164. DNS Relay Static Settings and Table window

To add an entry into the **DNS Relay Static Table**, simply enter a **Domain Name** with its corresponding IP address and click **Add** under the **Apply** heading. A successful entry will be presented in the table below, as shown in the example above. To erase an entry from the table, click the corresponding of the entry to delete.

DHCP / BOOTP Relay

The 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, with a default value of 4. The relay time threshold 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 0 and 65,536 seconds, with a default value of 0 seconds.

DHCP Auto Configuration Settings

This window is used to enable the DHCP Autoconfiguration feature on the Switch. When enabled, the Switch is instructed to receive a configuration file from a TFTP server, which will set the Switch to become a DHCP client automatically on boot up. To employ this method, the DHCP server must be set up to deliver the TFTP server IP address and configuration file name information in the DHCP reply packet. The TFTP server must be up and running and hold the necessary configuration file stored in its base directory when the request is received from the Switch. For more information about loading a configuration file for use by a client, see the DHCP server and/or TFTP server software instructions. The user may also consult the Upload screen description located in the Maintenance section of this manual.

If the Switch is unable to complete the DHCP auto configuration, the previously saved configuration file present in the Switch's memory will be used.



Figure 6- 165. DHCP Auto Configuration Settings window

To enable the DHCP Auto Configuration State, use the pull-down menu to choose **Enable** and click the Apply button.

DHCP / BOOTP Relay Information

To enable and configure BOOTP or DHCP on the Switch, click **Configuration > DHCP/BOOTP Relay > DHCP/BOOTP Relay Information**:

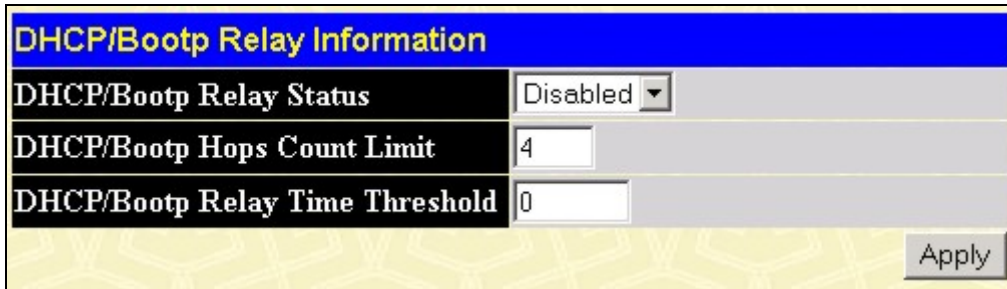


Figure 6- 166. DHCP/ BOOTP Relay Global Settings window

The following fields can be set:

Parameter	Description
DHCP/BOOTP Relay Status	This field can be toggled between <i>Enabled</i> and <i>Disabled</i> using the pull-down menu. It is used to enable or disable the BOOTP/DHCP Relay service on the Switch. The default is <i>Disabled</i>
DHCP/ Bootp Hops Count Limit	This field allows an entry between 1 and 16 to define the maximum number of router hops BOOTP messages can be forwarded across. The default hop count is 4.
DHCP/Bootp Relay Time Threshold	Allows an entry between 0 and 65535 seconds, and defines the maximum time limit for routing a BOOTP/DHCP packet. If a value of 0 is entered, the Switch will not process the value in the seconds field of the BOOTP or DHCP packet. If a non-zero value is entered, the Switch will use that value, along with the hop count to determine whether to forward a given BOOTP or DHCP packet.

DHCP/BOOTP Relay Settings

The **DHCP/ BOOTP Relay Settings** allow the user to set up a server, by IP address, for relaying DHCP / BOOTP information. The user may enter a previously configured IP interface on the Switch that will be connected directly to the DHCP/BOOTP server using the following window. Properly configured settings will be displayed in the **BOOTP Relay Table** at the bottom of the following window, once the user clicks the **Add** button under the **Apply** heading. The user may add up to four server IPs per IP interface on the Switch. Entries may be deleted by clicking it's corresponding **X**.

DHCP/Bootp Relay Settings				
Interface Name	IP Address			Apply
<input type="text"/>	<input type="text" value="0.0.0.0"/>			<input type="button" value="Add"/>
DHCP/Bootp Relay Table				
Interface	Server 1	Server 2	Server 3	Server 4
System	<input type="button" value="X"/> 10.53.13.94			

Figure 6- 167. DHCP/BOOTP Relay Interface Settings and DHCP/BOOTP Relay Interface Table window

The following parameters may be configured or viewed.

Parameter	Description
Interface Name	The IP interface on the Switch that will be connected directly to the Server.
IP Address	Enter the IP address of the DHCP/BOOTP server. Up to four server IPs can be configured per IP interface



NOTE: Secondary IP interfaces do not support DHCP/BOOTP relay, only primary IP interfaces support DHCP/BOOTP relay.

DHCP Relay Option 82 Settings

DHCP clients hold basic information for clients on the network. To get this information, servers send out packets holding BOOTP information necessary for the Switch and its functionality. Yet, there are times DHCP servers and clients do not reside on the same physical subnet and therefore the transfer of this information becomes more difficult. To ease the flow of this information, the Switch can now act as a DHCP Relay agent. When the relay agent receives the DHCP request, it adds the option configuration information, and the IP address of the relay agent (if the relay agent is configured), to the packet. Once the option information has been added to the packet, it is sent on to the DHCP server. Upon receiving the packet, if the server is capable of processing the option configuration information, it can implement policies like restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Once processed, the DHCP server echoes the option field in the DHCP reply. The DHCP server unicasts the reply back to the relay agent if the request was relayed to the server by the relay agent. The Switch then verifies that it originally inserted the option data. Finally, the relay agent removes the option field and forwards the packet to the switch port that is connected to the DHCP client that sent the DHCP request.

DHCP Relay Agent Information Option 82 Settings	
DHCP Relay Agent Information Option 82 State	Disabled ▾
DHCP Relay Agent Information Option 82 Check	Disabled ▾
DHCP Relay Agent Information Option 82 Policy	replace ▾
Apply	

Figure 6- 168. DHCP Relay Option Settings

The following fields can be set:

Parameter	Description
DHCP Relay Option State	<p>This field can be toggled between <i>Enabled</i> and <i>Disabled</i> using the pull-down menu. It is used to enable or disable the DHCP Agent Information Option on the Switch. The default is <i>Disabled</i>.</p> <p><i>Enabled</i> – When this field is toggled to <i>Enabled</i> the relay agent will insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients.</p> <p><i>Disabled</i> - If the field is toggled to <i>Disabled</i> the relay agent will not insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the check and policy settings will have no effect.</p>
DHCP Relay Option Check	<p>This field can be toggled between <i>Enabled</i> and <i>Disabled</i> using the pull-down menu. It is used to enable or disable the Switches ability to check the validity of the packet's option field.</p> <p><i>Enabled</i> – When <i>Enabled</i>, the relay agent will check the validity of the packet's option field. If the Switch receives a packet that contains the option field from a DHCP client, the Switch drops the packet because it is invalid. In packets received from DHCP servers, the relay agent will drop invalid messages.</p> <p><i>Disabled</i> - When <i>Disabled</i>, the relay agent will not check the validity of the packet's option 82 field.</p>
DHCP Relay Option Policy	<p>This field can be toggled between <i>Replace</i>, <i>Drop</i>, and <i>Keep</i> by using the pull-down menu and is used to set the Switches policy for handling packets when the DHCP Relay Option Check is set to <i>Disabled</i>. The default setting is <i>Replace</i>.</p> <p><i>Replace</i> - The option field will be replaced if the option field already exists in the packet received from the DHCP client.</p> <p><i>Drop</i> - The packet will be dropped if the option field already exists in the packet received from the DHCP client.</p> <p><i>Keep</i> - The option field will be retained if the option field already exists in the packet received from the DHCP client.</p>



NOTE: If the switch receives a packet that contains the option 82 field from a DHCP client and the information-checking feature is enabled, the switch drops the packet because it is invalid. However, in some instances users may configure a client with the option-82 field. In this situation, disable the information-check feature so that the Switch does not remove the option-82 field from the packet.

VRRP

VRRP or *Virtual Routing Redundancy Protocol* is a function on the Switch that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router that controls the IP address associated with a virtual router is called the Master, and will forward packets sent to this IP address. This will allow any Virtual Router IP address on the LAN to be used as the default first hop router by end hosts. Utilizing VRRP, the administrator can achieve a higher available default path cost without needing to configure every end host for dynamic routing or routing discovery protocols.

Statically configured default routes on the LAN are prone to a single point of failure. VRRP is designed to eliminate these failures by setting an election protocol that will assign a responsibility for a virtual router to one of the VRRP routers on the LAN. When a virtual router fails, the election protocol will select a virtual router with the highest priority to be the Master router on the LAN. This retains the link and the connection is kept alive, regardless of the point of failure.

To configure VRRP for virtual routers on the Switch, an IP interface must be present on the system and it must be a part of a VLAN. VRRP IP interfaces may be assigned to every VLAN, and therefore IP interface, on the Switch. VRRP routers within the same VRRP group must be consistent in configuration settings for this protocol to function optimally.

VRRP Global Settings

To enable VRRP globally on the Switch, click **Configuration > Layer 3 IP Networking > VRRP > VRRP Global Settings**:



Figure 6- 169. VRRP Global Settings window

The following fields can be set:

Parameter	Description
Global VRRP	Use the pull-down menu to enable or disable VRRP globally on the Switch. The default is <i>Disabled</i> .
Non-owner response PING	Enabling this parameter will allow the virtual IP address to be pinged from other host end nodes to verify connectivity. This will only enable the ping connectivity check function. This command is <i>Disabled</i> by default.

Click **Apply** to implement changes made.

VRRP Virtual Router Settings

The following window will allow the user to view the parameters for the VRRP function on the Switch. To view this window, click **Configuration > Layer 3 IP Networking > VRRP > VRRP Virtual Router Settings**:

VRRP Virtual Router Settings				
VRID	Interface Name	Authentication type	Display	Delete
1	System	No Authentication	View	<input type="button" value="X"/>

Figure 6- 170. VRRP Virtual Router Settings window

The following fields are displayed in the window above:

Parameter	Description
VRID	VRID - Displays the virtual router ID set by the user. This will uniquely identify the VRRP Interface on the network.
Interface Name	An IP interface name that has been enabled for VRRP. This entry must have been previously set in the IP Interfaces table.
Authentication Type	Displays the Authentication in use on this Virtual Interface. Possible authentication types include: <ul style="list-style-type: none"> <i>No authentication</i> - No authentication has been selected to compare VRRP packets received by a virtual router. <i>Simple Text Password</i> - A Simple password has been selected to compare VRRP packets received by a virtual router, for authentication. <i>IP Authentication Header</i> - An MD5 message digest algorithm has been selected to compare VRRP packets received by a virtual router, for authentication.
Display	Click the View button to display the settings for this particular VRRP entry.
Delete	Click the <input type="button" value="X"/> to delete this VRRP entry.

Click the **Add** button to display the following window to configure a VRRP interface. Or, the user may click the hyperlinked **Interface Name** to view the same window:

VRRP Virtual Router Settings	
VRID(1-255)	<input type="text" value="0"/>
Interface Name	<input type="text"/>
IP Address	<input type="text" value="0.0.0.0"/>
Admin. State	<input type="button" value="Enable"/>
Priority(1-254)	<input type="text" value="100"/>
Advertisement Interval(1-255)	<input type="text" value="1"/>
Preempt Mode	<input type="button" value="True"/>
Critical IP Address	<input type="text" value="0.0.0.0"/>
Checking Critical IP	<input type="button" value="Disable"/>
<input type="button" value="Apply"/>	
Show All VRRP Interface Entries	

Figure 6- 171. VRRP Virtual Router Settings – Add window

The following parameters may be set to configure an existing or new VRRP virtual router.

Parameter	Description
VRID (1-255)	Enter a value between 1 and 255 to uniquely identify this VRRP group on the Switch. All routers participating in this group must be assigned the same VRID value. This value MUST be different from other VRRP groups set on the Switch.

Interface Name	Enter the name of a previously configured IP interface for which to create a VRRP entry. This IP interface must be assigned to a VLAN on the Switch.
IP Address	Enter the IP address that will be assigned to the VRRP router. This IP address is also the default gateway that will be statically assigned to end hosts and must be set for all routers that participate in this group.
Admin. State	Used to enable (Up) and disable (Down) the VRRP IP interface on the Switch.
Priority (1-254)	Enter a value between 1 and 254 to indicate the router priority. The VRRP Priority value may determine if a higher priority VRRP router overrides a lower priority VRRP router. A higher priority will increase the probability that this router will become the Master router of the group. A lower priority will increase the probability that this router will become the backup router. VRRP routers that are assigned the same priority value will elect the highest physical IP address as the Master router. The default value is 100. (The value of 255 is reserved for the router that owns the IP address associated with the virtual router and is therefore set automatically.)
Advertisement Interval (1-255)	Enter a time interval value, in seconds, for sending VRRP message packets. This value must be consistent with all participating routers. The default is 1 second.
Preempt Mode	This entry will determine the behavior of backup routers within the VRRP group by controlling whether a higher priority backup router will preempt a lower priority Master router. A <i>True</i> entry, along with having the backup router's priority set higher than the masters priority, will set the backup router as the Master router. A <i>False</i> entry will disable the backup router from becoming the Master router. This setting must be consistent with all routers participating within the same VRRP group. The default setting is <i>True</i> .
Critical IP Address	Enter the IP address of the physical device that will provide the most direct route to the Internet or other critical network connections from this virtual router. This must be a real IP address of a real device on the network. If the connection from the virtual router to this IP address fails, the virtual router will automatically disabled. A new Master will be elected from the backup routers participating in the VRRP group. Different critical IP addresses may be assigned to different routers participating in the VRRP group, and can therefore define multiple routes to the Internet or other critical network connections.
Checking Critical IP	Use the pull-down menu to enable or disable the Critical IP address entered above.

Click **Apply** to implement changes made.

To view the settings for a particular VRRP setting, click the corresponding [View](#) in the **VRRP Interface Table** of the entry, which will display the following:

VRRP Virtual Router Entry Display	
VRID	1
Interface Name	System
Authentication type	No Authentication
Virtual IP Address	10.53.13.65
Virtual MAC Address	00:00:5e:00:01:01
Virtual Router State	Initialize
Admin. State	Enabled
Priority	255
Master IP Address	10.53.13.65
Critical IP Address	0.0.0.0
Checking Critical IP	Disabled
Advertisement Interval	1
Preempt Mode	True
Virtual Router Up Time	0
Show All VRRP Interface Entries	

Figure 6- 172. VRRP Virtual Router Settings - Display window

This window displays the following information:

Parameter	Description
VRID	Displays the virtual router ID set by the user. This will uniquely identify the VRRP Interface on the network.
Interface Name	An IP interface name that has been enabled for VRRP. This entry must have been previously set in the IP Interface Settings table.
Authentication type	Displays the type of authentication used to compare VRRP packets received by a virtual router. Possible authentication types include: <ul style="list-style-type: none"> • <i>No authentication</i> - No authentication has been selected to compare VRRP packets received by a virtual router. • <i>Simple Text Password</i> - A <i>Simple</i> password has been selected to compare VRRP packets received by a virtual router, for authentication. • <i>IP Authentication Header</i> - An MD5 message digest algorithm has been selected to compare VRRP packets received by a virtual router, for authentication.
Virtual IP Address	The IP address of the Virtual router configured on the Switch.
Virtual MAC Address	The MAC address of the device that holds the Virtual router.
Virtual Router State	Displays the current status of the virtual router. Possible states include <i>Initialize</i> , <i>Master</i> and <i>Backup</i> .
Admin. State	Displays the current state of the router. <i>Up</i> will be displayed if the virtual router is enabled and <i>Down</i> , if the virtual router is disabled.
Priority	Displays the priority of the virtual router. A higher priority will increase the probability that this router will become the Master router of the group. A lower priority will increase the probability that this router will become the backup router. The lower the number, the higher the priority.
Master IP Address	Displays the IP address of the Master router for the VRRP function.
Critical IP Address	Displays the critical IP address of the VRRP function. This address will judge if a virtual router is qualified to be a master router.
Checking Critical IP	Displays the status of the Critical IP address. May be enabled or disabled.
Advertisement Interval	Displays the time interval, in seconds, which VRRP messages are sent out to the network.
Preempt Mode	Displays the mode for determining the behavior of backup routers set on this VRRP interface. <i>True</i> will denote that this will be the backup router, if the routers priority is set higher than the master router. <i>False</i> will disable the backup router from becoming the master router.
Virtual Router Up Time	Displays the time, in minutes, since the virtual router has been initialized

VRRP Authentication Settings

The **VRRP Authentication Settings** window is used to set the authentication for each Interface configured for VRRP. This authentication is used to identify incoming message packets received by a router. If the authentication is not consistent with incoming packets, they will be discarded. The **Authentication Type** must be consistent with all routers participating within the VRRP group.

To view the following window, click **Configuration > Layer 3 IP Networking > VRRP > VRRP Interface Settings**.

VRRP Interface Settings	
Interface Name	Authentication type
System	No Authentication

Figure 6- 173. VRRP Authentication Settings window

To configure the authentication for a pre-created interface, click its hyperlinked name, revealing the following window to configure:

VRRP Interface Settings	
Interface Name	System
Auth. Type	None
Auth. Data	null
Apply	
Show All VRRP Interface Entries	

Figure 6- 174. VRRP Authentication Settings – Edit window

The following parameters may be viewed or configured:

Parameter	Description
Interface Name	The name of a previously created IP interface for which to configure the VRRP authentication.
Auth. Type	Specifies the type of authentication used. The Auth. Type must be consistent with all routers participating within the VRRP group. The choices are: <ul style="list-style-type: none"> <i>None</i> - Selecting this parameter indicates that VRRP protocol exchanges will not be authenticated. <i>Simple</i> - Selecting this parameter will require the user to set a simple password in the Auth. Data field for comparing VRRP message packets received by a router. If the two passwords are not exactly the same, the packet will be dropped. <i>IP</i> - Selecting this parameter will require the user to set a MD5 message digest for authentication in comparing VRRP messages received by the router. If the two values are inconsistent, the packet will be dropped.
Auth. Data	This field is only valid if the user selects <i>Simple</i> or <i>IP</i> in the Auth.Type field. <ul style="list-style-type: none"> <i>Simple</i> will require the user to enter an alphanumeric string of no more than eight characters to identify VRRP packets received by a router. <i>IP</i> will require the user to enter a MD5 message digest for authentication in comparing VRRP messages received by the router. <p>This entry must be consistent with all routers participating in the same IP interface.</p>

Click **Apply** to implement changes made.

Security Management

Security IP

User Accounts

Access Authentication Control (TACACS)

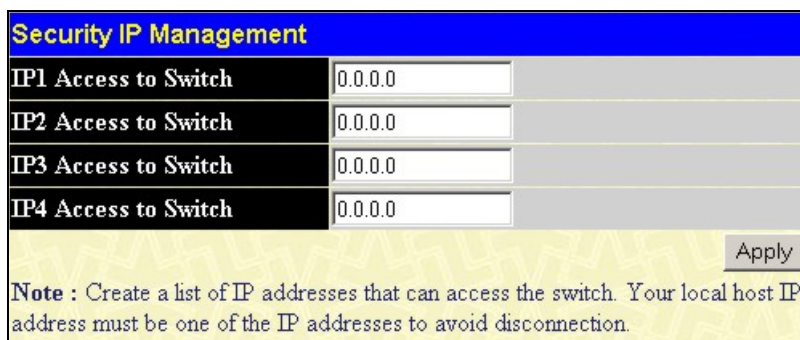
Secure Sockets Layer (SSL)

Secure Shell (SSH)

The following section will aid the user in configuring security functions for the Switch. The Switch includes various functions for security, including *TACACS*, *Security IPs*, *SSL*, and *SSH*, all discussed in detail in the following section.

Security IP

Go to the **Security Management** folder and click on the **Security IP Management** link; the following screen will appear.



Security IP Management	
IP1 Access to Switch	<input type="text" value="0.0.0.0"/>
IP2 Access to Switch	<input type="text" value="0.0.0.0"/>
IP3 Access to Switch	<input type="text" value="0.0.0.0"/>
IP4 Access to Switch	<input type="text" value="0.0.0.0"/>

Note : Create a list of IP addresses that can access the switch. Your local host IP address must be one of the IP addresses to avoid disconnection.

Figure 7- 1. Security IP window

Use the **Security IP Management** to permit remote stations to manage the Switch. If choosing to define one or more designated management stations, only the chosen stations, as defined by IP address, will be allowed management privilege through the web manager or Telnet session. To define a management station IP setting, type in the IP address and click the **Apply** button.

User Account Management

Use the **User Accounts Management** window to control user privileges. To view existing User Accounts, open the **Security Management** folder and click on the **User Account Management** link. This will open the **User Account Management** page, as shown below.



User Account Management	
User Name	Access Right
Darren	Admin

Figure 7- 2. User Account Management window

To add a new user, click on the **Add** button. To modify or delete an existing user, click on the **Modify** button for that user.

Figure 7- 3. User Accounts Modify Table - Add

Add a new user by typing in a **User Name**, and **New Password** and retype the same password in the **Confirm New Password**. Choose the level of privilege (*Admin* or *User*) from the **Access Right** drop-down menu.

Figure 7- 4. User Account Modify Table - Modify

Users may modify or delete an existing user account using the **User Account Modify Table**. To delete the user account, click on the **Delete** button. To change the password, type in the **New Password** and retype it in the **Confirm New Password** entry field. The level of privilege (*Admin* or *User*) can be viewed in the **Access Right** field.

Admin and User Privileges

There are two levels of user privileges, **Admin** and **User**. Some menu selections available to users with **Admin** privileges may not be available to those with **User** privileges.

The following table summarizes the Admin and User privileges:

Management	Admin	User
Configuration	Yes	Read Only
Network Monitoring	Yes	Read Only
Community Strings and Trap Stations	Yes	Read Only
Update Firmware and Configuration Files	Yes	No
System Utilities	Yes	No
Factory Reset	Yes	No
User Account Management		
Add/Update/Delete User Accounts	Yes	No
View User Accounts	Yes	No

Table 7- 1. Admin and User Privileges

After establishing a User Account with Admin-level privileges, be sure to save the changes by opening the **Maintenance** folder, opening the **Save Changes** window and clicking the **Save Configuration** button.

Secure Shell (SSH)

SSH is an abbreviation of *Secure Shell*, which is a program allowing secure remote login and secure network services over an insecure network. It allows a secure login to remote host computers, a safe method of executing commands on a remote end node, and will provide secure encrypted and authenticated communication between two non-trusted hosts. SSH, with its array of unmatched security features is an essential tool in today's networking environment. It is a powerful guardian against numerous existing security hazards that now threaten network communications.

The steps required to use the SSH protocol for secure communication between a remote PC (the SSH client) and the Switch (the SSH server) are as follows:

1. Create a user account with admin-level access using the User Accounts window in the **Security Management** folder. This is identical to creating any other admin-level User Account on the Switch, including specifying a password. This password is used to logon to the Switch, once a secure communication path has been established using the SSH protocol.
2. Configure the User Account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the **SSH User Authentication** window. There are three choices as to the method SSH will use to authorize the user, which are **Host Based**, **Password** and **Public Key**.
3. Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH client and the SSH server, using the **SSH Algorithm** window.
4. Finally, enable SSH on the Switch using the **SSH Configuration** window.

After completing the preceding steps, a SSH Client on a remote PC can be configured to manage the Switch using a secure, in band connection.

SSH Configuration

The following window is used to configure and view settings for the SSH server and can be opened by clicking **Security Management > Secure Shell (SSH) > SSH Configuration**:

Current SSH Configuration Settings	
SSH Server Status	Disabled
Max Session	8
Time Out	120
Auth. Fail	2
Session Rekeying	Never
Ports	22

New SSH Configuration Settings	
SSH Server Status	Disabled ▾
Max Session(1-8)	8
Time Out(120-600)	120
Auth. Fail(2-20)	2
Session Rekeying	Never ▾
Port(1-65535)	22

Figure 7- 5. Current SSH Configuration and New Settings window

To configure the SSH server on the Switch, modify the following parameters and click **Apply**:

Parameter	Description
SSH Server Status	Use the pull-down menu to enable or disable SSH on the Switch. The default is <i>Disabled</i> .
Max Session (1-8)	Enter a value between 1 and 8 to set the number of users that may simultaneously access the Switch. The default setting is 8.
Connection TimeOut (120-600)	Allows the user to set the connection timeout. The use may set a time between 120 and 600 seconds. The default setting is 120 seconds.
Auth. Fail (2-20)	Allows the Administrator to set the maximum number of attempts that a user may try to log on to the SSH Server utilizing the SSH authentication. After the maximum number of attempts has been exceeded, the Switch will be disconnected and the user must reconnect to the Switch to attempt another login. The number of maximum attempts may be set between 2 and 20. The default setting is 2.
Session Rekeying	This field is used to set the time period that the Switch will change the security shell encryptions by using the pull-down menu. The available options are <i>Never</i> , <i>10 min</i> , <i>30 min</i> , and <i>60 min</i> . The default setting is <i>Never</i> .
Port	Enter the virtual port number to be used with this feature. The common port number for SSH is 22.

SSH Algorithm

The SSH Algorithm window allows the configuration of the desired types of SSH algorithms used for authentication encryption. There are three categories of algorithms listed and specific algorithms of each may be enabled or disabled by using their corresponding pull-down menus. All algorithms are enabled by default. To open the following window, click **Security Management > Secure Shell (SSH) > SSH Authentication Mode and Algorithm Settings**:

Encryption Algorithm	
3DES-CBC	Enabled ▾
Blow-fish-CBC	Enabled ▾
AES128-CBC	Enabled ▾
AES192-CBC	Enabled ▾
AES256-CBC	Enabled ▾
Arcfour	Enabled ▾
Cast128-CBC	Enabled ▾
Twofish128	Enabled ▾
Twofish192	Enabled ▾
Twofish256	Enabled ▾
Data Integrity Algorithm	
HMAC-SHA1	Enabled ▾
HMAC-MD5	Enabled ▾
Public Key Algorithm	
HMAC-RSA	Enabled ▾
HMAC-DSA	Enabled ▾
Authentication Algorithm	
Password	Enabled ▾
Publickey	Enabled ▾
Host-based	Enabled ▾
Apply	

Figure 7- 6. SSH Algorithms window

The following algorithms may be set:

Parameter	Description
Encryption Algorithm	
3DES-CBC	Use the pull-down to enable or disable the Triple Data Encryption Standard encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
Blow-fish CBC	Use the pull-down to enable or disable the Blowfish encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
AES128-CBC	Use the pull-down to enable or disable the Advanced Encryption Standard AES128 encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
AES192-CBC	Use the pull-down to enable or disable the Advanced Encryption Standard AES192 encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
AES256-CBC	Use the pull-down to enable or disable the Advanced Encryption Standard AES-256 encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
ARC4	Use the pull-down to enable or disable the Arcfour encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
Cast128-CBC	Use the pull-down to enable or disable the Cast128 encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
Twofish128	Use the pull-down to enable or disable the twofish128 encryption algorithm. The default is <i>Enabled</i> .
Twofish192	Use the pull-down to enable or disable the twofish192 encryption algorithm. The default is <i>Enabled</i> .
Twofish256	Use the pull-down to enable or disable the twofish256 encryption algorithm. The default is <i>Enabled</i> .
Data Integrity Algorithm	
HMAC-SHA1	Use the pull-down to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Secure Hash algorithm. The default is <i>Enabled</i> .
HMAC-MD5	Use the pull-down to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the MD5 Message Digest encryption algorithm. The default is <i>Enabled</i> .
Public Key Algorithm	
HMAC-RSA	Use the pull-down to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the RSA encryption algorithm. The default is <i>Enabled</i> .
HMAC-DSA	Use the pull-down to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Digital Signature Algorithm (DSA) encryption. The default is <i>Enabled</i> .
Authentication Algorithm	
Password	This field may be enabled or disabled to choose if the administrator wishes to use a locally configured password for authentication on the Switch. This field is <i>Enabled</i> by default.
Public Key	This field may be enabled or disabled to choose if the administrator wishes to use a publickey configuration set on a SSH server, for authentication. This field is <i>Enabled</i> by default.
Host-based	This field may be enabled or disabled to choose if the administrator wishes to use a host computer for authentication. This parameter is intended for Linux users requiring SSH authentication techniques and the host computer is running the Linux operating system with a SSH program previously installed. This field is <i>Enabled</i> by default.

Click **Apply** to implement changes made.

SSH User Authentication Mode

The following windows are used to configure parameters for users attempting to access the Switch through SSH. To access the following window, click **Security Management > Secure Shell > SSH User Authentication**.

Current Accounts			
User Name	Auth. Mode	Host Name	Host IP
Darren	Password		

Figure 7- 7. Current Accounts window

In the example screen above, the User Account “Darren” has been previously set using the User Accounts window in the **Security Management** folder. A User Account **MUST** be set in order to set the parameters for the SSH user. To configure the parameters for a SSH user, click on the hyperlinked **User Name** in the **Current Accounts** window, which will reveal the following window to configure.

User Name	Darren
Auth. Mode	Password
Host Name	
Host IP	<input type="checkbox"/> 0.0.0.0
Apply	
Show All User Authentication Entries	

Figure 7- 8. SSH User window

The user may set the following parameters:

Parameter	Description
User Name	Enter a User Name of no more than 15 characters to identify the SSH user. This User Name must be a previously configured user account on the Switch.
Auth. Mode	<p>The administrator may choose one of the following to set the authorization for users attempting to access the Switch.</p> <p><i>Host Based</i> – This parameter should be chosen if the administrator wishes to use a remote SSH server for authentication purposes. Choosing this parameter requires the user to input the following information to identify the SSH user.</p> <ul style="list-style-type: none"> <i>Host Name</i> – Enter an alphanumeric string of no more than 32 characters to identify the remote SSH user. <i>Host IP</i> – Enter the corresponding IP address of the SSH user. <p><i>Password</i> – This parameter should be chosen if the administrator wishes to use an administrator-defined password for authentication. Upon entry of this parameter, the Switch will prompt the administrator for a password, and then to re-type the password for confirmation.</p> <p><i>Public Key</i> – This parameter should be chosen if the administrator wishes to use the publickey on a SSH server for authentication.</p>
Host Name	Enter an alphanumeric string of no more than 32 characters to identify the remote SSH user. This parameter is only used in conjunction with the <i>Host Based</i> choice in the Auth. Mode field.
Host IP	Enter the corresponding IP address of the SSH user. This parameter is only used in conjunction with the <i>Host Based</i> choice in the Auth. Mode field.

Click **Apply** to implement changes made.



NOTE: To set the **SSH User Authentication** parameters on the Switch, a User Account must be previously configured. For more information on configuring local User Accounts on the Switch, see the **User Accounts** section of this manual located in this section.

Access Authentication Control

The TACACS / XTACACS / TACACS+ / RADIUS commands allows secure access to the Switch using the TACACS / XTACACS / TACACS+ / RADIUS protocols. When a user logs in to the Switch or tries to access the administrator level privilege, he or she is prompted for a password. If TACACS / XTACACS / TACACS+ / RADIUS authentication is enabled on the Switch, it will contact a TACACS / XTACACS / TACACS+ / RADIUS server to verify the user. If the user is verified, he or she is granted access to the Switch.

There are currently three versions of the TACACS security protocol, each a separate entity. The Switch's software supports the following versions of TACACS:

- **TACACS** (Terminal Access Controller Access Control System) - Provides password checking and authentication, and notification of user actions for security purposes utilizing via one or more centralized TACACS servers, utilizing the UDP protocol for packet transmission.
- **Extended TACACS (XTACACS)** - An extension of the TACACS protocol with the ability to provide more types of authentication requests and more types of response codes than TACACS. This protocol also uses UDP to transmit packets.
- **TACACS+ (Terminal Access Controller Access Control System plus)** - Provides detailed access control for authentication for network devices. TACACS+ is facilitated through Authentication commands via one or more centralized servers. The TACACS+ protocol encrypts all traffic between the Switch and the TACACS+ daemon, using the TCP protocol to ensure reliable delivery

In order for the TACACS / XTACACS / TACACS+ / RADIUS security function to work properly, a TACACS / XTACACS / TACACS+ / RADIUS server must be configured on a device other than the Switch, called an Authentication Server Host and it must include usernames and passwords for authentication. When the user is prompted by the Switch to enter usernames and passwords for authentication, the Switch contacts the TACACS / XTACACS / TACACS+ / RADIUS server to verify, and the server will respond with one of three messages:

- The server verifies the username and password, and the user is granted normal user privileges on the Switch.
- The server will not accept the username and password and the user is denied access to the Switch.
- The server doesn't respond to the verification query. At this point, the Switch receives the timeout from the server and then moves to the next method of verification configured in the method list.

The Switch has four built-in **Authentication Server Groups**, one for each of the TACACS, XTACACS, TACACS+ and RADIUS protocols. These built-in Authentication Server Groups are used to authenticate users trying to access the Switch. The users will set **Authentication Server Hosts** in a preferable order in the built-in Authentication Server Groups and when a user tries to gain access to the Switch, the Switch will ask the first Authentication Server Hosts for authentication. If no authentication is made, the second server host in the list will be queried, and so on. The built-in Authentication Server Groups can only have hosts that are running the specified protocol. For example, the TACACS Authentication Server Groups can only have TACACS Authentication Server Hosts.

The administrator for the Switch may set up six different authentication techniques per user-defined method list (TACACS / XTACACS / TACACS+ / RADIUS / local / none) for authentication. These techniques will be listed in an order preferable, and defined by the user for normal user authentication on the Switch, and may contain up to eight authentication techniques. When a user attempts to access the Switch, the Switch will select the first technique listed for authentication. If the first technique goes through its Authentication Server Hosts and no authentication is returned, the Switch will then go to the next technique listed in the server group for authentication, until the authentication has been verified or denied, or the list is exhausted.

Please note that users granted access to the Switch will be granted normal user privileges on the Switch. To gain access to administrator level privileges, the user must access the **Enable Admin** window and then enter a password, which was previously configured by the administrator of the Switch.



NOTE: TACACS, XTACACS and TACACS+ are separate entities and are not compatible. The Switch and the server must be configured exactly the same, using the same protocol. (For example, if the Switch is set up for TACACS authentication, so must be the host server.)

Authentication Policy & Parameters

This command will enable an administrator-defined authentication policy for users trying to access the Switch. When enabled, the device will check the **Login Method List** and choose a technique for user authentication upon login.

To access the following window, click **Security Management > Access Authentication Control > Authentication Policy & Parameter Settings**:

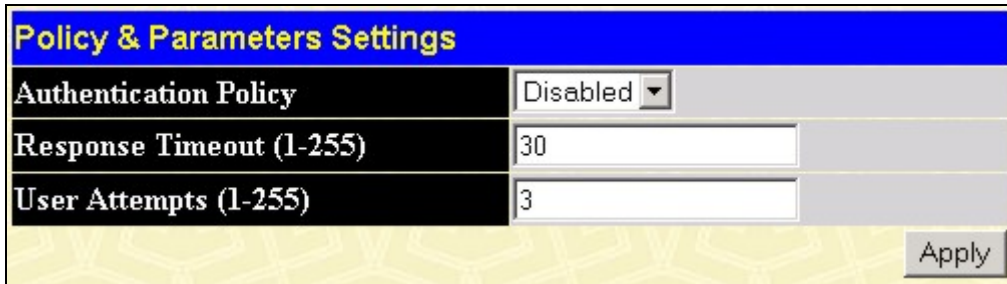


Figure 7- 9. Authentication Policy and Parameter Settings window

The following parameters can be set:

Parameters	Description
Authentication Policy	Use the pull down menu to enable or disable the Authentication Policy on the Switch.
Response Timeout (1-255)	This field will set the time the Switch will wait for a response of authentication from the user. The user may set a time between 1 and 255 seconds. The default setting is 30 seconds.
User Attempts (1-255)	This command will configure the maximum number of times the Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the Switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. TELNET and web users will be disconnected from the Switch. The user may set the number of attempts from 1 to 255. The default setting is 3.

Click **Apply** to implement changes made.

Application's Authentication Settings

This window is used to configure switch configuration applications (console, Telnet, SSH, web) for login at the user level and at the administration level (**Enable Admin**) utilizing a previously configured method list. To view the following window, click **Security Management > Access Authentication Control > Application Authentication Settings**:

Application's authentication settings		
Application	Login Method List	Enable Method List
Console	default ▾	default ▾
Telnet	default ▾	default ▾
SSH	default ▾	default ▾
HTTP	default ▾	default ▾
		Apply

Figure 7- 10. Application's Authentication Settings window

The following parameters can be set:

Parameter	Description
Application	Lists the configuration applications on the Switch. The user may configure the Login Method List and Enable Method List for authentication for users utilizing the Console (Command Line Interface) application, the Telnet application, SSH and the Web (HTTP) application.
Login Method List	Using the pull down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user. See the Login Method Lists window, in this section, for more information.
Enable Method List	Using the pull down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user. See the Enable Method Lists window, in this section, for more information.

Click **Apply** to implement changes made.

Authentication Server Group

This window will allow users to set up *Authentication Server Groups* on the Switch. A server group is a technique used to group TACACS/XTACACS/TACACS+/RADIUS server hosts into user-defined categories for authentication using method lists. The user may define the type of server group by protocol or by previously defined server group. The Switch has three built-in Authentication Server Groups that cannot be removed but can be modified. Up to eight authentication server hosts may be added to any particular group.

To view the following window, click **Security Management > Access Authentication Control > Authentication Server Group**:

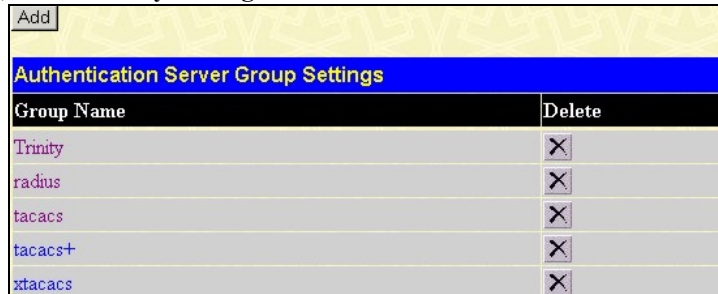


Figure 7- 11. Authentication Server Group window

This screen displays the Authentication Server Groups on the Switch. The Switch has four built-in Authentication Server Groups that cannot be removed but can be modified. To modify a particular group, click its hyperlinked **Group Name**, which will then display the following window.

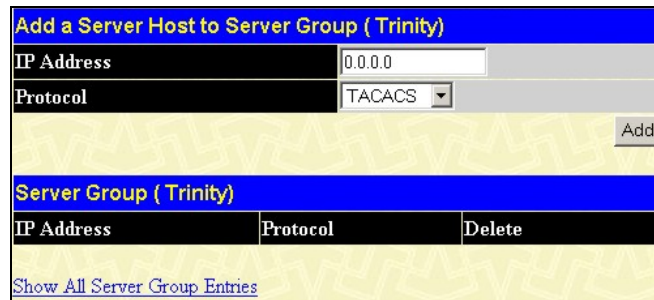


Figure 7- 12. Add a Server Host to Server Group (XTACACS) window.

To add an Authentication Server Host to the list, enter its IP address in the IP Address field, choose the protocol associated with the IP address of the Authentication Server Host and click **Add** to add this Authentication Server Host to the group.

To add a server group other than the ones listed, click the add button, revealing the following window to configure.

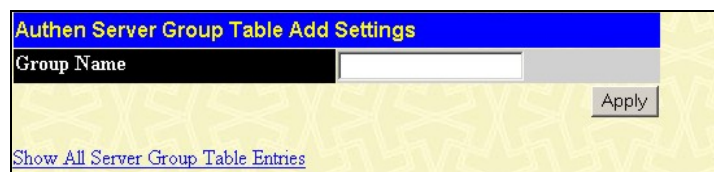


Figure 7- 13. Authentication Server Group Table Add Settings window

Enter a group name of up to 15 characters into the **Group Name** field and click **Apply**. The entry should appear in the **Authentication Server Group Settings** window, as shown in Figure 8-12 (Trinity).



NOTE: The user must configure Authentication Server Hosts using the Authentication Server Hosts window before adding hosts to the list. Authentication Server Hosts must be configured for their specific protocol on a remote centralized server before this function can work properly.

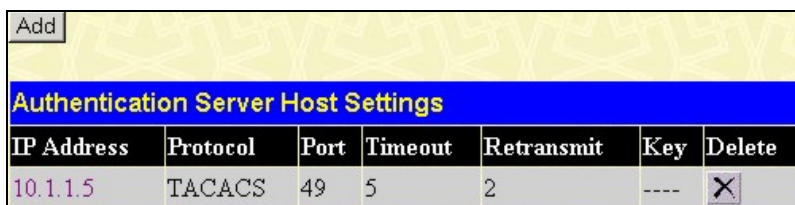


NOTE: The three built in server groups can only have server hosts running the same TACACS daemon. TACACS/XTACACS/TACACS+ protocols are separate entities and are not compatible with each other.

Authentication Server Host

This window will set user-defined *Authentication Server Hosts* for the TACACS / XTACACS / TACACS+ / RADIUS security protocols on the Switch. When a user attempts to access the Switch with Authentication Policy enabled, the Switch will send authentication packets to a remote TACACS / XTACACS / TACACS+ / RADIUS server host on a remote host. The TACACS / XTACACS / TACACS+ / RADIUS server host will then verify or deny the request and return the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS / XTACACS / TACACS+ / RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.

To view the following window, click **Security Management > Access Authentication Control > Authentication Server Host**:



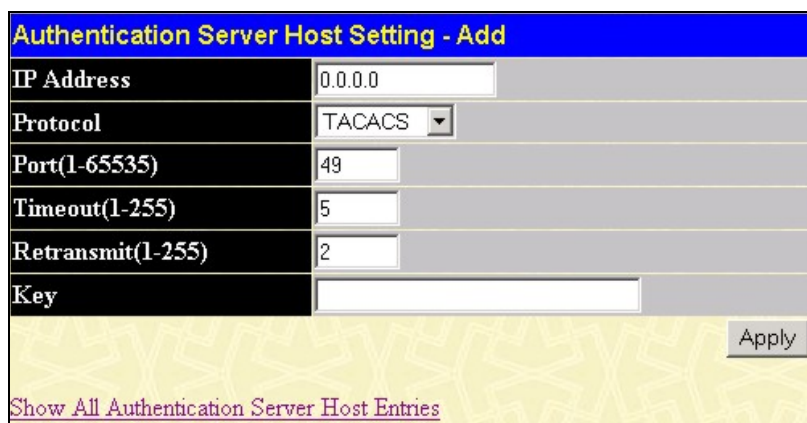
IP Address	Protocol	Port	Timeout	Retransmit	Key	Delete
10.1.1.5	TACACS	49	5	2	----	X

Figure 7- 14. Authentication Server Host window

To add an Authentication Server Host, click the **Add** button, revealing the following window:



NOTE: More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+ are separate entities and are not compatible with each other



Authentication Server Host Setting - Add	
IP Address	0.0.0.0
Protocol	TACACS
Port(1-65535)	49
Timeout(1-255)	5
Retransmit(1-255)	2
Key	
Apply	
Show All Authentication Server Host Entries	

Figure 7- 15. Authentication Server Host Setting - Add window

Configure the following parameters to add an Authentication Server Host:

Parameter	Description
IP Address	The IP address of the remote server host to add.
Protocol	The protocol used by the server host. The user may choose one of the following: <ul style="list-style-type: none"> <i>TACACS</i> - Enter this parameter if the server host utilizes the TACACS protocol. <i>XTACACS</i> - Enter this parameter if the server host utilizes the XTACACS protocol. <i>TACACS+</i> - Enter this parameter if the server host utilizes the TACACS+ protocol. <i>RADIUS</i> - Enter this parameter if the server host utilizes the RADIUS protocol.
Port (1-65535)	Enter a number between 1 and 65535 to define the virtual port number of the authentication protocol on a server host. The default port number is 49 for TACACS/XTACACS/TACACS+ servers and 1813 for RADIUS servers but the user may set a unique port number for higher security.
Timeout (1-255)	Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is 5 seconds.
Retransmit (1-255)	Enter the value in the retransmit field to change how many times the device will resend an authentication request when the TACACS server does not respond.
Key	Authentication key to be shared with a configured TACACS+ or RADIUS servers only. Specify an alphanumeric string up to 254 characters.

Click **Apply** to add the server host.

Login Method Lists

This command will configure a user-defined or default **Login Method List** of authentication techniques for users logging on to the Switch. The sequence of techniques implemented in this command will affect the authentication result. For example, if a user enters a sequence of techniques, for example TACACS - XTACACS- local, the Switch will send an authentication request to the first TACACS host in the server group. If no response comes from the server host, the Switch will send an authentication request to the second TACACS host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, XTACACS. If no authentication takes place using the XTACACS list, the local account database set in the Switch is used to authenticate the user. When the local method is used, the privilege level will be dependant on the local account privilege configured on the Switch.

Successful login using any of these techniques will give the user a "User" privilege only. If the user wishes to upgrade his or her status to the administrator level, the user must use the **Enable Admin** window, in which the user must enter a previously configured password, set by the administrator. (See the **Enable Admin** part of this section for more detailed information concerning the **Enable Admin** command.)

To view the following screen click **Security Management > Access Authentication Control > Login Method Lists:**

Login Method List Settings					
Method List Name	Method 1	Method 2	Method 3	Method 4	Delete
default	local				X

Figure 7- 16. Login Method List Settings window

The Switch contains one **Method List** that is set and cannot be removed, yet can be modified. To delete a Login Method List defined by the user, click the **X** under the **Delete** heading corresponding to the entry desired to be deleted. To modify a Login Method List, click on its hyperlinked **Method List Name**. To configure a new Method List, click the **Add** button.

Both actions will result in the same screen to configure:

Figure 7- 17. Login Method List - Edit window (default)

Figure 7- 18. Login Method List – Add window

To define a Login Method List, set the following parameters and click **Apply**:

Parameter	Description
Method List Name	Enter a method list name defined by the user of up to 15 characters.
Method 1, 2, 3, 4	<p>The user may add one, or a combination of up to four (4) of the following authentication methods to this method list:</p> <ul style="list-style-type: none"> • <i>tacacs</i> - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server. • <i>xtacacs</i> - Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server. • <i>tacacs+</i> - Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server. • <i>radius</i> - Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server. • <i>server_group</i> - Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch. • <i>local</i> - Adding this parameter will require the user to be authenticated using the local user account database on the Switch. • <i>none</i> - Adding this parameter will require no authentication to access the Switch.

Enable Method Lists

The *Enable Method Lists* window is used to set up Method Lists to promote users with user level privileges to Administrator (Admin) level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight (8) Enable Method Lists can be implemented on the Switch, one of which is a default Enable Method List. This default Enable Method List cannot be deleted but can be configured.

The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like TACACS - XTACACS - Local Enable, the Switch will send an authentication request to the first TACACS host in the server group. If no verification is found, the Switch will send an authentication request to the second TACACS host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, XTACACS. If no authentication takes place using the XTACACS list, the Local Enable password set in the Switch is used to authenticate the user.

Successful authentication using any of these methods will give the user an "Admin" privilege.




NOTE: To set the Local Enable Password, see the next section, entitled Local Enable Password.

To view the following table, click **Security Management > Access Authentication Control > Enable Method Lists**:

Add					
Enable Method List Settings					
Method List Name	Method 1	Method 2	Method 3	Method 4	Delete
default	local_enable				

Figure 7- 19. Enable Method List Settings window

To delete an Enable Method List defined by the user, click the  under the **Delete** heading corresponding to the entry desired to be deleted. To modify an Enable Method List, click on its hyperlinked **Method List Name**. To configure a Method List, click the **Add** button.

Both actions will result in the same screen to configure:

Figure 7- 20. Enable Method List - Edit window

Figure 7- 21. Enable Method List - Add window

To define an Enable Login Method List, set the following parameters and click **Apply**:

Parameter	Description
Method List Name	Enter a method list name defined by the user of up to 15 characters.
Method 1, 2, 3, 4	<p>The user may add one, or a combination of up to four (4) of the following authentication methods to this method list:</p> <ul style="list-style-type: none"> • <i>local_enable</i> - Adding this parameter will require the user to be authenticated using the local enable password database on the Switch. The local enable password must be set by the user in the next section entitled Local Enable Password. • <i>none</i> - Adding this parameter will require no authentication to access the Switch. • <i>radius</i> - Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server. • <i>tacacs</i> - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server. • <i>xtacacs</i> - Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server. • <i>tacacs+</i> - Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server. • <i>server_group</i> - Adding a previously configured server group will require the user to be authenticated using a user-defined server group previously configured on the Switch.

Local Enable Password

This window will configure the locally enabled password for the **Enable Admin** command. When a user chooses the "local_enable" method to promote user level privileges to administrator privileges, he or she will be prompted to enter the password configured here that is locally set on the Switch.

To view the following window, click **Security Management > Access Authentication Control > Local Enable Password**:

Figure 7- 22. Configure Local Enable Password window

To set the Local Enable Password, set the following parameters and click **Apply**.

Parameter	Description
Old Local Enable	If a password was previously configured for this entry, enter it here in order to change it to a new password
New Local Enable	Enter the new password that you wish to set on the Switch to authenticate users attempting to access Administrator Level privileges on the Switch. The user may set a password of up to 15 characters.
Confirm Local Enable	Confirm the new password entered above. Entering a different password here from the one set in the New Local Enabled field will result in a fail message.

Click **Apply** to implement changes made.

Enable Admin

The **Enable Admin** window is for users who have logged on to the Switch on the normal user level, and wish to be promoted to the administrator level. After logging on to the Switch, users will have only user level privileges. To gain access to administrator level privileges, the user will open this window and will have to enter an authentication password. Possible authentication methods for this function include TACACS/XTACACS/TACACS+/RADIUS, user defined server groups, local enable (local account on the Switch), or no authentication (none). Because XTACACS and TACACS do not support the enable function, the user must create a special account on the server host, which has the username "enable", and a password configured by the administrator that will support the "enable" function. This function becomes inoperable when the authentication policy is disabled.

To view the following window, click **Security Management > Access Authentication Control > Enable Admin**:

Figure 7- 23. Enable Admin Screen

When this screen appears, click the **Enable Admin** button revealing a window for the user to enter authentication (password, username), as seen below. A successful entry will promote the user to Administrator level privileges on the Switch.



Figure 7- 24. Enter Network Password window

Secure Socket Layer (SSL)

Secure Sockets Layer or SSL is a security feature that will provide a secure communication path between a host and client through the use of authentication, digital signatures and encryption. These security functions are implemented through the use of a *ciphersuite*, which is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session and consists of three levels:

1. **Key Exchange:** The first part of the cyphersuite string specifies the public key algorithm to be used. This switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the *DHE DSS* Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and host as they “exchange keys” in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.
2. **Encryption:** The second part of the ciphersuite that includes the encryption used for encrypting the messages sent between client and host. The Switch supports two types of cryptology algorithms:
 - Stream Ciphers – There are two types of stream ciphers on the Switch, *RC4 with 40-bit keys* and *RC4 with 128-bit keys*. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.
 - CBC Block Ciphers – CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The Switch supports the *3DES EDE* encryption code defined by the Data Encryption Standard (DES) to create the encrypted text.
3. **Hash Algorithm:** This part of the ciphersuite allows the user to choose a message digest function which will determine a Message Authentication Code. This Message Authentication Code will be encrypted with a sent message to provide integrity and prevent against replay attacks. The Switch supports two hash algorithms, *MD5* (Message Digest 5) and *SHA* (Secure Hash Algorithm).

These three parameters are uniquely assembled in four choices on the Switch to create a three-layered encryption code for secure communication between the server and the host. The user may implement any one or combination of the ciphersuites available, yet different ciphersuites will affect the security level and the performance of the secured connection. The information included in the ciphersuites is not included with the Switch and requires downloading from a third source in a file form called a *certificate*. This function of the Switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the Switch by utilizing a TFTP server. The Switch supports SSLv3. Other versions of SSL may not be compatible with this Switch and may cause problems upon authentication and transfer of messages from client to host.

Download Certificate

This window is used to download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. The Switch only supports certificate files with .der file extensions. Currently, all xStack® DES-6500 chassis switch come with a certificate pre-loaded though the user may need to download more, depending on user circumstances.

To view the following window, click **Security Management > Secure Socket Layer (SSL) > Download Certificate:**



Figure 7- 25. Download Certificate window

To download certificates, set the following parameters and click **Apply**.

Parameter	Description
Server IP	Enter the IP address of the TFTP server where the certificate files are located.

Certificate File Name	Enter the path and the filename of the certificate file to download. This file must have a .der extension. (Ex. c:/cert.der)
Key File Name	Enter the path and the filename of the key file to download. This file must have a .der extension (Ex. c:/pkey.der)

Click **Apply** to implement changes made.

Configuration

This screen will allow the user to enable SSL on the Switch and implement any one or combination of listed ciphersuites on the Switch. A *ciphersuite* is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The Switch possesses four possible ciphersuites for the SSL function, which are all enabled by default. To utilize a particular ciphersuite, disable the unwanted ciphersuites, leaving the desired one for authentication.

When the SSL function has been enabled, the web will become disabled. To manage the Switch through the web based management while utilizing the SSL function, the web browser must support SSL encryption and the header of the URL must begin with https://. (Ex. https://10.90.90.90) Any other method will result in an error and no access can be authorized for the web-based management.

To view the following window, click **Security Management > Secure Socket Layer (SSL) > Configuration**:

The screenshot shows the 'SSL Configuration' window. It has a blue header with the title 'SSL Configuration'. Below the header is a section titled 'Ciphersuite' with a blue background. This section contains four rows, each with a ciphersuite name, a status dropdown menu, and a hexadecimal value:

RSA with RC4 128 MD5	Enabled	0x0004
RSA with 3DES EDE CBC SHA	Enabled	0x000a
DHE DSS with 3DES EDE CBC SHA	Enabled	0x0013
RSA EXPORT with RC4 40 MD5	Enabled	0x0003

Below the ciphersuite section is another section titled 'Configuration' with a blue background. It contains two rows:

Cache Timeout(60-86400 sec)	600
SSL Status	Disabled

At the bottom right of the window is an 'Apply' button.

Figure 7- 26. Ciphersuite window

To set up the SSL function on the Switch, configure the following parameters and click **Apply**.

Parameter	Description
Ciphersuite	
RSA with RC4 128 MD5	This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. Use the pull down menu to enable or disable this ciphersuite. This field is <i>Enabled</i> by default.
RSA with 3DES EDE CBC SHA	This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. Use the pull down menu to enable or disable this ciphersuite. This field is <i>Enabled</i> by default.
DHS DSS with 3DES EDE CBC SHA	This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. Use the pull down menu to enable or disable this ciphersuite. This field is <i>Enabled</i> by default.
RSA EXPORT with RC4 40 MD5	This ciphersuite combines the RSA Export key exchange and stream cipher RC4 encryption with 40-bit keys. Use the pull down menu to enable or disable this ciphersuite. This field is <i>Enabled</i> by default.

Configuration

SSL Status	Use the pull down menu to enable or disable the SSL status on the switch. The default is <i>Disabled</i> .
Cache Timeout (60-86400)	This field will set the time between a new key exchange between a client and a host using the SSL function. A new SSL session is established every time the client and host go through a key exchange. Specifying a longer timeout will allow the SSL session to reuse the master key on future connections with that particular host, therefore speeding up the negotiation process. The default setting is 600 seconds.



NOTE: Certain implementations concerning the function and configuration of SSL are not available on the web-based management of this Switch and need to be configured using the command line interface. For more information on SSL and its functions, see the **xStack® DES-6500 Modular Layer 3 Chassis Ethernet Switch CLI**, located on the documentation CD of this product.



NOTE: Enabling the SSL command will disable the web-based switch management. To log on to the Switch again, the header of the URL must begin with `https://`. Entering anything else into the address field of the web browser will result in an error and no authentication will be granted.

SNMP Manager

SNMP Settings

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the Switch, switch group or network.

Managed devices that support SNMP include software (referred to as an agent), which runs locally on the device. A defined set of variables (managed objects) is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The xStack[®] DES-6500 chassis switch supports the SNMP versions 1, 2c, and 3. You can specify which version of the SNMP you want to use to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

In SNMP v.1 and v.2c, user authentication is accomplished using 'community strings', which function like passwords. The remote user SNMP application and the Switch SNMP must use the same community string. SNMP packets from any station that has not been authenticated are ignored (dropped).

The default community strings for the Switch used for SNMP v.1 and v.2c management access are:

public - Allows authorized management stations to retrieve MIB objects.

private - Allows authorized management stations to retrieve and modify MIB objects.

SNMPv3 uses a more sophisticated authentication process that is separated into two parts. The first part is to maintain a list of users and their attributes that are allowed to act as SNMP managers. The second part describes what each user on that list can do as an SNMP manager.

The Switch allows groups of users to be listed and configured with a shared set of privileges. The SNMP version may also be set for a listed group of SNMP managers. Thus, you may create a group of SNMP managers that are allowed to view read-only information or receive traps using SNMPv1 while assigning a higher level of security to another group, granting read/write privileges using SNMPv3.

Using SNMPv3 individual users or groups of SNMP managers can be allowed to perform or be restricted from performing specific SNMP management functions. The functions allowed or restricted are defined using the Object Identifier (OID) associated with a specific MIB. An additional layer of security is available for SNMPv3 in that SNMP messages may be encrypted. To read more about how to configure SNMPv3 settings for the Switch read the next section.

Traps

Traps are messages that alert network personnel 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 trap recipient (or network manager). Typical traps include trap messages for Authentication Failure, Topology Change and New Root.

MIBs

Management and counter information are stored by 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. The proprietary MIB may also be retrieved by specifying the MIB Object Identifier. MIB values can be either read-only or read-write.

The xStack[®] DES-6500 chassis switch incorporates a flexible SNMP management for the switching environment. SNMP management can be customized to suit the needs of the networks and the preferences of the network administrator. Use the SNMP V3 menus to select the SNMP version used for specific tasks.

The xStack[®] DES-6500 chassis switch supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. The administrator can specify the SNMP version used to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

SNMP settings are configured using the menus located on the SNMP V3 folder of the web manager. Workstations on the network that are allowed SNMP privileged access to the Switch can be restricted with the Management Station IP Address menu.

SNMP Trap Settings

The following window is used to enable or disable SNMP traps on the Switch. There are two types of traps located on the Switch, SNMP traps and SNMP Authenticate traps which the user may enable or disable by using the corresponding pull-down menu. After changes are made, click the **Apply** button to save it to the Switch's memory.

The image shows a web interface window titled "SNMP Trap Settings". It contains two rows of settings. The first row is "Traps State" with a dropdown menu set to "Enabled". The second row is "Authenticate Traps State" with a dropdown menu also set to "Enabled". At the bottom right of the window is an "Apply" button.

Figure 8 - 1. SNMP Trap Settings window

SNMP User Table

The **SNMP User Table** displays all of the SNMP users currently configured on the Switch.

In the **SNMP Manager** folder, click on the **SNMP User Table** link. This will open the **SNMP User Table**, as shown below.

The image shows a web interface window titled "SNMP User Table". At the top left is an "Add" button. Below it, the text "Total Entries: 1 (Note: Maximum of 10 entries.)" is displayed. The main content is a table with the following structure:

User Name	Group Name	SNMP Version	Delete
initial	initial	V3	<input type="checkbox"/>

Figure 8 - 2. SNMP User Table

To delete an existing SNMP User Table entry, click the below the **Delete** heading corresponding to the entry to delete.

To display the detailed entry for a given user, click on the hyperlinked User Name. This will open the **SNMP User Table Display** page, as shown below.

The image shows a web interface window titled "SNMP User Table Display". It displays the following details:

User Name	initial
Group Name	initial
SNMP Version	V3
Auth-Protocol	None
Priv-Protocol	None

At the bottom of the window is a link: [Show All SNMP User Table Entries](#)

Figure 8 - 3. SNMP User Table Display

The following parameters are displayed:

Parameter	Description
User Name	An alphanumeric string of up to 32 characters. This is used to identify the SNMP users.
Group Name	This name is used to specify the SNMP group created can request SNMP messages.

SNMP Version	V1 - Indicates that SNMP version 1 is in use. V2 - Indicates that SNMP version 2 is in use. V3 - Indicates that SNMP version 3 is in use.
Auth-Protocol	None - Indicates that no authentication protocol is in use. MD5 - Indicates that the HMAC-MD5-96 authentication level will be used. SHA - Indicates that the HMAC-SHA authentication protocol will be used.
Priv-Protocol	None - Indicates that no privacy (encryption) protocol is in use. DES - Indicates that DES 56-bit encryption is in use based on the CBC-DES (DES-56) standard.

To return to the **SNMP User Table**, click the [Show All SNMP User Table Entries](#) link.

To add a new entry to the **SNMP User Table Configuration**, click on the **Add** button on the **SNMP User Table** page. This will open the **SNMP User Table Configuration** page, as shown below.

Figure 8 - 4. SNMP User Table Configuration window

The following parameters can set:

Parameter	Description
User Name	Enter an alphanumeric string of up to 32 characters. This is used to identify the SNMP user.
Group Name	This name is used to specify the SNMP group created can request SNMP messages.
SNMP Version	V1 - Specifies that SNMP version 1 will be used. V2 - Specifies that SNMP version 2 will be used. V3 - Specifies that SNMP version 3 will be used.
Method	This field only becomes possible to configure when the encrypted check box is clicked in the following field. This field requires the user to choose the type of encryption to be employed for this SNMP user. The user may choose: <i>By Password</i> – Requires the SNMP user to enter a password for authentication and privacy. The password is defined by specifying the auth password below. This method is recommended. <i>By Key</i> - Requires the SNMP user to enter a encryption key for authentication and privacy. The key is defined by specifying the key in hex form below. This method is not recommended.

Auth-Protocol	<p><i>MD5</i> - Specifies that the HMAC-MD5-96 authentication level will be used. This field is only operable when <i>V3</i> is selected in the SNMP Version field and the Encrypted field has been checked. This field will require the user to enter a password.</p> <p><i>SHA</i> - Specifies that the HMAC-SHA authentication protocol will be used. This field is only operable when <i>V3</i> is selected in the SNMP Version field and the Encrypted field has been checked. This field will require the user to enter a password.</p>
Priv-Protocol	<p><i>None</i> - indicates that no privacy (encryption) protocol is in use.</p> <p><i>DES</i> - Specifies that DES 56-bit encryption is in use, based on the CBC-DES (DES-56) standard. This field is only operable when <i>V3</i> is selected in the SNMP Version field and the Encrypted field has been checked. This field will require the user to enter a password between 8 and 16 alphanumeric characters.</p>
Encrypted	Checking the corresponding box will enable encryption for SNMP V3 and is only operable in SNMP V3 mode.

To implement changes made, click **Apply**. To return to the **SNMP User Table**, click the [Show All SNMP User Table Entries](#) link.

SNMP View Table

The SNMP View Table is used to assign views to community strings that define which MIB objects can be accessed by a remote SNMP manager. To view the **SNMP View Table**, open the **SNMP Manager** folder and click the **SNMP View Table** entry. The following screen should appear:

SNMP View Table			
View Name	Subtree	View Type	Delete
restricted	1.3.6.1.2.1.1	Included	X
restricted	1.3.6.1.2.1.11	Included	X
restricted	1.3.6.1.6.3.10.2.1	Included	X
restricted	1.3.6.1.6.3.11.2.1	Included	X
restricted	1.3.6.1.6.3.15.1.1	Included	X
CommunityView	1	Included	X
CommunityView	1.3.6.1.6.3	Excluded	X
CommunityView	1.3.6.1.6.3.1	Included	X

Figure 8- 5. SNMP View Table

To delete an existing **SNMP View Table** entry, click the **X** in the **Delete** column corresponding to the entry to delete. To create a new entry, click the **Add** button and a separate menu will appear.

SNMP View Table Configuration	
View Name	<input type="text"/>
Subtree OID	<input type="text"/>
View Type	Included <input type="button" value="v"/>
<input type="button" value="Apply"/>	
Show All SNMP View Table Entries	

Figure 8 - 6. SNMP View Table Configuration window

The SNMP Group created with this table maps SNMP users (identified in the **SNMP User Table**) to the views created in the previous menu.

The following parameters can set:

Parameter	Description
View Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP view being created.
Subtree OID	Type the Object Identifier (OID) Subtree for the view. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.
View Type	Select Included to include this object in the list of objects that an SNMP manager can access. Select Excluded to exclude this object from the list of objects that an SNMP manager can access.

To implement your new settings, click **Apply**. To return to the **SNMP View Table**, click the [Show All SNMP View Table Entries](#) link.

SNMP Group Table

An SNMP Group created with this table maps SNMP users (identified in the SNMP User Table) to the views created in the previous menu. To view the **SNMP Group Table**, open the **SNMP Manager** folder and click the **SNMP Group Table** entry. The following screen should appear:

SNMP Group Table			
Group Name	Security Model	Security Level	Delete
public	SNMPv1	NoAuthNoPriv	X
public	SNMPv2	NoAuthNoPriv	X
initial	SNMPv3	NoAuthNoPriv	X
private	SNMPv1	NoAuthNoPriv	X
private	SNMPv2	NoAuthNoPriv	X
ReadGroup	SNMPv1	NoAuthNoPriv	X
ReadGroup	SNMPv2	NoAuthNoPriv	X
WriteGroup	SNMPv1	NoAuthNoPriv	X
WriteGroup	SNMPv2	NoAuthNoPriv	X

Figure 8- 7. SNMP Group Table

To delete an existing **SNMP Group Table** entry, click the corresponding **X** under the **Delete** heading.

To display the current settings for an existing **SNMP Group Table** entry, click the hyperlink for the entry under the **Group Name**.

SNMP Group Table Display	
Group Name	public
Read View Name	CommunityView
Write View Name	
Notify View Name	CommunityView
Security Model	SNMPv1
Security Level	NoAuthNoPriv
Show All SNMP Group Table Entries	

Figure 8 - 8. SNMP Group Table Display – View window

To add a new entry to the Switch's **SNMP Group Table**, click the **Add** button in the upper left-hand corner of the **SNMP Group Table** page. This will open the **SNMP Group Table Configuration** page, as shown below.

SNMP Group Table Configuration	
Group Name	<input type="text"/>
Read View Name	<input type="text"/>
Write View Name	<input type="text"/>
Notify View Name	<input type="text"/>
Security Model	SNMPv1
Security Level	NoAuthNoPriv
Apply	
Show All SNMP Group Table Entries	

Figure 8 - 9. SNMP Group Table Configuration – Add window

The following parameters can set:

Parameter	Description
Group Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP group of SNMP users.
Read View Name	This name is used to specify the SNMP group created can request SNMP messages.
Write View Name	Specify a SNMP group name for users that are allowed SNMP write privileges to the Switch's SNMP agent.
Notify View Name	Specify a SNMP group name for users that can receive SNMP trap messages generated by the Switch's SNMP agent.
Security Model	<p><i>SNMPv1</i> - Specifies that SNMP version 1 will be used.</p> <p><i>SNMPv2</i> - Specifies that SNMP version 2c will be used. The SNMPv2 supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.</p> <p><i>SNMPv3</i> - Specifies that the SNMP version 3 will be used. SNMPv3 provides secure access to devices through a combination of authentication and encrypting packets over the network.</p>
Security Level	<p>The Security Level settings only apply to SNMPv3.</p> <ul style="list-style-type: none"> <i>NoAuthNoPriv</i> - Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. <i>AuthNoPriv</i> - Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. <i>AuthPriv</i> - Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.

To implement your new settings, click **Apply**. To return to the **SNMP Group Table**, click the [Show All SNMP Group Table Entries](#) link.

SNMP Community Table

Use this table to create an SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the Switch. One or more of the following characteristics can be associated with the community string:

- An Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the Switch's SNMP agent.
- Any MIB view that defines the subset of all MIB objects will be accessible to the SNMP community.
- Read/write or read-only level permission for the MIB objects accessible to the SNMP community.

To configure **SNMP Community** entries, open the **SNMP Manager** folder, and click the **SNMP Community Table** link, which will open the following screen:

SNMP Community Table			
Community Name	View Name	Access Right	
<input type="text"/>	<input type="text"/>	Read_Only	
<input type="button" value="Apply"/>			
Total Entries: 2 (Note: Maximum of 10 entries.)			
SNMP Community Table			
Community Name	View Name	Access Right	Delete
private	CommunityView	Read_Write	<input type="button" value="X"/>
public	CommunityView	Read_Only	<input type="button" value="X"/>

Figure 8 - 10. SNMP Community Table window

The following parameters can set:

Parameter	Description
Community Name	Type an alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.
View Name	Type an alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. The view name must exist in the SNMP View Table.
Access Right	<p><i>Read Only</i> - Specifies that SNMP community members using the community string created can only read the contents of the MIBs on the Switch.</p> <p><i>Read Write</i> - Specifies that SNMP community members using the community string created can read from, and write to the contents of the MIBs on the Switch.</p>

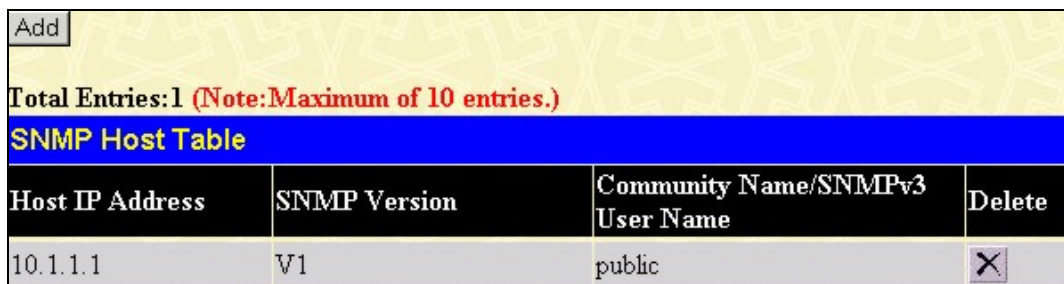
To implement the new settings, click **Apply**. To delete an entry from the **SNMP Community Table**, click the under the **Delete** heading, corresponding to the entry to delete.

SNMP Host Table

Use the **SNMP Host Table** to set up SNMP trap recipients. Open the **SNMP Manager** folder and click on the **SNMP Host Table** link. This will open the **SNMP Host Table** page, as shown below.

To delete an existing **SNMP Host Table** entry, click the corresponding  under the **Delete** heading.

To display the current settings for an existing **SNMP Group Table** entry, click the blue link for the entry under the **Host IP Address** heading.




SNMP Host Table			
Host IP Address	SNMP Version	Community Name/SNMPv3 User Name	Delete
10.1.1.1	V1	public	

Figure 8 - 11. SNMP Host Table

To add a new entry to the Switch's **SNMP Host Table**, click the **Add** button in the upper left-hand corner of the page. This will open the **SNMP Host Table Configuration** page, as shown below.

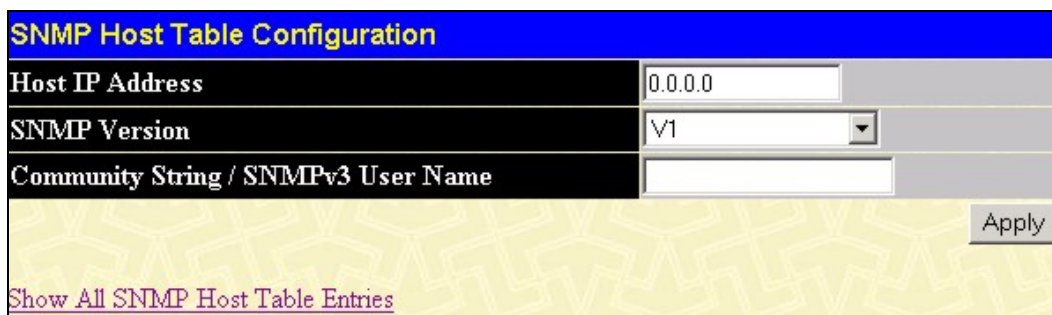


Figure 8 - 12. SNMP Host Table Configuration window

The following parameters can set:

Parameter	Description
Host IP Address	Type the IP address of the remote management station that will serve as the SNMP host for the Switch.
SNMP Version	<p>V1 - To specifies that SNMP version 1 will be used.</p> <p>V2 - To specify that SNMP version 2 will be used.</p> <p>V3-NoAuth-NoPriv - To specify that the SNMP version 3 will be used, with a NoAuth-NoPriv security level.</p> <p>V3-Auth-NoPriv - To specify that the SNMP version 3 will be used, with an Auth-NoPriv security level.</p> <p>V3-Auth-Priv - To specify that the SNMP version 3 will be used, with an Auth-Priv security level.</p>
Community String or SNMP V3 User Name	Type in the community string or SNMP V3 user name as appropriate.

To implement your new settings, click **Apply**. To return to the **SNMP Host Table**, click the [Show All SNMP Host Table Entries](#) link.

SNMP Engine ID

The Engine ID is a unique identifier used for SNMP V3 implementations. This is an alphanumeric string used to identify the SNMP engine on the Switch.

To display the Switch's SNMP Engine ID, open the **SNMP Manger** folder and click on the **SNMP Engine ID** link. This will open the **SNMP Engine ID Configuration** window, as shown below.

The image shows a web-based configuration window titled "SNMP Engine ID Configuration". The title bar is blue with the text in yellow. Below the title bar, there is a label "Engine ID" in a black box on the left. To the right of the label is a text input field containing the alphanumeric string "800000ab030080c83526a0". At the bottom right of the window is a button labeled "Apply". The background of the window has a light yellow pattern of repeating "SNMP" text.

Figure 8 - 13. SNMP Engine ID Configuration window

To change the Engine ID, type the new Engine ID in the space provided and click the **Apply** button.

Monitoring

CPU Utilization

Port Utilization

Packets

Errors

Size

Stacking Information

Device Status

MAC Address

Switch History Log

IGMP Snooping Group

IGMP Snooping Forward

Browse Router Port

Port Access Control

Layer 3 Feature

Browse IP Address

Browse Routing Table

Browse ARP Table

Browse IP Multicast Forwarding Table

Browse IP Multicast Interface Table

Browse IGMP Group Table

OSPF Monitor

DVMRP Monitor

PIM Monitor

CPU Utilization

The **CPU Utilization** displays the percentage of the CPU being used, expressed as an integer percentage and calculated as a simple average by time interval. To view the **CPU Utilization** window, open the **Monitoring** folder and click the **CPU Utilization** link.

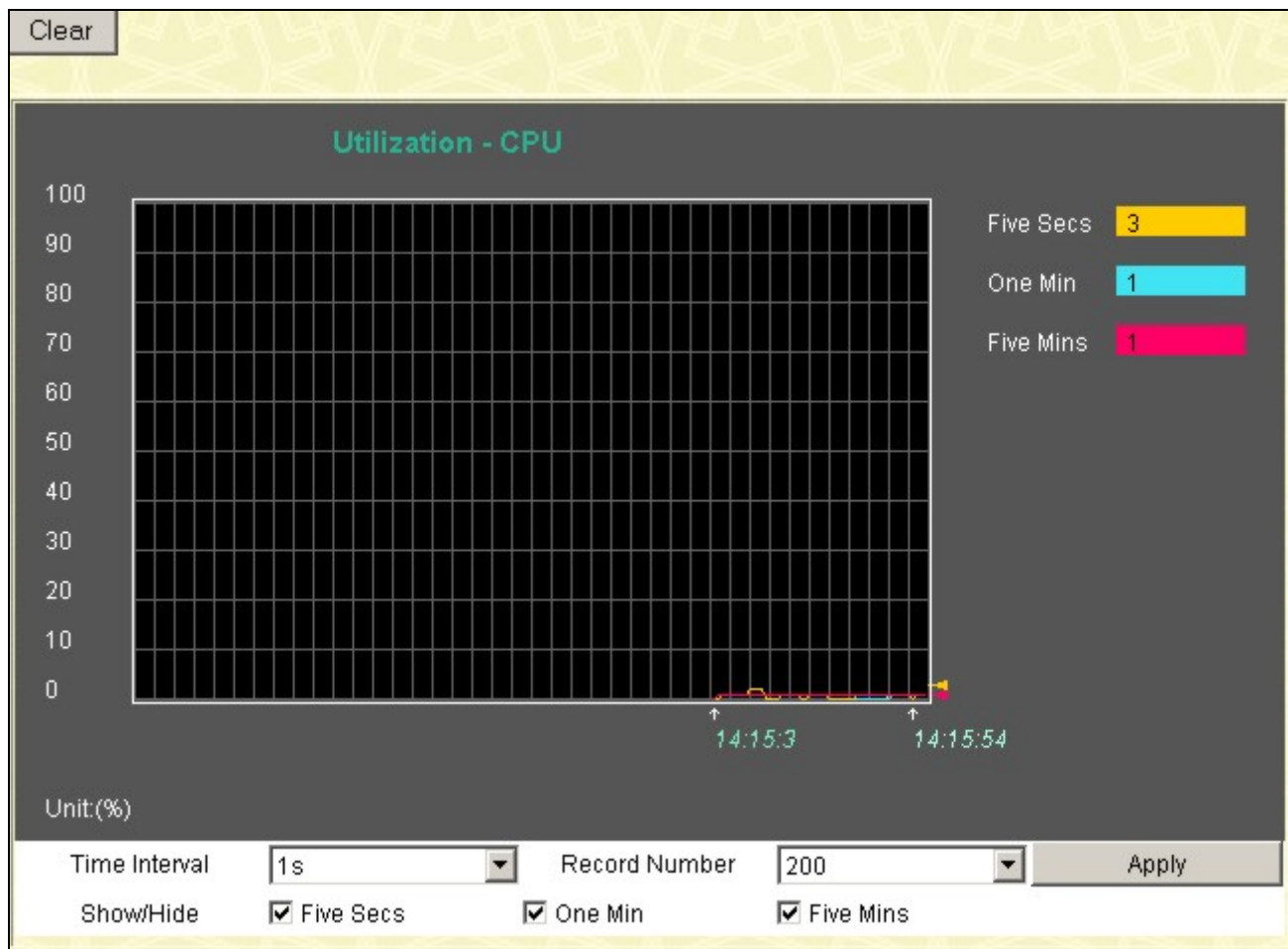


Figure 9- 1. CPU Utilization graph

To view the CPU utilization by port, use the real-time graphic of the Switch and/or switch stack at the top of the web page by simply clicking on a port. Click **Apply** to implement the configured settings. The window will automatically refresh with new updated statistics.

The information is described as follows:

Parameter	Description
Time Interval [1s]	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number [200]	Select number of times the Switch will be polled between 20 and 200. The default value is 200.

Port Utilization

The **Port Utilization** page displays the percentage of the total available bandwidth being used on the port.

To view the port utilization, open the **Monitoring** folder and then the **Port Utilization** link:

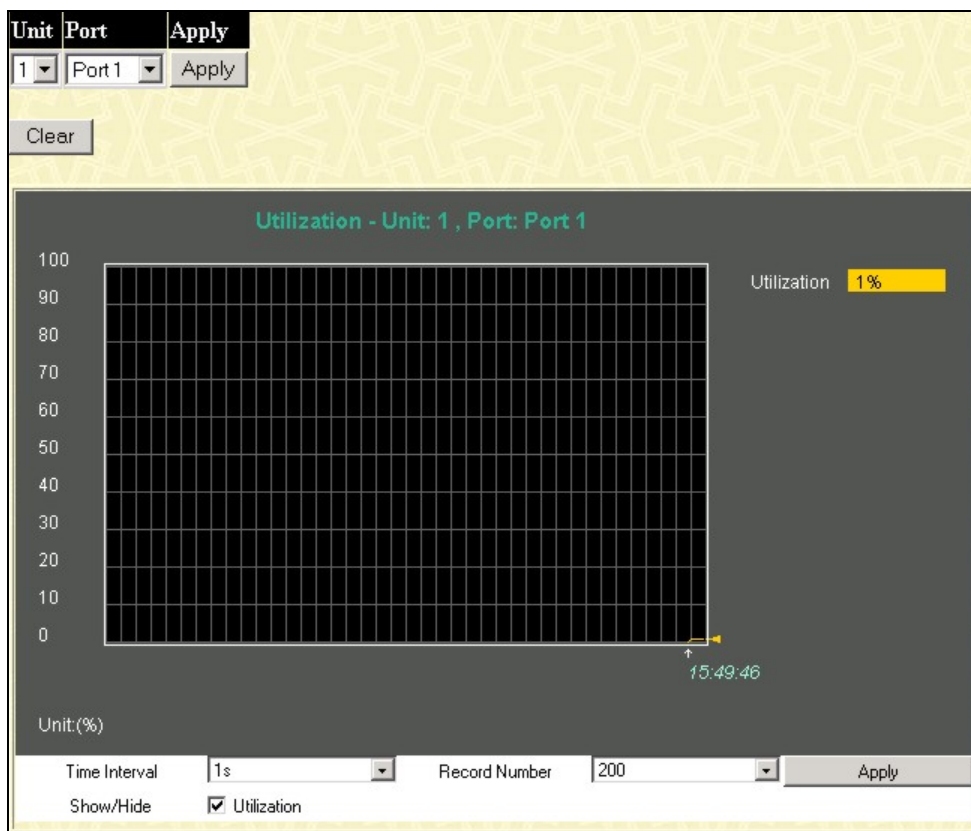


Figure 9- 2. Port Utilization window

To select a port for which to view these statistics, first select the line card slot in the chassis switch by using the **Unit** pull-down menu and then select the port by using the **Port** pull down menu. The user may also use the real-time graphic of the Switch and/or switch stack at the top of the web page by simply clicking on a port. The following field can be set:

Parameter	Description
Time Interval	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between 20 and 200. The default value is 200.

Click **Clear** to refresh the graph. Click **Apply** to implement changes made.

Packets

The Web Manager allows various packet statistics to be viewed as either a line graph or a table. Six windows are offered.

Received (RX)

Click the **Received (RX)** link in the **Packets** folder of the **Monitoring** menu to view the following graph of packets received on the Switch. To select a port to view these statistics for, first select the Switch in the switch stack by using the **Unit** pull-down menu and then select the port by using the **Port** pull down menu. The user may also use the real-time graphic of the Switch and/or switch stack at the top of the web page by simply clicking on a port.

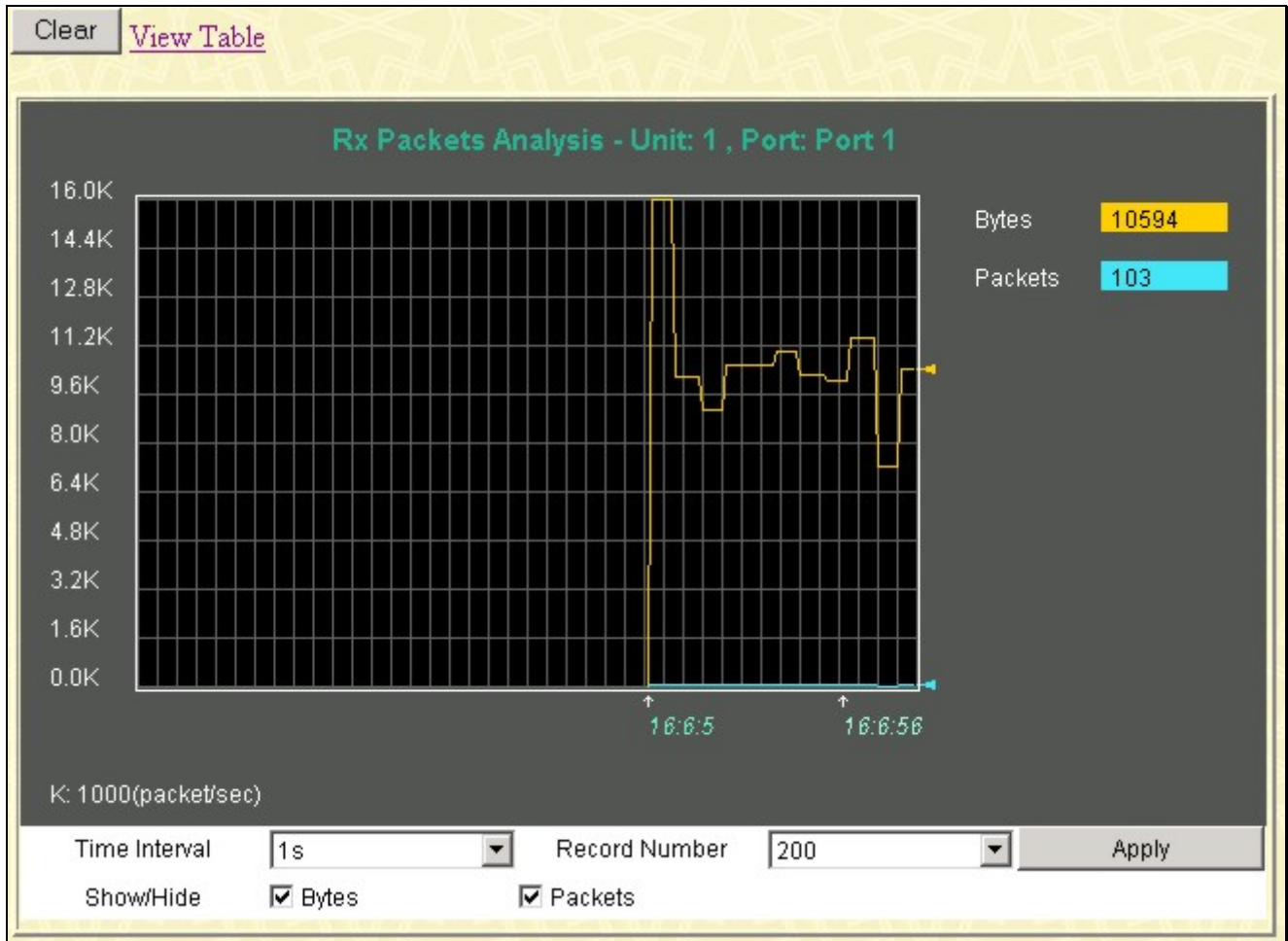


Figure 9- 3. Rx Packets Analysis window (line graph for Bytes and Packets)

To view the **Received Packets Table**, click the link [View Table](#), which will show the following table:

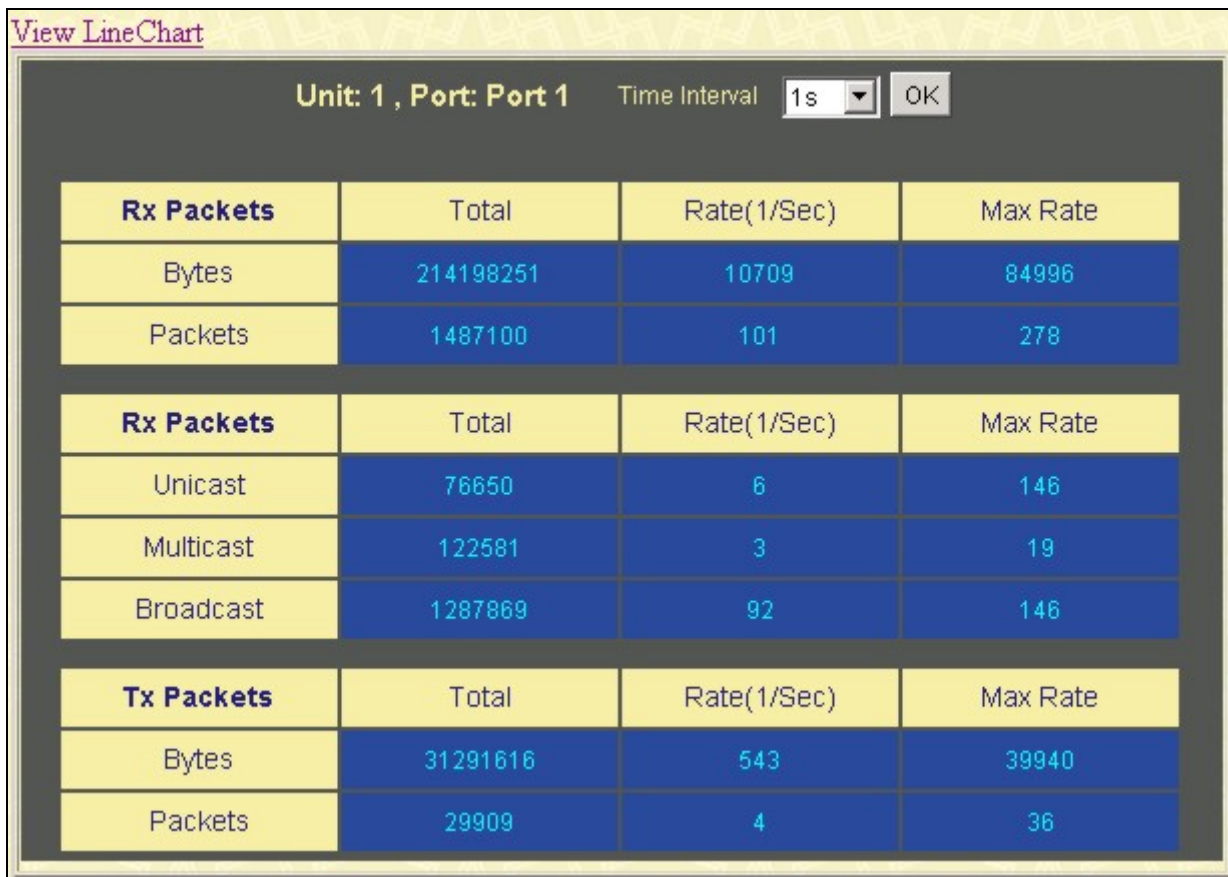


Figure 9- 4. Rx Packets Analysis Table

The following fields may be set or viewed:

Parameter	Description
Time Interval [1s]	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number [200]	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
Bytes	Counts the number of bytes received on the port.
Packets	Counts the number of packets received on the port.
Unicast	Counts the total number of good packets that were received by a unicast address.
Multicast	Counts the total number of good packets that were received by a multicast address.
Broadcast	Counts the total number of good packets that were received by a broadcast address.
Show/Hide	Check whether to display Bytes and Packets.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

UMB Cast (RX)

Click the **UMB Cast (RX)** link in the **Packets** folder of the **Monitoring** menu to view the following graph of UMB cast packets received on the Switch. To select a port to view these statistics for, first select the Switch in the switch stack by using the **Unit** pull-down menu and then select the port by using the **Port** pull down menu. The user may also use the real-time graphic of the Switch and/or switch stack at the top of the web page by simply clicking on a port.

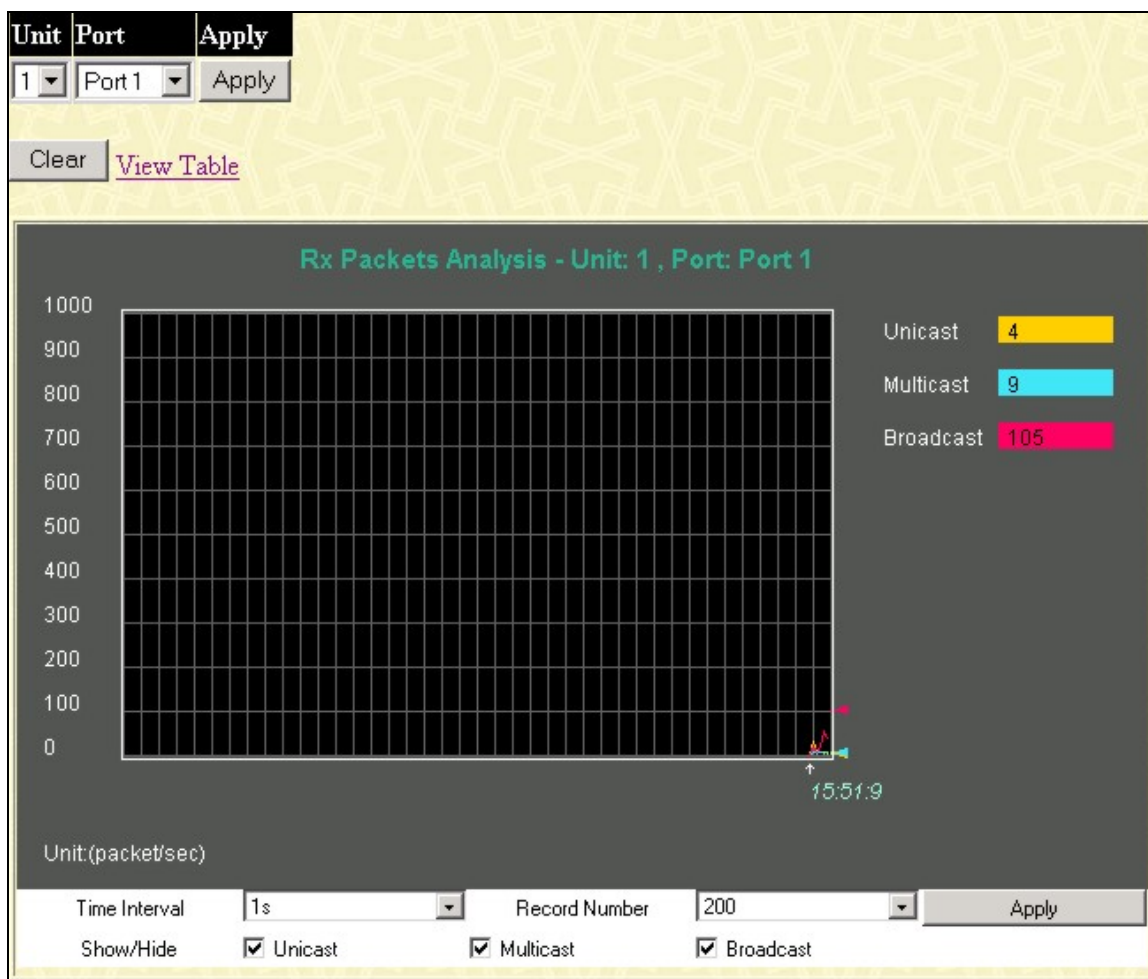


Figure 9- 5. Rx Packets Analysis window (line graph for Unicast, Multicast, and Broadcast Packets)

To view the **UMB Cast Table**, click the [View Table](#) link, which will show the following table:

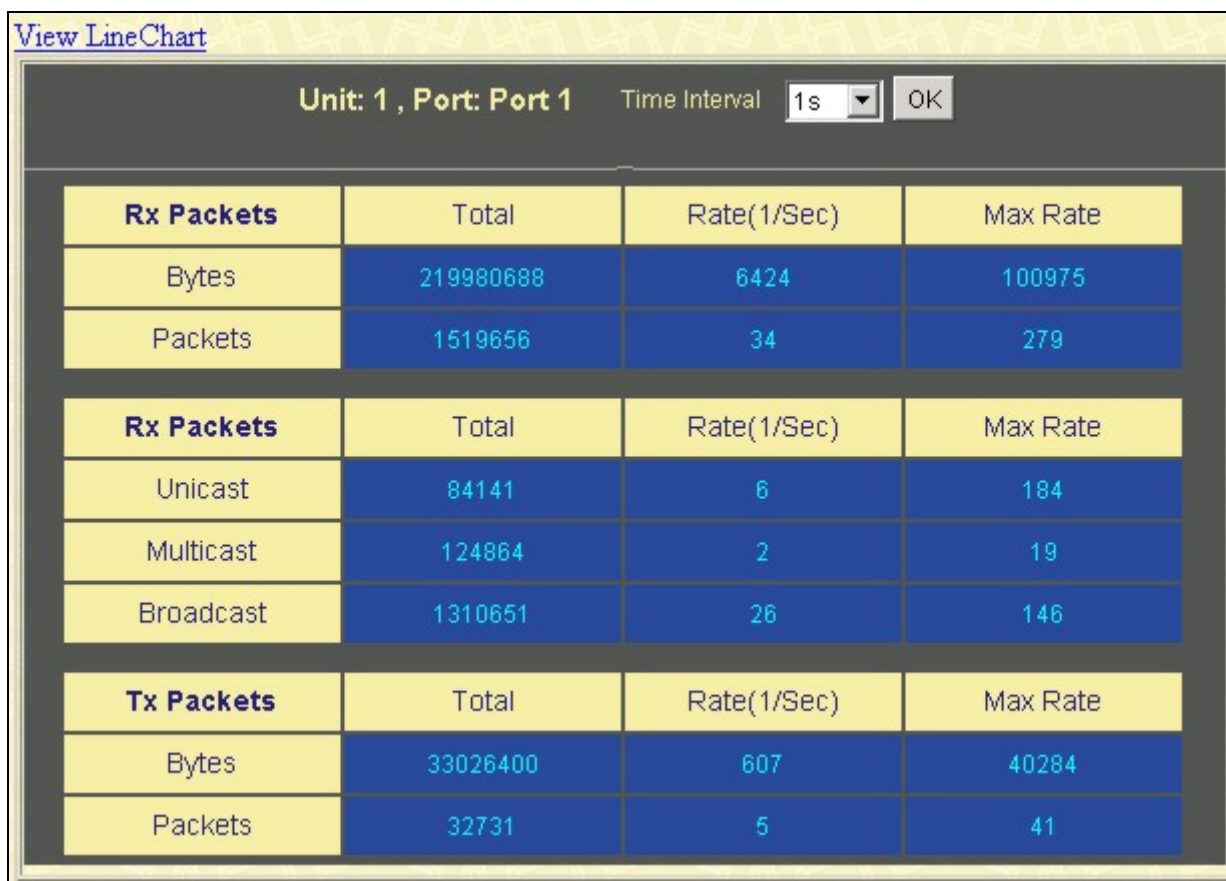


Figure 9- 6. Rx Packets Analysis window (table for Unicast, Multicast, and Broadcast Packets)

The following fields may be set or viewed:

Parameter	Description
Time Interval [1s]	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number [200]	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
Unicast	Counts the total number of good packets that were received by a unicast address.
Multicast	Counts the total number of good packets that were received by a multicast address.
Broadcast	Counts the total number of good packets that were received by a broadcast address.
Show/Hide	Check whether or not to display Multicast, Broadcast, and Unicast Packets.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

Transmitted (TX)

Click the **Transmitted (TX)** link in the **Packets** folder of the **Monitoring** menu to view the following graph of packets transmitted from the Switch. To select a port to view these statistics for, first select the Switch in the switch stack by using the **Unit** pull-down menu and then select the port by using the Port pull down menu. The user may also use the real-time graphic of the Switch and/or switch stack at the top of the web page by simply clicking on a port.

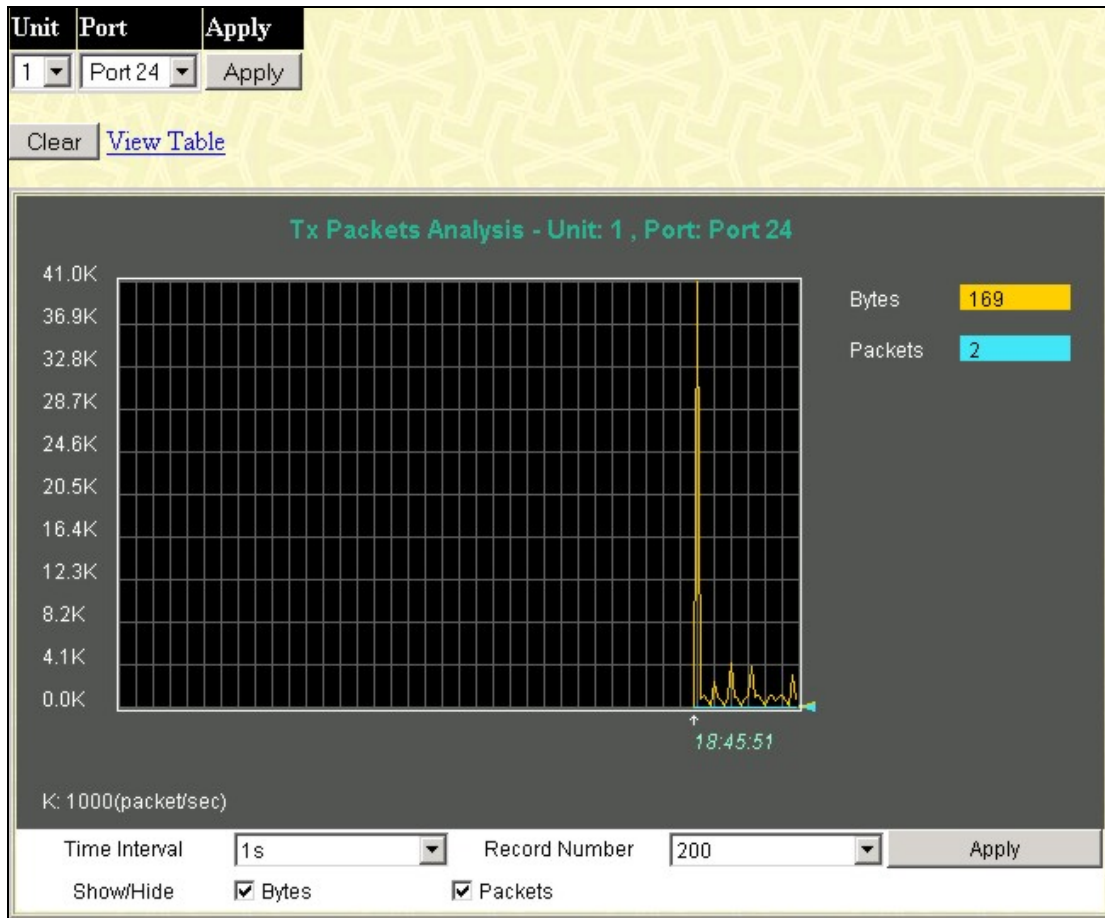


Figure 9- 7. Tx Packets Analysis window (line graph for Bytes and Packets)

To view the **Transmitted (TX) Table**, click the link [View Table](#), which will show the following table:

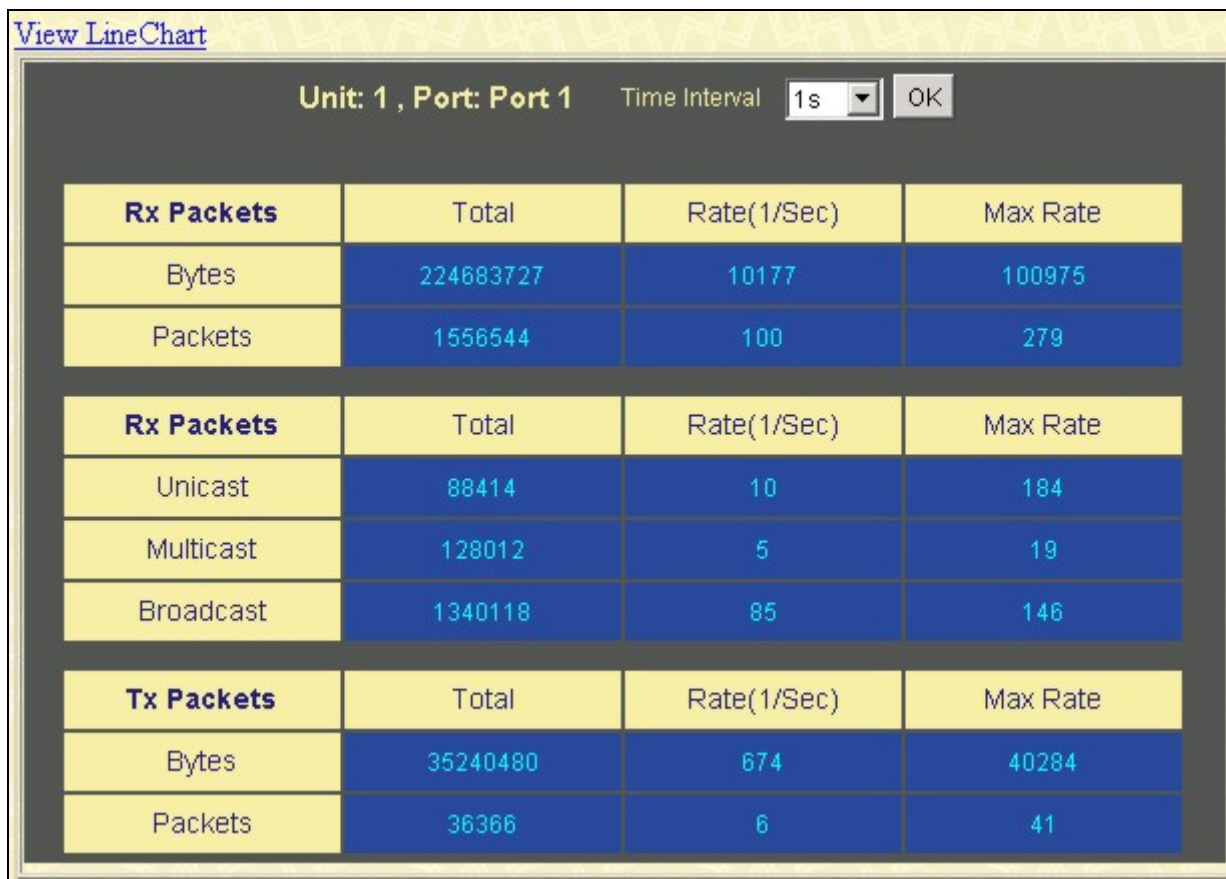


Figure 9- 8. Tx Packets Analysis window (table for Bytes and Packets)

The following fields may be set or viewed:

Parameter	Description
Time Interval [1s]	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number [200]	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
Bytes	Counts the number of bytes successfully sent from the port.
Packets	Counts the number of packets successfully sent on the port.
Unicast	Counts the total number of good packets that were transmitted by a unicast address.
Multicast	Counts the total number of good packets that were transmitted by a multicast address.
Broadcast	Counts the total number of good packets that were transmitted by a broadcast address.
Show/Hide	Check whether or not to display Bytes and Packets.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

Errors

The Web Manager allows port error statistics compiled by the Switch's management agent to be viewed as either a line graph or a table. Four windows are offered.

Received (RX)

Click the **Received (RX)** link in the **Error** folder of the **Monitoring** menu to view the following graph of error packets received on the Switch. To select a port to view these statistics for, first select the line card in the chassis by using the **Unit** pull-down menu and then select the port by using the **Port** pull down menu. The user may also use the real-time graphic of the Switch and/or switch stack at the top of the web page by simply clicking on a port.

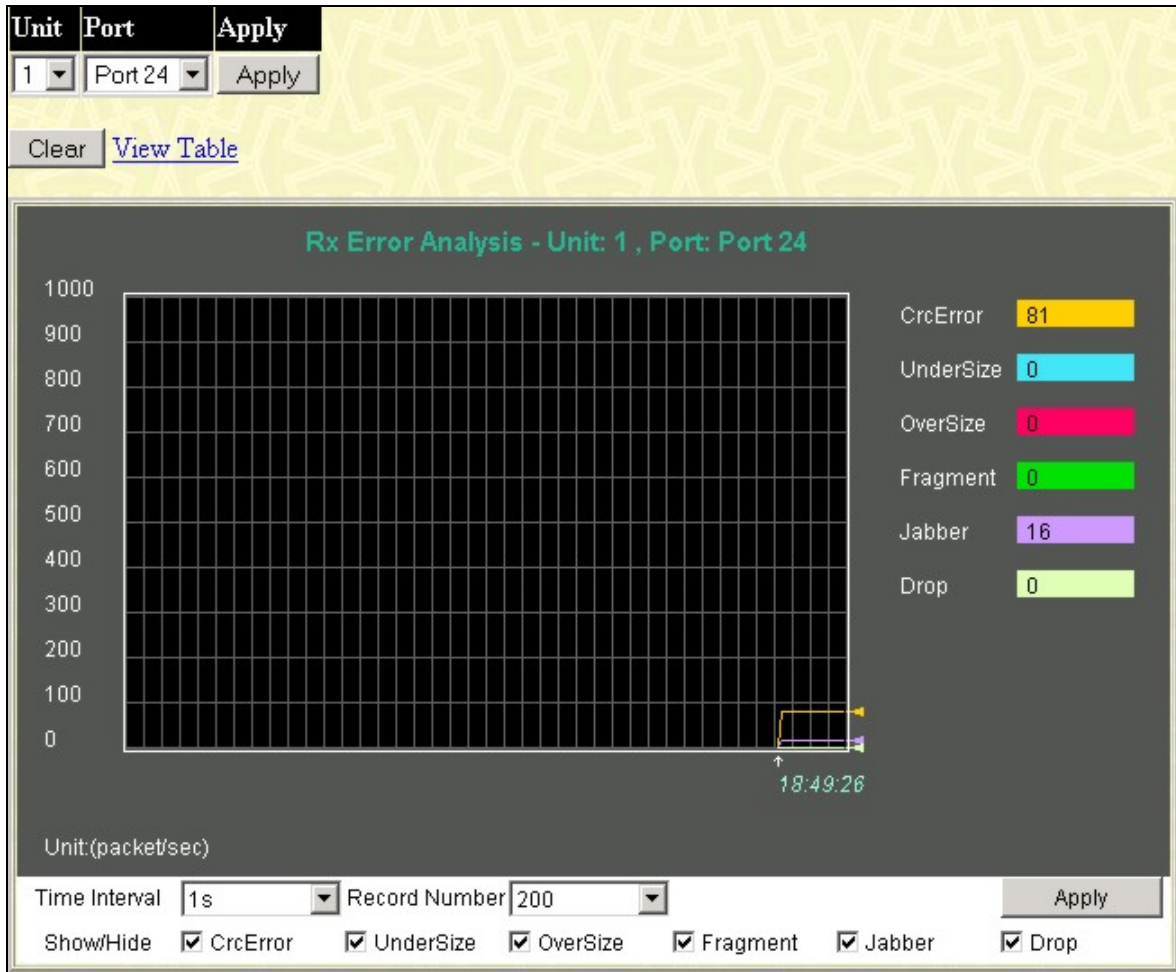


Figure 9- 9. Rx Error Analysis window (line graph)

To view the **Received Error Packets Table**, click the link **View Table**, which will show the following table:

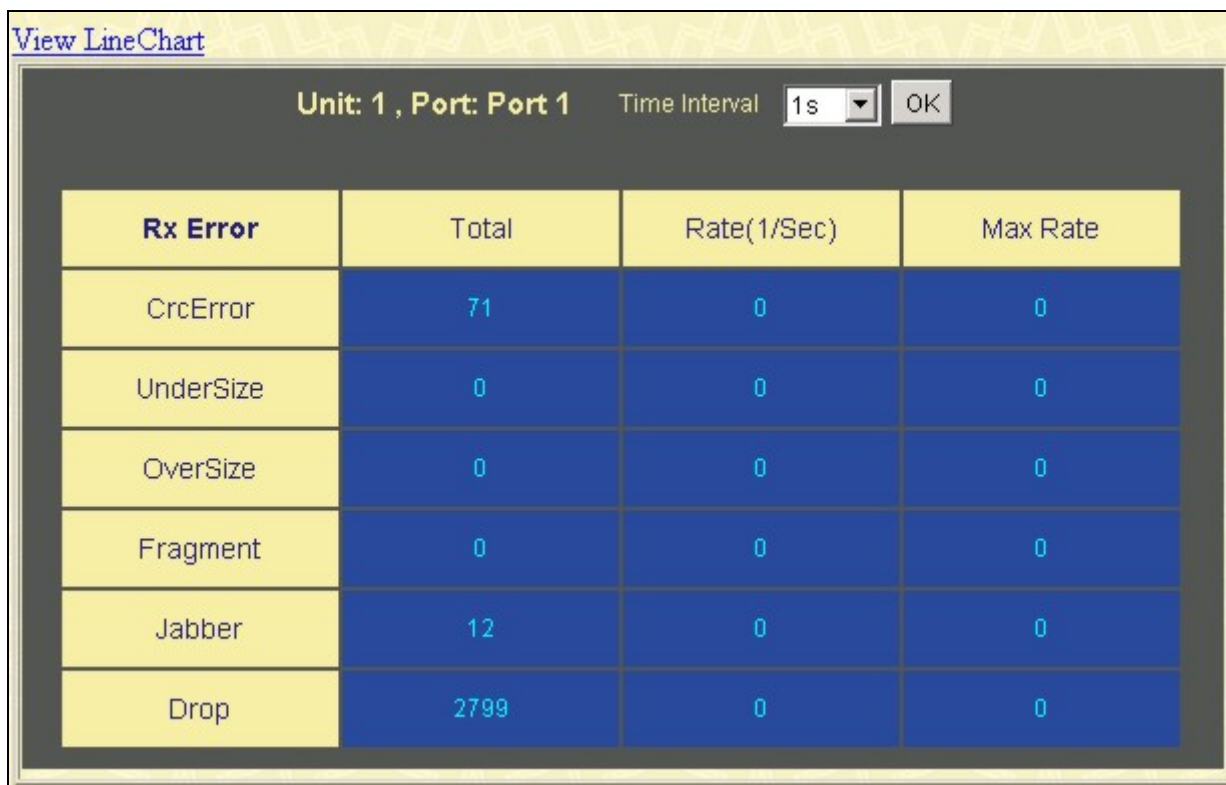


Figure 7- 27. Rx Error Analysis window (table)

The following fields can be set:

Parameter	Description
Time Interval [1s]	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number [200]	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
Crc Error	Counts otherwise valid packets that did not end on a byte (octet) boundary.
UnderSize	The number of packets detected that are less than the minimum permitted packets size of 64 bytes and have a good CRC. Undersize packets usually indicate collision fragments, a normal network occurrence.
OverSize	Counts packets received that were longer than 1518 octets, or if a VLAN frame is 1522 octets, and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1522.
Fragment	The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.
Jabber	The number of packets with lengths more than the MAX_PKT_LEN bytes. Internally, MAX_PKT_LEN is equal to 1522.
Drop	The number of packets that are dropped by this port since the last Switch reboot.
Show/Hide	Check whether or not to display Crc Error, Under Size, Over Size, Fragment, Jabber, and Drop errors.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

Transmitted (TX)

Click the Transmitted (TX) link in the Error folder of the Monitoring menu to view the following graph of error packets received on the Switch. To select a port to view these statistics for, first select the Switch in the switch stack by using the **Unit** pull-down menu and then select the port by using the **Port** pull down menu. The user may also use the real-time graphic of the Switch and/or switch stack at the top of the web page by simply clicking on a port.

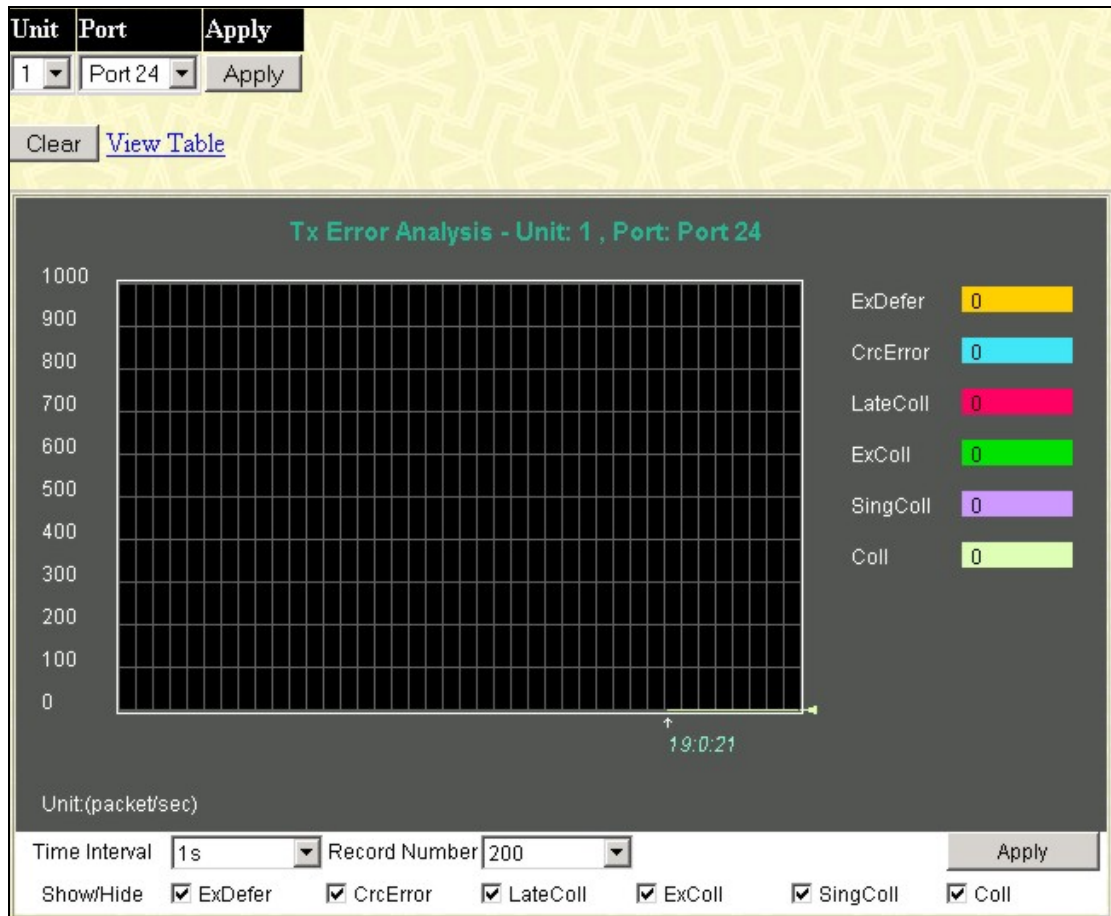


Figure 7- 28. Tx Error Analysis window (line graph)

To view the **Transmitted Error Packets Table**, click the link [View Table](#), which will show the following table:

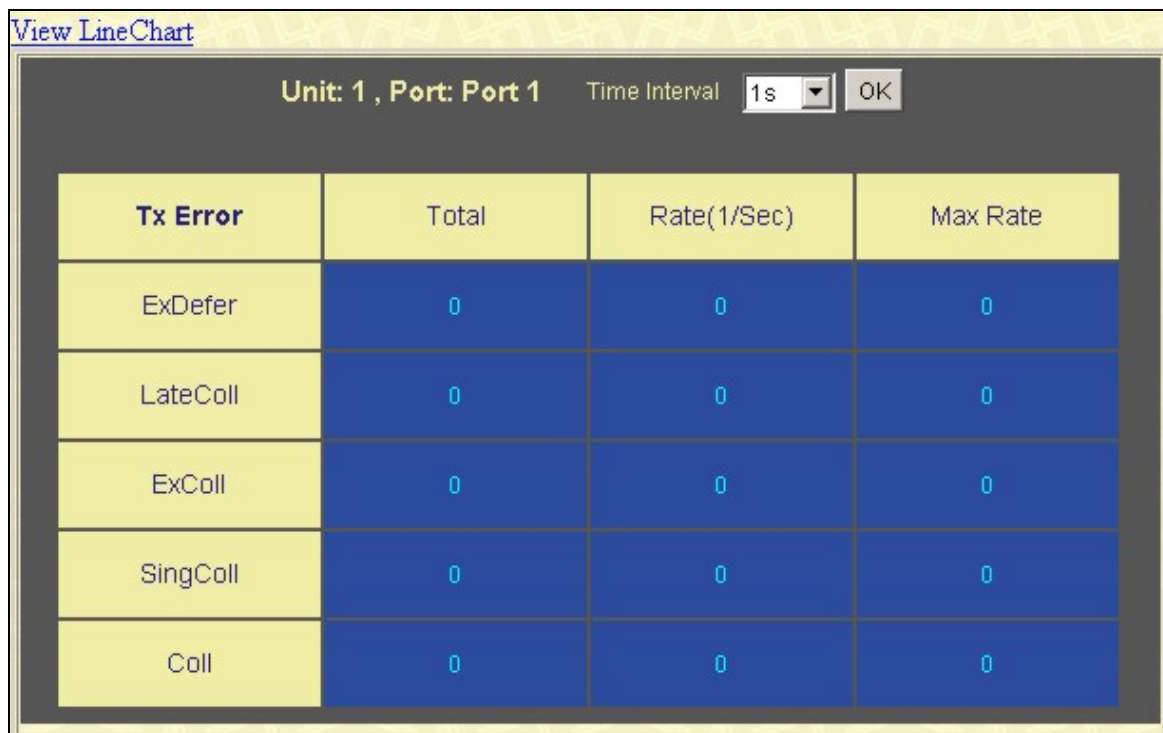


Figure 7- 29. Tx Error Analysis window (table)

The following fields may be set or viewed:

Parameter	Description
Time Interval [1s]	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number [200]	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
ExDefer	Counts the number of packets for which the first transmission attempt on a particular interface was delayed because the medium was busy.
CRC Error	Counts otherwise valid packets that did not end on a byte (octet) boundary.
LateColl	Counts the number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
ExColl	Excessive Collisions. The number of packets for which transmission failed due to excessive collisions.
SingColl	Single Collision Frames. The number of successfully transmitted packets for which transmission is inhibited by more than one collision.
Coll	An estimate of the total number of collisions on this network segment.
Show/Hide	Check whether or not to display ExDefer, LateColl, ExColl, SingColl, and Coll errors.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

Size

The Web Manager allows packets received by the Switch, arranged in six groups and classed by size, to be viewed as either a line graph or a table. Two windows are offered. To select a port to view these statistics for, first select the Switch in the switch stack by using the **Unit** pull-down menu and then select the port by using the **Port** pull down menu. The user may also use the real-time graphic of the Switch and/or switch stack at the top of the web page by simply clicking on a port.

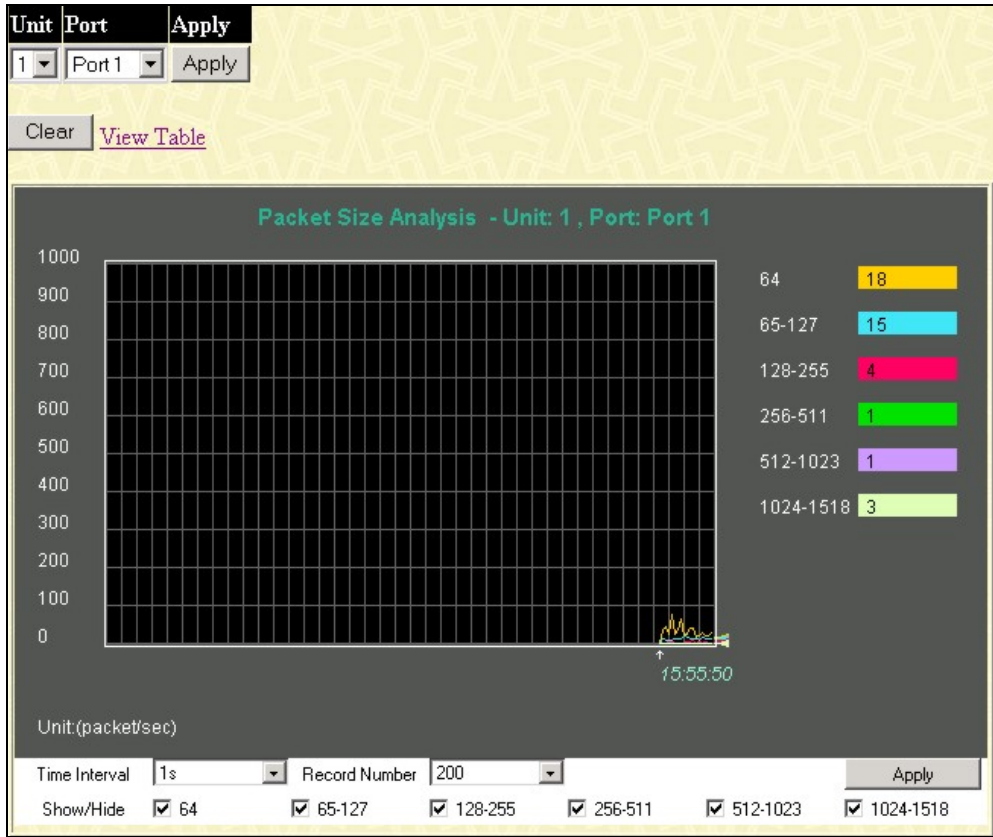


Figure 7- 30. Rx Size Analysis window (line graph)

To view the **Packet Size Analysis Table**, click the link [View Table](#), which will show the following table:

[View Line Chart](#)

Unit: 1, Port: Port 1 Time Interval 1s OK

Packet Size	Total	Rate(1/Sec)	Max Rate
64	1196636	82	82
65-127	134118	3	3
128-255	147578	11	11
256-511	41448	1	1
512-1023	31272	0	0
1024-1518	77984	2	2

Figure 7- 31. Rx Size Analysis window (table)

The following fields can be set or viewed:

Parameter	Description
Time Interval [1s]	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number [200]	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
64	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
65-127	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256-511	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512-1023	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1518	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Show/Hide	Check whether or not to display 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 packets received.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

Stacking Information

The following window displays detailed information about the stacking of the line cards set in the chassis. The xStack® DES-6500 may incorporate up to eight hot-swappable line cards for varying port counts of up to one hundred and ninety-two (192) 10/100 Mbps Fast Ethernet ports or up to ninety-two (92) 1000Mbps Gigabit Ethernet ports.

When the line cards are properly interconnected through their optional Stacking Modules, information about the resulting switch stack is displayed under the **Stack Information** link.

To view the stacking information, click on the **Stacking Information** link from the **Monitoring** folder:

Stacking Information						
Box ID	Type	Exist	Priority	Prom Version	Runtime Version	H/W Version
1	DES-6507	exist	16	2.00-B20	3.50-B07	1A1
2	USR-NOT-CFG	no				
3	DES-6508	no				
4	DES-6507	no				
5	USR-NOT-CFG	no				
6	DES-6509	no				
7	DES-6509	no				
8	DES-6509	no				

Topology : STAR
 Current state : MASTER
 Box count : 1

Figure 9- 10. Stacking Information window

The **Stacking Information** window holds the following information:

Parameters	Description
Box ID	Displays the slot order in the chassis.
Type	Displays the model name of the corresponding switch in a stack.
Exist	Denotes whether a switch does or does not exist in a stack.
Priority	Displays the priority ID of the line card. The lower the number, the higher the priority. The line card with the lowest priority number in the stack denotes the Master module.
Prom Version	Shows the PROM in use for the Switch. This may be different from the values shown in the illustration.
Runtime Version	Shows the firmware version in use for the line card. This may be different from the values shown in the illustrations.
H/W Version	Shows the hardware version in use for the line card. This may be different from the values shown in the illustration.
Topology	Show the current stacking topology employed using this Switch.
Current State	Displays the current stacking state of the Switch, which may be MASTER or SLAVE.
Box Count	Displays the number of line cards currently in use in the chassis.

Device Status

The **Device Status** window can be found in the **Monitoring** menu by clicking the **Device Status** link. This window shows the status of the physical attributes of the Switch, including power sources and fans.

Device Status				
	Status	Output Voltage	Fan1	Fan2
RPS1	Powered	Normal	Normal	Normal
RPS2	Not Exist	--	--	--
System FAN1 : Normal				
System FAN2 : Normal				
System FAN3 : Normal				
System FAN4 : Normal				

Figure 9- 11. Device Status window

The following fields may be viewed in this window:

Parameter	Description
Redundant Power Supply	Displays the RPS' that may be in use.
Status	A read only field denoting the current status of the internal power supply. <i>Powered</i> will suggest the mechanism is functioning correctly while <i>Not Exist</i> will show the mechanism is not functioning correctly.
Output Voltage	A read only field denoting the current status of the external power supply. <i>Normal</i> will suggest the mechanism is functioning correctly while <i>Fail</i> will show the mechanism is not functioning correctly.
Fan1	A read only field denoting if the Switch's #1 fan is functioning properly.
Fan2	A read only field denoting if the Switch's #2 fan is functioning properly.
System FAN	A read only field describing the operating status of other system fans in use on the Switch.

MAC Address

This allows the Switch's dynamic MAC address forwarding table to be viewed. When the Switch learns an association between a MAC address and a port number, it makes an entry into its forwarding table. These entries are then used to forward packets through the Switch.

To view the MAC Address forwarding table, from the **Monitoring** menu, click the **MAC Address** link:

The screenshot shows a web interface for viewing the MAC Address Table. At the top, there are search filters for VLAN Name, MAC Address, and Unit - Port. Below these are buttons for 'Find', 'Delete', 'View All Entry', and 'Delete All Entry'. The main part of the interface is a table titled 'MAC Address Table' with columns for VID, Vlan Name, MAC Address, Unit, Port, and Type. The table contains 225 entries, all with a Type of 'Dynamic'. A 'Next' button is located at the bottom right of the table, and a 'Total Entries: 225' label is at the bottom left.

VID	Vlan Name	MAC Address	Unit	Port	Type
1	default	00-00-01-02-03-a2	3	1	Dynamic
1	default	00-00-50-77-16-00	3	1	Dynamic
1	default	00-00-5e-00-01-5f	3	1	Dynamic
1	default	00-00-81-17-11-00	3	1	Dynamic
1	default	00-00-e2-93-66-06	3	1	Dynamic
1	default	00-01-06-30-10-63	3	1	Dynamic
1	default	00-01-30-12-13-02	3	1	Dynamic
1	default	00-02-a5-fd-66-97	3	1	Dynamic
1	default	00-03-09-18-10-01	3	1	Dynamic
1	default	00-03-44-ae-bc-12	3	1	Dynamic
1	default	00-03-47-91-4a-1c	3	1	Dynamic
1	default	00-03-47-93-11-34	3	1	Dynamic
1	default	00-03-6d-1e-76-79	3	1	Dynamic
1	default	00-05-5d-30-c1-11	3	1	Dynamic
1	default	00-05-5d-64-96-97	3	1	Dynamic
1	default	00-05-5d-6a-a5-36	3	1	Dynamic
1	default	00-05-5d-7e-80-fa	3	1	Dynamic
1	default	00-05-5d-7e-91-c0	3	1	Dynamic
1	default	00-05-5d-84-6f-74	3	1	Dynamic
1	default	00-05-5d-9a-fe-5d	3	1	Dynamic

Figure 9- 12. MAC Address Table

The following fields can be viewed or set:

Parameter	Description
VLAN Name	Enter a VLAN Name for the forwarding table to be browsed by.
MAC Address	Enter a MAC address for the forwarding table to be browsed by.
Unit – Port	Select the switch Unit ID of the switch in the Switch stack and then the port by using the corresponding pull-down menus.
Find	Allows the user to move to a sector of the database corresponding to a user defined port, VLAN, or MAC address.
VID	The VLAN ID of the VLAN of which the port is a member.
VLAN Name	The VLAN Name of the VLAN of which the port is a member.
MAC Address	The MAC address entered into the address table.
Unit	Refers to the Unit of the switch stack from which the MAC address was learned.
Port	The port to which the MAC address above corresponds.
Type	Describes the method which the Switch discovered the MAC address. The possible entries are Dynamic, Self, and Static.
Next	Click this button to view the next page of the address table.
View All Entry	Clicking this button will allow the user to view all entries of the address table.
Delete All Entry	Clicking this button will allow the user to delete all entries of the address table.

Switch History Log

The Web manager allows the Switch's history log, as compiled by the Switch's management agent, to be viewed. To view the Switch history log, open the **Maintenance** folder and click the **Switch History Log** link.

Switch History Log		
Sequence	Time	Log Text
159	2005-04-20, 15:07:42	Successful login through Web (Username: Anonymous)
158	2005-04-20, 14:55:40	Port 3:1 link up, 100Mbps FULL duplex
157	2005-04-20, 14:55:40	Port 2:8 link down
156	2005-04-20, 14:55:40	Port 2:7 link down
155	2005-04-20, 14:55:40	Port 2:6 link down
154	2005-04-20, 14:55:39	Port 2:5 link down
153	2005-04-20, 14:55:39	Port 2:4 link down
152	2005-04-20, 14:55:39	Port 2:3 link down
151	2005-04-20, 14:55:39	Port 2:2 link down
150	2005-04-20, 14:55:39	Port 2:1 link down
149	2005-04-20, 14:55:39	Unit 9, Console session timed out (Username: Anonymous)
148	2005-04-20, 14:55:39	Unit 9, System started up
147	2005-04-15, 15:58:53	Successful login through Web (Username: admin)
146	2005-04-15, 15:58:52	Unit 9, Configuration saved to flash (Username: Darren)
145	2005-04-15, 15:58:27	Unit 9, Successful login through Console (Username: Darren)
144	2005-04-15, 15:58:15	Unit 9, Login failed through Console (Username: Anonymous)
143	2005-04-15, 15:45:27	Unit 9, Console session timed out (Username: Anonymous)
142	2005-04-15, 14:32:29	Unit 9, Configuration saved to flash (Username: Anonymous)
141	2005-04-15, 14:02:25	Unit 9, Successful login through Console (Username: Anonymous)
140	2005-04-15, 14:01:58	Unit 9, Console session timed out (Username: Anonymous)
Clear		Next

Figure 9- 13. Switch History Log window

The Switch can record event information in its own logs, to designated SNMP trap receiving stations, and to the PC connected to the console manager. Click **Next** to go to the next page of the **Switch History Log**. Clicking **Clear** will allow the user to clear the **Switch History Log**.

The information is described as follows:

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.
Log Text	Displays text describing the event that triggered the history log entry.

IGMP Snooping Group

This window allows the Switch's **IGMP Snooping Group Table** to be viewed. IGMP Snooping allows the Switch to read the Multicast Group IP address and the corresponding MAC address from IGMP packets that pass through the Switch. The number of IGMP reports that were snooped is displayed in the **Reports** field.

To view the **IGMP Snooping Group Table**, click **IGMP Snooping Group** on the **Monitoring** menu:

VID:	<input type="text" value="0"/>	<input type="button" value="Search"/>																						
Total Entries : 0																								
IGMP Snooping Group Table																								
VLAN ID	Multicast Group	MAC Address	Reports																					
0	0.0.0.0	00:00:00:00:00:00	0																					
Unit	Port Map																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1																								
2																								
3																								
4																								
5																								
6																								
7																								
8																								

Figure 9- 14. IGMP Snooping Group Table

The user may search the **IGMP Snooping Group Table** by VID by entering it in the top left hand corner and clicking **Search**.

The following field can be viewed:

Parameter	Description
VLAN ID	The VLAN ID of the multicast group.
Multicast Group	The IP address of the multicast group.
MAC Address	The MAC address of the multicast group.
Reports	The total number of reports received for this group.
Port Map	These are the ports where the IGMP packets were snooped are displayed.



NOTE: To configure IGMP snooping for the xStack® DES-6500 chassis switch, go to the **Configuration** folder and select **IGMP Snooping**. Configuration and other information concerning IGMP snooping may be found in Section 6 of this manual under **IGMP Snooping**.

IGMP Snooping Forwarding

This window will display the current IGMP snooping forwarding table entries currently configured on the Switch. To view the following screen, open the **Monitoring** folder and click the **IGMP Snooping Forwarding** link.

VID: <input type="text" value="0"/>		<input type="button" value="Search"/>																							
Total Entries : 0																									
IGMP Snooping Forwarding Table																									
VLAN Name		Source IP		Multicast Group																					
		0.0.0.0		0.0.0.0																					
Unit	Port Map																								
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
1																									
2																									
3																									
4																									
5																									
6																									
7																									
8																									

Figure 9- 15. IGMP Snooping Forwarding Table

The user may search the **IGMP Snooping Forwarding Table** by VLAN Name using the top left hand corner **Search**.

The following field can be viewed:

Parameter	Description
VLAN Name	The VLAN Name of the multicast group.
Source IP	The Source IP address of the multicast group.
Multicast Group	The IP address of the multicast group.
Port Map	These are the ports to which the IP multicast packets are being forwarded.

Browse Router Port

This displays which of the Switch's ports are currently configured as router ports. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port, designated by **S**. A router port that is dynamically configured by the Switch is designated by **D** and a Forbidden port is designated by **F**.

Total Entries : 1																								
Browse Router Port																								
VLAN ID												VLAN Name												
1												default												
Unit	Ports																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1																								
2																								
3																								
4																								
5																								
6																								
7																								
8																								

S : Static
D : Dynamic
F : Fobidden

Figure 9- 16. Browse Router Port window

Port Access Control

The following screens are used to monitor 802.1x statistics of the Switch, on a per port basis. To view the **Port Access Control** screens, open the monitoring folder and click the **Port Access Control** folder. There are six screens to monitor.



NOTE: The **Authenticator State**, **Authenticator Statistics**, **Authenticator Session Statistics** and **Authenticator Diagnostics** windows in this section cannot be viewed on the xStack® DES-6500 chassis switch unless 802.1x is enabled by port or by MAC address. To enable 802.1x, go to the Port Access Entity folder in the configuration folder and select the heading **802.1X Auth Mode Settings**.

Authenticator State

The following section describes the 802.1X Status on the Switch. To view the Authenticator State, click **Monitoring > Port Access Control > Authenticator State**.

Port	Auth_PAE_State	Backend_State	PortStatus
1	ForceAuth	Success	Authorized
2	ForceAuth	Success	Authorized
3	ForceAuth	Success	Authorized
4	ForceAuth	Success	Authorized
5	ForceAuth	Success	Authorized
6	ForceAuth	Success	Authorized
7	ForceAuth	Success	Authorized
8	ForceAuth	Success	Authorized
9	ForceAuth	Success	Authorized
10	ForceAuth	Success	Authorized
11	ForceAuth	Success	Authorized
12	ForceAuth	Success	Authorized

Figure 9- 17. Authenticator State window – Port-based 802.1x

Unit	Port	Apply
1	Port 1	Apply

Authenticator State of Unit 1 Port 1 of Unit 1				Time Interval	OK
Index	Mac Address	Auth PAE State	Backend State	Port Status	
1	N/A	N/A	N/A	N/A	
2	N/A	N/A	N/A	N/A	
3	N/A	N/A	N/A	N/A	
4	N/A	N/A	N/A	N/A	
5	N/A	N/A	N/A	N/A	
6	N/A	N/A	N/A	N/A	
7	N/A	N/A	N/A	N/A	
8	N/A	N/A	N/A	N/A	
9	N/A	N/A	N/A	N/A	
10	N/A	N/A	N/A	N/A	
11	N/A	N/A	N/A	N/A	
12	N/A	N/A	N/A	N/A	
13	N/A	N/A	N/A	N/A	
14	N/A	N/A	N/A	N/A	
15	N/A	N/A	N/A	N/A	
16	N/A	N/A	N/A	N/A	

Figure 9- 18. Authenticator State window – MAC-Based 802.1x

This window displays the **Authenticator State** for individual ports on a selected device. To select unit within the switch stack, use the pull-down menu at the top of the window and click **Apply**. A polling interval between *1* and *60* seconds can be set using the drop-down menu at the top of the window and clicking **OK**.

The information on this window is described as follows:

Parameter	Description
Auth PAE State	The Authenticator PAE State value can be: <i>Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, Force_Auth, Force_Unauth, or N/A</i> . <i>N/A</i> (Not Available) indicates that the port's authenticator capability is disabled.
Backend State	The Backend Authentication State can be <i>Request, Response, Success, Fail, Timeout, Idle, Initialize, or N/A</i> . <i>N/A</i> (Not Available) indicates that the port's authenticator capability is disabled.
Port Status	Controlled Port Status can be <i>Authorized, Unauthorized, or N/A</i> .

Authenticator Diagnostics

This table contains the diagnostic information regarding the operation of the Authenticator associated with each port. The user may choose the line card and port to view these statistics for by using the pull-down menus in the top left and corner. This window is identical for both MAC-based and port-based 802.1X, except for the inclusion of the MAC address for MAC-based. To view the **Authenticator Diagnostics**, click **Monitoring > Port Access Control > Authenticator Diagnostics**.

The user can specify a switch in a switch stack using that switch's **Unit** ID by using the pull down menu in the top left hand corner. The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second.

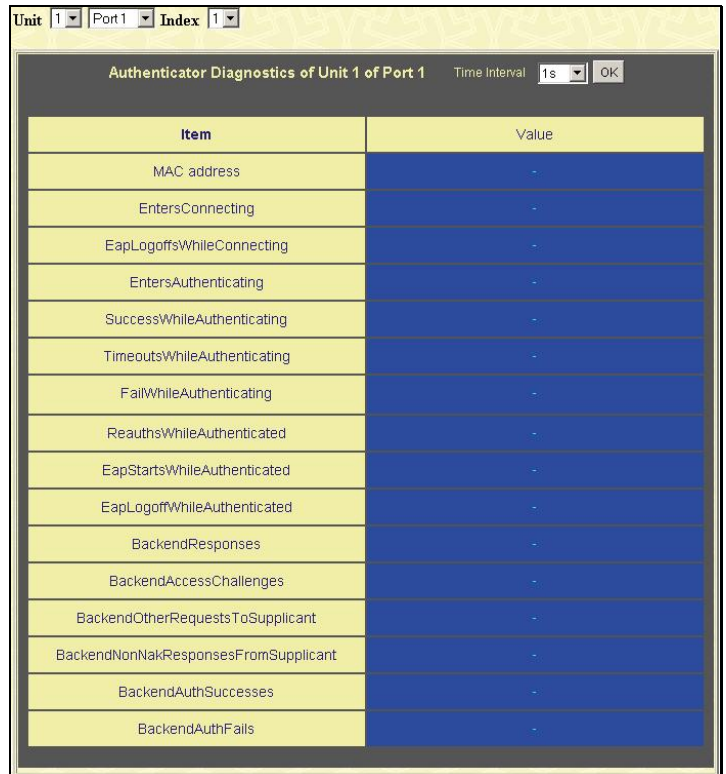


Figure 9- 19. Authenticator Diagnostics window

The following fields can be viewed:

Parameter	Description
MAC address	The identification number assigned to the Port by the System in which the Port resides. This field is only displayed when 802.1X is enabled by MAC address.
EnterConnecting	Counts the number of times that the state machine transitions to the CONNECTING state from any other state.
EapLogoffsWhile Connecting	Counts the number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOL-Logoff message.
EntersAuthenticating	Counts the number of times that the state machine transitions from CONNECTING to AUTHENTICATING, as a result of an EAP-Response/Identity message being received from the Supplicant.
SuccessWhileAuthenticating	Counts the number of times that the state machine transitions from AUTHENTICATING to AUTHENTICATED, as a result of the Backend Authentication state machine indicating successful authentication of the Supplicant (authSuccess = TRUE).
TimeoutsWhileAuthenticating	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of the Backend Authentication state machine indicating authentication timeout (authTimeout = TRUE).
FailWhileAuthenticating	Counts the number of times that the state machine transitions from AUTHENTICATING to HELD, as a result of the Backend Authentication state machine indicating authentication failure (authFail = TRUE).

ReauthsWhileAuthenticating	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a reauthentication request (reAuthenticate = TRUE).
EapStartsWhileAuthenticating	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Start message being received from the Supplicant.
EapLogoffWhileAuthenticating	Counts the number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Logoff message being received from the Supplicant.
ReauthsWhileAuthenticated	Counts the number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of a reauthentication request (reAuthenticate = TRUE).
EapStartsWhileAuthenticated	Counts the number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of an EAPOL-Start message being received from the Supplicant.
EapLogoffWhileAuthenticated	Counts the number of times that the state machine transitions from AUTHENTICATED to DISCONNECTED, as a result of an EAPOL-Logoff message being received from the Supplicant.
BackendResponses	Counts the number of times that the state machine sends an initial Access-Request packet to the Authentication server (i.e., executes sendRespToServer on entry to the RESPONSE state). Indicates that the Authenticator attempted communication with the Authentication Server.
BackendAccessChallenges	Counts the number of times that the state machine receives an initial Access-Challenge packet from the Authentication server (i.e., aReq becomes TRUE, causing exit from the RESPONSE state). Indicates that the Authentication Server has communication with the Authenticator.
BackendOtherRequestsToSupplicant	Counts the number of times that the state machine sends an EAP-Request packet (other than an Identity, Notification, Failure, or Success message) to the Supplicant (i.e., executes txReq on entry to the REQUEST state). Indicates that the Authenticator chose an EAP-method.
BackendNonNakResponsesFromSupplicant	Counts the number of times that the state machine receives a response from the Supplicant to an initial EAP-Request, and the response is something other than EAP-NAK (i.e., rxResp becomes TRUE, causing the state machine to transition from REQUEST to RESPONSE, and the response is not an EAP-NAK). Indicates that the Supplicant can respond to the Authenticator's chosen EAP-method.
BackendAuthSuccesses	Counts the number of times that the state machine receives an Accept message from the Authentication Server (i.e., a Success becomes TRUE, causing a transition from RESPONSE to SUCCESS). Indicates that the Supplicant has successfully authenticated to the Authentication Server.
BackendAuthFails	Counts the number of times that the state machine receives a Reject message from the Authentication Server (i.e., a Fail becomes TRUE, causing a transition from RESPONSE to FAIL). Indicates that the Supplicant has not authenticated to the Authentication Server.

Authenticator Session Statistics

This table contains the session statistics objects for the Authenticator PAE associated with each port. To view the **Authenticator Session Statistics**, click **Monitoring > Port Access Control > Authenticator Session Statistics**.

Item	Value
SessionOctetsRx	0
SessionOctetsTx	0
SessionFramesRx	0
SessionFramesTx	0
SessionId	
SessionAuthenticMethod	Remote Authentication Server
SessionTime	0
SessionTerminateCause	SupplicantLogoff
SessionUserName	

Figure 9- 20. Authenticator Session Statistics window

The user can specify a switch in a switch stack using that switch’s Unit ID by using the pull down menu in the top left hand corner. The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where “s” stands for seconds. The default value is one second.

The following fields can be viewed:

Parameter	Description
SessionOctetsRx	The number of octets received in user data frames on this port during the session.
SessionOctetsTx	The number of octets transmitted in user data frames on this port during the session.
SessionFramesRx	The number of user data frames received on this port during the session.
SessionFramesTx	The number of user data frames transmitted on this port during the session.
SessionID	A unique identifier for the session, in the form of a printable ASCII string of at least three characters.

SessionAuthenticMethod	<p>The authentication method used to establish the session. Valid Authentic Methods include:</p> <p>(1) Remote Authentic Server - The Authentication Server is external to the Authenticator's System.</p> <p>(2) Local Authentic Server - The Authentication Server is located within the Authenticator's System.</p>
SessionTime	<p>The duration of the session in seconds.</p>
SessionTerminateCause	<p>The reason for the session termination. There are eight possible reasons for termination.</p> <ol style="list-style-type: none"> 1) Supplicant Logoff 2) Port Failure 3) Supplicant Restart 4) Reauthentication Failure 5) AuthControlledPortControl set to ForceUnauthorized 6) Port re-initialization 7) Port Administratively Disabled 8) Not Terminated Yet
SessionUserName	<p>The User-Name representing the identity of the Supplicant PAE.</p>

Authenticator Statistics

This table contains the statistics objects for the Authenticator PAE associated with each port. An entry appears in this table for each port that supports the Authenticator function. To view the Authenticator Statistics, click **Monitoring > Port Access Control > Authenticator Statistics**.

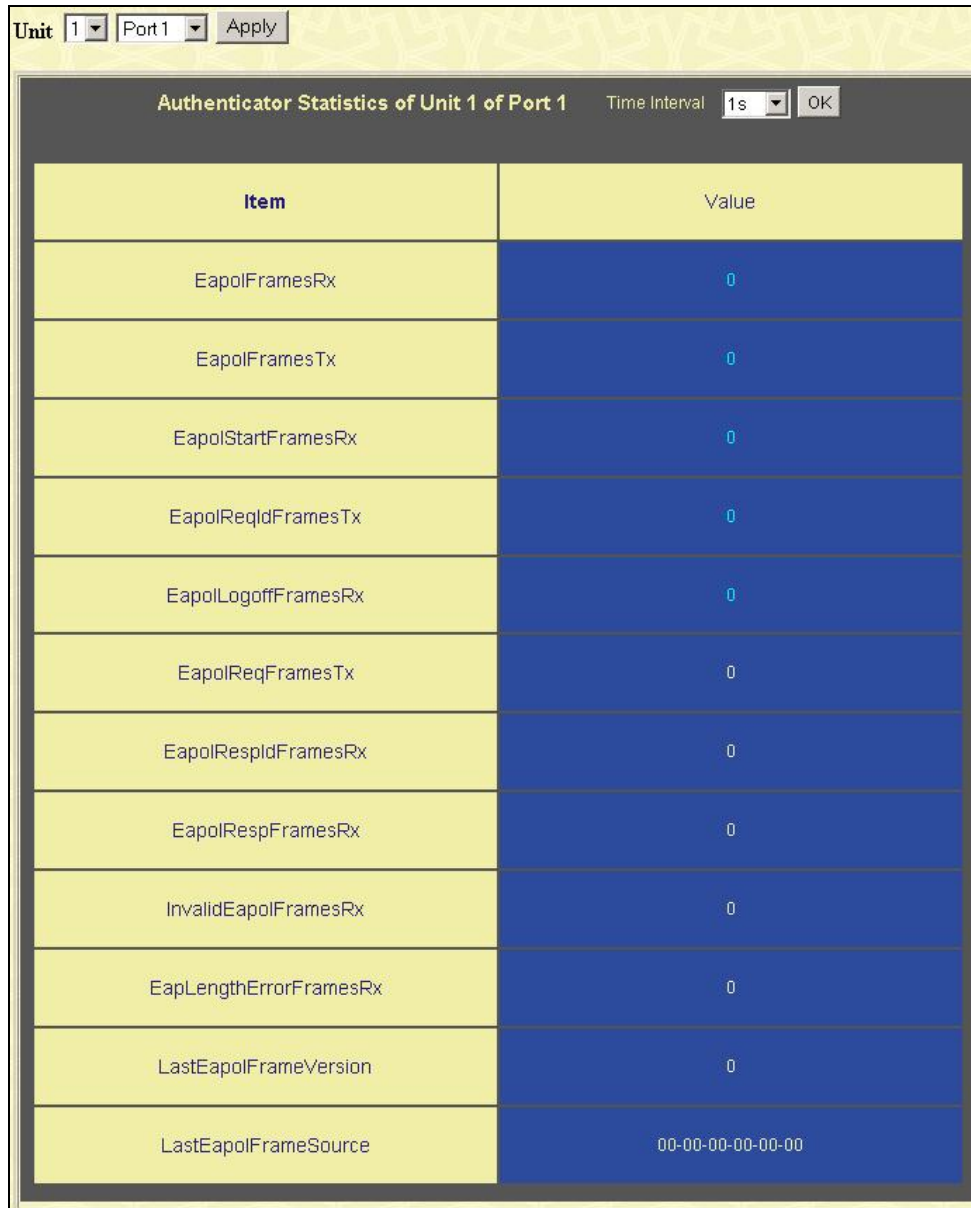


Figure 9- 21. Authenticator Statistics window

The user can specify a switch in a switch stack using that switch’s Unit ID by using the pull down menu in the top left hand corner. The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where “s” stands for seconds. The default value is one second.

The following fields can be viewed:

Parameter	Description
EapolFramesRx	The number of valid EAPOL frames that have been received by this Authenticator.
EapolFramesTx	The number of EAPOL frames that have been transmitted by this Authenticator.
EapolStartFramesRx	The number of EAPOL Start frames that have been received by this Authenticator.
EapolReqIdFramesTx	The number of EAP Req/Id frames that have been transmitted by this Authenticator.

EapolLogoffFramesRx	The number of EAPOL Logoff frames that have been received by this Authenticator.
EapolReqFramesTx	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.
EapolRespIdFramesRx	The number of EAP Resp/Id frames that have been received by this Authenticator.
EapolRespFramesRx	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
InvalidEapolFramesRx	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
EapLengthErrorFramesRx	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
LastEapolFrameVersion	The protocol version number carried in the most recently received EAPOL frame.
LastEapolFrameSource	The source MAC address carried in the most recently received EAPOL frame.

RADIUS Account Client

This window shows managed objects used for managing RADIUS accounting clients, and the current statistics associated with them. To view the **RADIUS Accounting**, click **Monitoring > Port Access Control > RADIUS Account Client**.

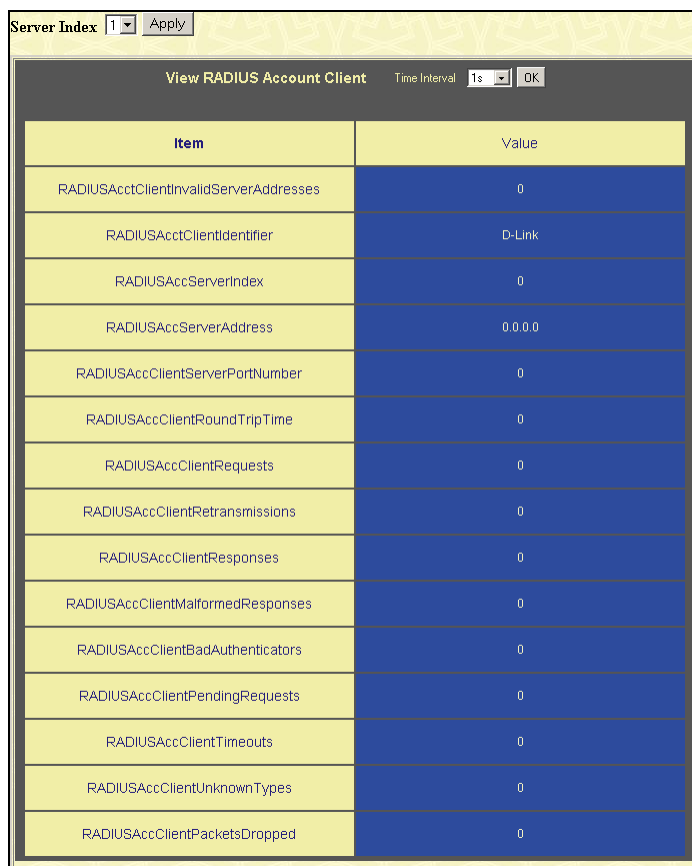


Figure 9- 22. RADIUS Accounting window

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where “s” stands for seconds. The default value is one second. To clear the current statistics shown, click the *Clear* button in the top left hand corner.

The following fields can be viewed:

Parameter	Description
ClientInvalidServerAddresses	The number of RADIUS Accounting-Response packets received from unknown addresses.
ClientIdentifier	The NAS-Identifier of the RADIUS accounting client. (This is not necessarily the same as sysName in MIB II.)
ServerIndex	The identification number assigned to each RADIUS Accounting server that the client shares a secret with.
ServerAddress	The (conceptual) table listing the RADIUS accounting servers with which the client shares a secret.
ServerPortNumber	The UDP port the client is using to send requests to this server.
ClientRoundTripTime	The time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
ClientRequests	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.

ClientRetransmissions	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.
ClientResponses	The number of RADIUS packets received on the accounting port from this server.
ClientMalformedResponses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
ClientBadAuthenticators	The number of RADIUS Accounting-Response packets, which contained invalid authenticators, received from this server.
ClientPendingRequests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an Accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.
ClientTimeouts	The number of accounting timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.
ClientUnknownTypes	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
ClientPacketsDropped	The number of RADIUS packets, which were received from this server on the accounting port and dropped for some other reason.



Note: To configure 802.1x features for the xStack[®] DES-6500 chassis switch, go to the **Configuration** folder and select **Port Access Entity**. Configuration and other information concerning 802.1x may be found in Section 6 of this manual under **Port Access Entity**.

RADIUS Auth Client

This table contains information concerning the activity of the RADIUS authentication client on the client side of the RADIUS authentication protocol. To view the **RADIUS Authentication**, click **Monitoring > Port Access Control > RADIUS Auth Client**.

The screenshot shows a window titled "View RADIUS Auth Client" with a "Time Interval" dropdown set to "1s" and an "OK" button. At the top left, there is a "Server Index" dropdown set to "1" and an "Apply" button. The main content is a table with two columns: "Item" and "Value".

Item	Value
RADIUSAuthClientInvalidServerAddresses	0
RADIUSAuthClientIdentifier	D-Link
RADIUSAuthServerIndex	0
RADIUSAuthServerAddress	0.0.0.0
RADIUSAuthClientServerPortNumber	0
RADIUSAuthClientRoundTripTime	0
RADIUSAuthClientAccessRequests	0
RADIUSAuthClientAccessRetransmissions	0
RADIUSAuthClientAccessAccepts	0
RADIUSAuthClientAccessRejects	0
RADIUSAuthClientAccessChallenges	0
RADIUSAuthClientMalformedAccessResponses	0
RADIUSAuthClientBadAuthenticators	0
RADIUSAuthClientPendingRequests	0
RADIUSAuthClientTimeouts	0
RADIUSAuthClientUnknownTypes	0
RADIUSAuthClientPacketsDropped	0

Figure 9- 23. RADIUS Authentication window

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where “s” stands for seconds. The default value is one second. To clear the current statistics shown, click the *Clear* button in the top left hand corner.

The following fields can be viewed:

Parameter	Description
ClientInvalidServerAddresses	The number of RADIUS Access-Response packets received from unknown addresses.
ClientIdentifier	The NAS-Identifier of the RADIUS authentication client. (This is not necessarily the same as sysName in MIB II.)
ServerIndex	The identification number assigned to each RADIUS Authentication server that the client shares a secret with.
AuthServerAddress	The (conceptual) table listing the RADIUS authentication servers with which the client shares a secret.

ClientServerPortNumber	The UDP port the client is using to send requests to this server.
ClientRoundTripTime	The time interval (in hundredths of a second) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
ClientAccessRequests	The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.
ClientAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
ClientAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
ClientAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from this server.
ClientAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.
ClientAccessResponses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or Signature attributes or known types are not included as malformed access responses.
ClientBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Signature attributes received from this server.
ClientPendingRequests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject or Access-Challenge, a timeout or retransmission.
ClientTimeouts	The number of authentication timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
ClientUnknownTypes	The number of RADIUS packets of unknown type which were received from this server on the authentication port
ClientPacketsDropped	The number of RADIUS packets of which were received from this server on the authentication port and dropped for some other reason.

Layer 3 Feature

This folder in the **Monitoring** section will display information concerning settings configured in **Layer 3 IP Networking** of the **Configuration** folder. These settings and parameters have been previously described in **Section 6** of this manual, under **Layer 3 IP Networking**.

Browse IP Address Table

The **Browse IP Address Table** may be found in the **Monitoring** menu in the **Layer 3 Feature** folder. The **Browse IP Address Table** is a read only screen where the user may view IP addresses discovered by the Switch. To search a specific IP address, enter it into the field labeled **IP Address** at the top of the screen and click **Find** to begin your search.

IP Address		0.0.0.0	Find
IP Address Table			
Interface	IP Address	Port	Learned
System	10.0.25.1	3:1	Dynamic
System	10.0.58.4	3:1	Dynamic
System	10.1.1.101	3:1	Dynamic
System	10.1.1.102	3:1	Dynamic
System	10.1.1.103	3:1	Dynamic
System	10.1.1.151	3:1	Dynamic
System	10.1.1.152	3:1	Dynamic
System	10.1.1.157	3:1	Dynamic
System	10.1.1.161	3:1	Dynamic
System	10.1.1.162	3:1	Dynamic
System	10.1.1.163	3:1	Dynamic
System	10.1.1.164	3:1	Dynamic
System	10.1.1.166	3:1	Dynamic
System	10.1.1.168	3:1	Dynamic
System	10.1.1.169	3:1	Dynamic
System	10.1.1.170	3:1	Dynamic
System	10.1.1.171	3:1	Dynamic
System	10.1.1.172	3:1	Dynamic
System	10.1.1.173	3:1	Dynamic
System	10.1.1.174	3:1	Dynamic

Total Entries: 317

Next

Figure 9- 24. IP Address Table

Browse Routing Table

The **Browse Routing Table** window may be found in the **Monitoring** menu in the **Layer 3 Feature** folder. This screen shows the current IP routing table of the Switch. To find a specific IP route, enter an IP address into the **Destination Address** field along with a proper subnet mask into the **Mask** field and click **Find**.

Destination Address	<input type="text" value="0.0.0.0"/>				
Mask	<input type="text" value="0.0.0.0"/>	<input type="button" value="Find"/>			
Routing Table					
IP Address	Netmask	Gateway	Interface	Cost	Protocol
10.0.0.0	255.0.0.0	0.0.0.0	System	1	Local
Total Entries: 1					

Figure 9- 25. Browse Routing Table window

Browse ARP Table

The **Browse ARP Table** window may be found in the **Monitoring** menu in the **Layer 3 Feature** folder. This window will show current ARP entries on the Switch. To search a specific ARP entry, enter an interface name into the **Interface Name** or an **IP address** and click **Find**. To clear the **ARP Table**, click **Clear All**.

Interface Name	<input type="text"/>		
IP Address	<input type="text" value="0.0.0.0"/>	<input type="button" value="Find"/> <input type="button" value="Clear All"/>	
ARP Table			
Interface Name	IP Address	MAC Address	Type
System	10.0.0.0	ff-ff-ff-ff-ff-ff	Local/Broadcast
System	10.0.0.107	00-80-c8-34-56-79	Dynamic
System	10.0.46.1	00-80-c8-91-15-eb	Dynamic
System	10.0.51.12	00-50-ba-da-00-1d	Dynamic
System	10.1.1.2	00-05-5d-19-a5-ab	Static
System	10.1.1.101	00-50-ba-15-48-56	Dynamic
System	10.1.1.102	00-50-ba-97-d7-c0	Dynamic
System	10.1.1.151	00-50-ba-70-d6-d0	Dynamic
System	10.1.1.152	00-13-00-00-00-01	Dynamic
System	10.1.1.154	00-50-ba-97-d9-56	Dynamic
System	10.1.1.157	00-50-ba-71-20-d6	Dynamic
System	10.1.1.161	00-50-ba-70-e4-89	Dynamic
System	10.1.1.166	00-50-ba-70-e4-58	Dynamic
System	10.1.1.167	00-50-ba-70-e4-45	Dynamic
System	10.1.1.168	00-50-ba-70-e4-57	Dynamic
System	10.1.1.169	00-50-ba-70-e4-4e	Dynamic
System	10.1.1.170	00-50-ba-70-e4-7a	Dynamic
System	10.1.1.171	00-50-ba-70-cc-19	Dynamic
System	10.1.1.172	00-50-ba-70-e4-49	Dynamic
System	10.1.1.173	00-50-ba-70-e4-6e	Dynamic
Total Entries: 306			<input type="button" value="Next"/>

Figure 9- 26. Browse ARP Table window

Browse IP Multicast Forwarding Table

The **Browse IP Multicast Forwarding Table** window may be found in the **Monitoring** menu in the **Layer 3 Feature** folder. This window will show current IP multicasting information on the Switch. To search a specific entry, enter an multicast group IP address into the **Multicast Group** field or a **Source IP** address and click **Find**.

Multicast Group	<input type="text" value="0.0.0.0"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Source IP Address	<input type="text" value="0.0.0.0"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Find"/>						
IP Multicast Forwarding Table						
Multicast Group	Source IP Address	Source Netmask	Upstream Neighbor	Expire Time	Protocol	
224.2.140.247	10.0.0.0	255.0.0.0	10.100.100.251	109	DVMRP	
224.2.142.32	10.0.0.0	255.0.0.0	10.100.100.251	105	DVMRP	
229.55.150.208	10.0.0.0	255.0.0.0	10.100.100.251	118	DVMRP	
239.255.255.250	10.0.0.0	255.0.0.0	10.100.100.251	39	DVMRP	
Total Entries: 4						

Figure 9- 27. Browse IP Multicast Forwarding Table

Browse IP Multicast Interface Table

The **Browse IP Multicast Interface Table** window may be found in the **Monitoring** menu in the **Layer 3 Feature** folder. This window will show current IP multicasting interfaces located on the Switch. To search a specific entry, enter an multicast interface name into the **Interface Name** field or choose a **Protocol** from the pull down list and click **Find**.

Interface Name	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Protocol	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Find"/>					
IP Multicast Interface Table					
Interface Name	IP Address	Source Mask	Multicast Routing		
System	10.53.13.100	255.0.0.0	INACT		
Total Entries: 1					

Figure 9- 28. Browse IP Multicast Interface Table

Browse IGMP Group Table

The **Browse IGMP Group Table** window may be found in the **Monitoring** menu in the **Layer 3 Feature** folder. This window will show current IGMP group entries on the Switch. To search a specific IGMP group entry, enter an interface name into the **Interface Name** field or a **Multicast Group** IP address and click **Find**.

Interface Name	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Multicast Group	<input type="text" value="0.0.0.0"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Find"/>									
IGMP Group Table									
Interface Name	Multicast Group	Last Reporter IP	IP Querier	IP Expire	Group Filter Mode	V1 Host Timer	V2 Host Timer	Detail	
Total Entries: 0									

Figure 9- 29. Browse IGMP Group Table

To view the specific details for an entry, click the corresponding [View](#) button.

OSPF Monitor

This section offers windows regarding OSPF (Open Shortest Path First) information on the Switch, including the **OSPF LSDB Table**, **OSPF Neighbor Table** and the **OSPF Virtual Neighbor Table**. To view these tables, open the **Monitoring** folder and click **OSPF Monitoring**.

Browse OSPF LSDB Table

This table can be found in the **OSPF Monitoring** folder by clicking on the **Browse OSPF LSDB Table** link. The **OSPF Link-State Database Table** displays the current link-state database in use by the OSPF routing protocol on a per-OSPF area basis.

Search Type	ALL				
Area ID	0.0.0.0				
Adv. Router ID	0.0.0.0				
LSDB Type	RTRLink				Find
OSPF LSDB Table					
Area ID	LSDB Type	Adv. Router ID	Link State ID	Cost	Sequence
0.0.0.0	RTRLink	1.0.0.0	1.0.0.0	*	0x80000007
0.0.0.0	RTRLink	2.0.0.0	2.0.0.0	*	0x80000005
0.0.0.0	RTRLink	10.9.68.96	10.9.68.96	*	0x80000018
0.0.0.0	RTRLink	14.99.68.254	14.99.68.254	*	0x80000004
0.0.0.0	RTRLink	211.1.1.251	211.1.1.251	*	0x80000006
0.0.0.0	NETLink	10.9.68.96	10.9.68.96	*	0x80000001
0.0.0.0	Summary	1.0.0.0	11.1.1.1	10	0x80000002
0.0.0.0	Summary	2.0.0.0	11.1.1.1	11	0x80000002
0.0.0.0	Summary	211.1.1.251	11.1.1.1	10	0x80000001
0.0.0.0	Summary	1.0.0.0	11.1.1.2	10	0x80000002
0.0.0.0	Summary	2.0.0.0	11.1.1.2	11	0x80000002
0.0.0.0	Summary	211.1.1.251	11.1.1.2	10	0x80000001
0.0.0.0	Summary	1.0.0.0	11.1.1.3	10	0x80000002
0.0.0.0	Summary	2.0.0.0	11.1.1.3	11	0x80000002
0.0.0.0	Summary	211.1.1.251	11.1.1.3	10	0x80000001
0.0.0.0	Summary	1.0.0.0	201.0.0.0	1	0x80000003
0.0.0.0	Summary	211.1.1.251	201.0.0.0	1	0x80000001
0.0.0.0	Summary	2.0.0.0	201.1.0.0	1	0x80000002
0.0.0.0	Summary	2.0.0.0	201.2.0.0	2	0x80000002
0.0.0.0	Summary	211.1.1.251	201.2.0.0	1	0x80000002
					Next

Figure 9- 30. Browse OSPF LSDB Table

The user may search for a specific entry by entering the following information into the fields at the top of the screen:

To browse the **OSPF LSDB Table**, first select which browse method to use in the **Search Type** field. The choices are *All*, *Area ID*, *Advertise Router ID*, *LSDB*, *Area ID & Advertise Router ID*, *Area ID & LSDB*, and *Advertise Router ID & LSDB*.

If *Area ID* is selected as the browse method, users must enter the IP address in the **Area ID** field, and then click *Find*.

If *Adv. Router ID* is selected, users must enter the IP address in the **Advertisement Router ID** field, and then click **Find**.

If *LSDB* is selected, users must select the type of link state (*RtrLink*, *NetLink*, *Summary*, *ASummary* and *ASExtLink*) in the **LSDB Type** field, and then click **Find**.

The following fields are displayed in the **OSPF LSDB Table**:

Parameter	Description										
Area ID	Allows the entry of an OSPF Area ID. This Area ID will then be used to search the table, and display an entry – if there is one.										
LSDB Type	Displays which one of eight types of link advertisements by which the current link was discovered by the Switch: <i>All</i> , Router link (<i>RTRLINK</i>), Network link (<i>NETLINK</i>), Summary link (<i>Summary</i>), Autonomous System link (<i>ASSummary</i>), Autonomous System external link (<i>ASEExternal</i>), MCGLink (<i>Multicast Group</i>), and NSSA (<i>Not So Stubby Area</i>)										
Adv. Router ID	Displays the Advertising Router's ID.										
Link State ID	This field identifies the portion of the Internet environment that is being described by the advertisement. The contents of this field depend on the advertisement's LS type. <table border="1"> <thead> <tr> <th>LS Type</th> <th>Link State ID</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>The originating router's Router ID.</td> </tr> <tr> <td>2</td> <td>The IP interface address of the network's Designated Router.</td> </tr> <tr> <td>3</td> <td>The destination network's IP address.</td> </tr> <tr> <td>4</td> <td>The Router ID of the described AS boundary router.</td> </tr> </tbody> </table>	LS Type	Link State ID	1	The originating router's Router ID.	2	The IP interface address of the network's Designated Router.	3	The destination network's IP address.	4	The Router ID of the described AS boundary router.
LS Type	Link State ID										
1	The originating router's Router ID.										
2	The IP interface address of the network's Designated Router.										
3	The destination network's IP address.										
4	The Router ID of the described AS boundary router.										
Cost	Displays the cost of the table entry.										
Sequence	Displays a sequence number corresponding to number of times the current link has been advertised as changed.										

Browse OSPF Neighbor Table

This table can be found in the **OSPF Monitoring** folder by clicking on the **Browse OSPF Neighbor Table** link. Routers that are connected to the same area or segment become neighbors in that area. Neighbors are elected via the Hello protocol. IP multicast is used to send out Hello packets to other routers on the segment. Routers become neighbors when they see themselves listed in a Hello packet sent by another router on the same segment. In this way, two-way communication is guaranteed to be possible between any two neighbor routers. This table displays OSPF neighbors of the Switch.

IP Address	<input type="text" value="0.0.0.0"/>	<input type="button" value="Find"/>			
OSPF Neighbor Table					
IP Address	Neighbor Router ID	Option	Priority	State	Events
Total Entries: 0					

Figure 9- 31. OSPF Neighbor Table

To search for OSPF neighbors, enter an IP address and click **Find**. Valid OSPF neighbors will appear in the **OSPF Neighbor Table** below.

OSPF Virtual Neighbor

This table can be found in the **OSPF Monitoring** folder by clicking on the **Browse OSPF Virtual Neighbor Table** link. This table displays a list of **Virtual OSPF Neighbors** of the Switch. The user may choose specifically search a virtual neighbor by using one of the two search options at the top of the screen, which are:

Transit Area ID	<input type="text" value="0.0.0.0"/>				
Virtual Neighbor Router ID	<input type="text" value="0.0.0.0"/>		<input type="button" value="Browse"/>		
OSPF Virtual Neighbor Table					
Transit Area ID	Virtual Neighbor Router ID	Virtual Neighbor IP Address	Virtual Neighbor Option	Virtual Neighbor State	Events
255.255.255.255	2.0.0.0	201.1.1.250	2	Full	5
Total Entries: 1					

Figure 9- 32.OSPF Virtual Neighbor Table

Parameter	Description
Transit Area ID	Allows the entry of an OSPF Area ID – previously defined on the Switch – that allows a remote area to communicate with the backbone (area 0). A Transit Area cannot be a Stub Area or a Backbone Area.
Virtual Neighbor Router ID	The OSPF router ID for the remote router. This IP address uniquely identifies the remote area's Area Border Router.

DVMRP Monitoring

This menu allows the **DVMRP** (Distance-Vector Multicast Routing Protocol) to be monitored for each IP interface defined on the Switch. This folder, found in the **Monitoring** folder, offers 3 screens for monitoring; **Browse DVMRP Routing Table**, **Browse DVMRP Neighbor Address Table** and **Browse DVMRP Routing Next Hop Table**. Information on DVMRP and its features in relation to the xStack[®] DES-6500 chassis switch can be found in Section 6, under **IP Multicast Routing Protocol**.

Browse DVMRP Routing Table

Multicast routing information is gathered and stored by DVMRP in the **DVMRP Routing Table**, which may be found in the **Monitoring** folder under **Browse DVMRP Monitoring**, contains one row for each port in a DVMRP mode. Each routing entry contains information about the source and multicast group, and incoming and outgoing interfaces. You may define your search by entering a **Source IP Address** and its subnet mask into the fields at the top of the page.

Source IP Address	<input type="text" value="0.0.0.0"/>					
Source Netmask	<input type="text" value="0.0.0.0"/>	<input type="button" value="Browse"/>				
DVMRP Routing Table						
Source IP Address	Source Netmask	Upstream Neighbor	Metric	Learned	Interface Name	Expire Time
10.0.0.0	255.0.0.0	10.100.100.251	1	Local	n10	---
11.0.0.0	255.0.0.0	10.20.6.251	2	Dynamic	n10	86
12.0.0.0	255.0.0.0	10.20.6.251	3	Dynamic	n10	86
13.0.0.0	255.0.0.0	10.20.6.251	4	Dynamic	n10	86
192.1.0.0	255.255.0.0	10.20.6.251	2	Dynamic	n10	86
192.2.0.0	255.255.0.0	10.20.6.251	4	Dynamic	n10	86
192.168.1.0	255.255.255.0	10.254.254.251	2	Dynamic	n10	90
201.1.0.0	255.255.0.0	201.1.1.1	1	Local	n2001	---
201.2.0.0	255.255.0.0	201.2.1.1	1	Local	n2002	---
201.3.0.0	255.255.0.0	201.3.1.1	1	Local	n2003	---
201.4.0.0	255.255.0.0	201.4.1.1	1	Local	n2004	---
201.5.0.0	255.255.0.0	201.5.1.1	1	Local	n2005	---
201.6.0.0	255.255.0.0	201.6.1.1	1	Local	n2006	---
201.7.0.0	255.255.0.0	201.7.1.1	1	Local	n2007	---
201.8.0.0	255.255.0.0	201.8.1.1	1	Local	n2008	---
223.255.255.252	255.255.255.252	10.20.6.251	2	Dynamic	n10	86
Total Entries: 16						

Figure 9- 33. DVMRP Routing Table

Browse DVMRP Neighbor Table

This table, found in the **Monitoring** menu under **DVMRP Monitor > Browse DVMRP Neighbor Table** contains information about DVMRP neighbors of the Switch. To search this table, enter either an **Interface Name** or **Neighbor Address** into the respective field and click the **Find** button. DVMRP neighbors of that entry will appear in the **DVMRP Neighbor Table** below.

Interface Name	<input type="text"/>		
Neighbor Address	<input type="text" value="0.0.0.0"/>		
Net Mask	<input type="text" value="255.255.255.0"/>		<input type="button" value="Find"/>
DVMRP Neighbor Table			
Interface Name	Neighbor Address	Generation ID	Expire Time
Total Entries: 0			

Figure 9- 34. DVMRP Neighbor Table

Browse DVMRP Routing Next Hop Table

The **DVMRP Routing Next Hop Table** contains information regarding the next-hop for forwarding multicast packets on outgoing interfaces. Each entry in the **DVMRP Routing Next Hop Table** refers to the next-hop of a specific source to a specific multicast group address. This table is found in the **Monitoring** menu under **DVMRP Monitoring**, with the heading **Browse DVMRP Routing Next Hop Table**. To search this table, enter either an **Interface Name** or **Source IP Address** into the respective field and click the **Find** button. The next hop of that DVMRP Routing entry will appear in the **DVMRP Routing Next Hop Table** below.

Interface Name	<input type="text"/>		
Source IP Address	<input type="text" value="0.0.0.0"/>		
Net Mask	<input type="text" value="255.255.255.0"/>		<input type="button" value="Find"/>
DVMRP Routing Next Hop Table			
Source IP Address	Source Mask	Interface Name	Type
Total Entries: 0			

Figure 9- 35. DVMRP Routing Next Hop Table

PIM Monitoring

Multicast routers use **Protocol Independent Multicast (PIM)** to determine which other multicast routers should receive multicast packets. To find out more information concerning PIM and its configuration on the Switch, see the **IP Multicast Routing Protocol** chapter of Section 6, **Configuration**.

Browse PIM Neighbor Table

The **PIM Neighbor Table** contains information regarding each of a router's PIM neighbors. This screen may be found by clicking **Monitoring > PIM Monitor > Browse PIM Neighbor Table**. To search this table, enter either an **Interface Name** or **Neighbor IP Address** into the respective field and click the **Find** button. PIM neighbors of that entry will appear in the **PIM Neighbor Table** below.

Interface Name	<input type="text"/>	
Neighbor IP Address	<input type="text" value="0.0.0.0"/>	<input type="button" value="Find"/>
PIM Neighbor Table		
Interface Name	Neighbor IP Address	Expire Time
n10	10.9.68.96	101
Total Entries: 1		

Figure 12- 1. PIM Neighbor Table

PIM IP MRoute Table

The PIM IP MRoute Table is used to view information regarding the multicast data route entries in the Switch. This screen may be found by clicking **Monitoring > Layer 3 Feature > PIM Monitor > Browse PIM IP MRoute Table**.

PIM IP MRoute Table							
Group Address	Source Address	Upstream Assert Timer	Assert Metric	Assert Metric Pref	Assert RPT Bit	Flag	Type
225.10.10.15	10.62.58.78	0	0	0	0	spt	(S,G)
229.55.150.208	10.6.51.1	0	0	0	0	spt	(S,G)
229.55.150.208	10.38.45.151	0	0	0	0	spt	(S,G)
229.55.150.208	10.38.45.192	0	0	0	0	spt	(S,G)
229.55.150.208	10.51.16.1	0	0	0	0	spt	(S,G)
229.55.150.208	10.59.23.10	0	0	0	0	spt	(S,G)
239.255.255.250	10.26.66.3	0	0	0	0	spt	(S,G)
239.255.255.250	10.48.75.101	0	0	0	0	spt	(S,G)
239.255.255.250	10.60.97.12	0	0	0	0	spt	(S,G)
Total Entries: 9							

Figure 12- 2. PIM IP MRoute Table

Browse PIM RP Set Table

The following window is used to assess information regarding the Rendezvous Point (RP) Set on the Switch. This screen may be found by clicking **Monitoring > Layer 3 Feature > PIM Monitor > Browse PIM RP Set Table**.

Bootstrap Router : 0.0.0.0				
PIM RP Set Table				
Group Address	RP Address	Holdtime	Expired Time	Type
224.0.0.0	11.1.1.252	0	0	static
239.0.0.0	31.1.1.246	0	0	static
239.0.0.1	31.1.1.246	0	0	static
239.0.0.2	31.1.1.246	0	0	static
239.0.0.3	31.1.1.246	0	0	static
239.0.0.4	31.1.1.246	0	0	static
239.0.0.5	31.1.1.246	0	0	static
239.0.0.6	31.1.1.246	0	0	static
239.0.0.7	31.1.1.246	0	0	static
239.0.0.8	31.1.1.246	0	0	static
239.0.0.9	31.1.1.246	0	0	static
239.0.0.10	31.1.1.246	0	0	static
239.0.0.11	31.1.1.246	0	0	static
239.0.0.12	31.1.1.246	0	0	static
239.0.0.13	31.1.1.246	0	0	static
239.0.0.14	31.1.1.246	0	0	static
239.0.0.15	31.1.1.246	0	0	static
239.0.0.16	31.1.1.246	0	0	static
239.0.0.17	31.1.1.246	0	0	static
239.0.0.18	31.1.1.246	0	0	static

Total Entries: 20

Figure 12- 3. PIM RP Set Table

Switch Maintenance

- TFTP Services*
- Ping Test*
- TraceRoute*
- Save Configuration*
- Reset*
- Reboot Services*
- Logout*

TFTP Services

Trivial File Transfer Protocol (TFTP) services allow the Switch’s 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.

Download Firmware

To update the Switch’s firmware, open the **TFTP Services** folder in the **Maintenance** folder and then click the **Download Firmware** link:

Figure 10- 1. Download Firmware window

Unit Number – Select which slot in the chassis for which to update the firmware. This allows the selection of a particular slot from slot stack if you have properly inserted the line cards in the chassis. **All** indicates all slots in the chassis will download the same firmware.

Enter the IP address of the TFTP server in the **Server IP Address** field.

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 D drive of the TFTP server.

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 – such as NetSight, or can be obtained as a separate program.

Click **Start** to record the IP address of the TFTP server and initiate the file transfer.



NOTE: Please check the firmware version of the CPU and line cards of the xStack® DES-6500 chassis switch before upgrading to firmware release 3.00.B33. For firmware upgrading information, cautions and procedures for release 3, please see Appendix B at the end of the manual.



Due to a backward compatibility issue, when a user upgrades to R3 firmware (3.00-B33), all settings previously configured for any ACL function (CPU ACL included) on the Switch will be lost. We recommend that the user save a configuration file of current settings before upgrading to R3 firmware.

Download Configuration

To download a configuration file from a TFTP server, click on the **TFTP Service** folder in the **Maintenance** folder and then the **Download Configuration File** link:

Download Configuration	
Server IP Address	0.0.0.0
File Name	
Increment	<input type="checkbox"/>
Start	

Figure 10- 2. Download Configuration window

Enter the IP address of the TFTP server and specify the location of the switch configuration file on the TFTP server. Click the **Increment** check box to download a part of this file only.

Click **Start** to initiate the file transfer.

Upload Configuration

To upload the Switch's settings to a TFTP server, click on the **TFTP Service** folder in the **Maintenance** folder and then click the **Upload Configuration** link:

Upload Configuration	
Server IP Address	0.0.0.0
File Name	
Start	

Figure 10- 3. Upload Configuration window

Enter the IP address of the TFTP server and the path and filename for the configuration file on the TFTP server.

Click **Start** to initiate the file transfer.

Upload History Log

To upload the Switch history log file to a TFTP server, open the **TFTP Service** folder in the **Maintenance** folder and then click the **Upload Log** link:

Upload History Log	
Server IP Address	0.0.0.0
File Name	
Start	

Figure 10- 4. Upload Log window

Enter the IP address of the TFTP server and the path and filename for the history log on the TFTP server.

Click **Start** to record the IP address of the TFTP server and to initiate the file transfer.

Ping Test

Ping is a small program that sends ICMP Echo packets to the IP address you specify. The destination node then responds to or "echoes" the packets sent from the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.

The user may use Infinite times radio button, in the **Repeat Pinging for:** field, which will tell the ping program to keep sending ICMP Echo packets to the specified IP address until the program is stopped. The user may opt to choose a specific number of times to ping the **Target IP Address** by clicking its radio button and entering a number between 1 and 255. Click **Start** to initiate the Ping program.

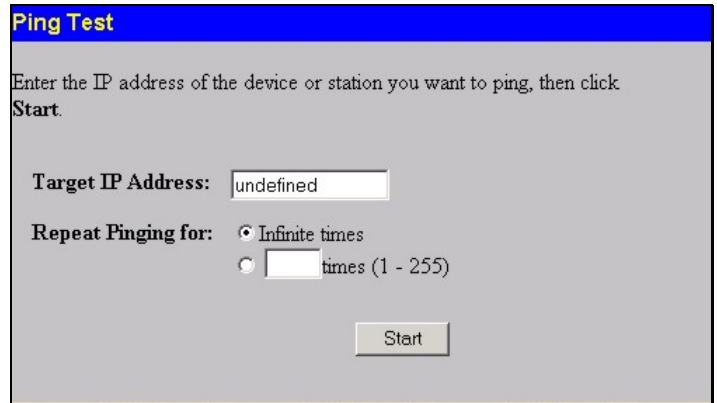


Figure 10- 5. Ping Test

Traceroute

The following window will aid the user in back tracing the route taken by a packet before arriving at the Switch. When initiated, the Traceroute program will display the IP addresses of the previous hops a packet takes from the **Target IP Address** entered in the window, until it reaches the Switch.

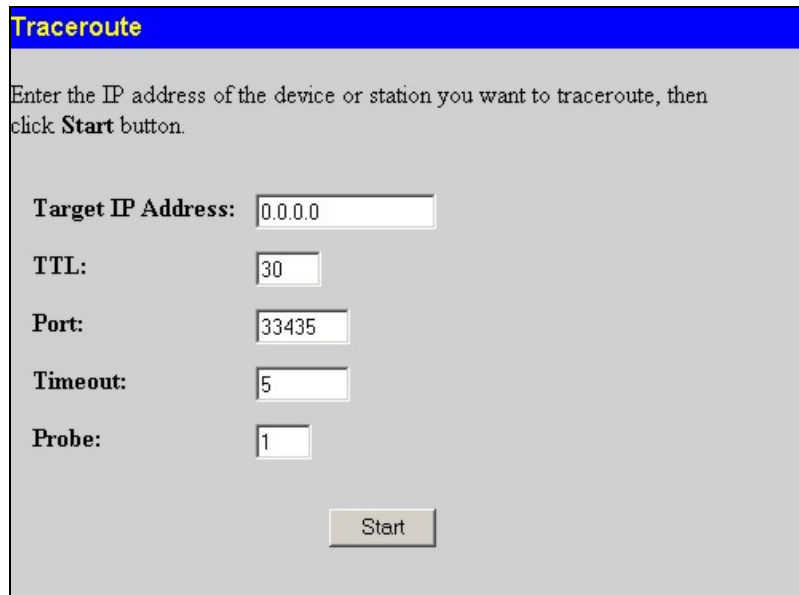


Figure 10- 6. Traceroute window

To trace the route of a packet, set the following parameters located in this window, and click **Start**.

Parameter	Description
Target IP Address	Enter the IP address of the computer to be traced.
TTL	The time to live value of the trace route request. This is the maximum number of routers the traceroute command will cross while seeking the network path between two devices.
Port	The virtual port number. The port number must be above 1024. The value range is from 30000 to 64900.
Timeout	Defines the time-out period while waiting for a response from the remote device. The user may choose an entry between 1 and 65535 seconds.
Probe	The probe value is the number of times the Switch will send probe packets to the next hop on the intended traceroute path. The default is 1.

Save Configuration

The xStack® DES-6500 chassis switch has two levels of memory, normal RAM and non-volatile or NV-RAM. Configuration changes are made effective clicking the **Apply** button. 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, click on the **Save** button in the **Save Changes** page, as shown below.

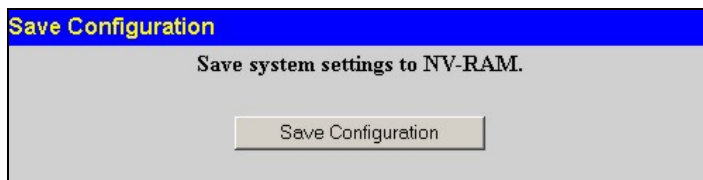


Figure 10- 7. Save Changes screen

Reset

The **Reset** function has several options when resetting the Switch. Some of the current configuration parameters can be retained while resetting all other configuration parameters to their factory defaults.



NOTE: Only the **Reset System** option will enter the factory default parameters into the Switch's non-volatile RAM, and then restart the Switch. All other options enter the factory defaults into the current configuration, but do not save this configuration. **Reset System** will return the Switch's configuration to the state it was when it left the factory

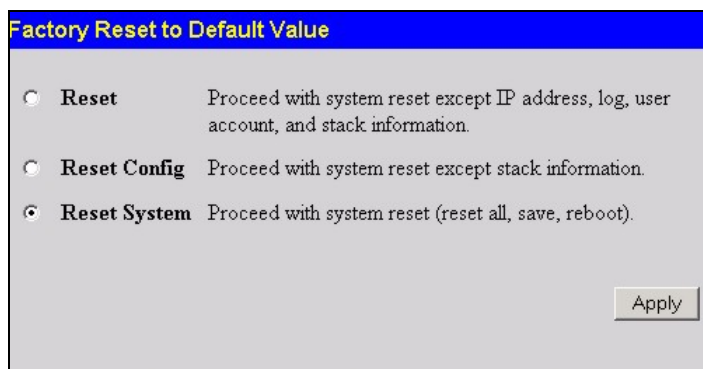


Figure 10- 8. Factory Reset to Default Value window

Reboot Device

The following menu is used to restart the Switch.



Figure 10- 9. Reboot System window

Clicking the **Yes** click-box will instruct the Switch to save the current configuration to non-volatile RAM before restarting the Switch.

Clicking the **No** click-box instructs the Switch not to save the current configuration before restarting the Switch. All of the configuration information entered from the last time **Save Changes** was executed, will be lost.

Click the **Restart** button to restart the Switch.

Logout

Use the **Logout** page to logout of the Switch's Web-based management agent by clicking on the **Log Out** button.

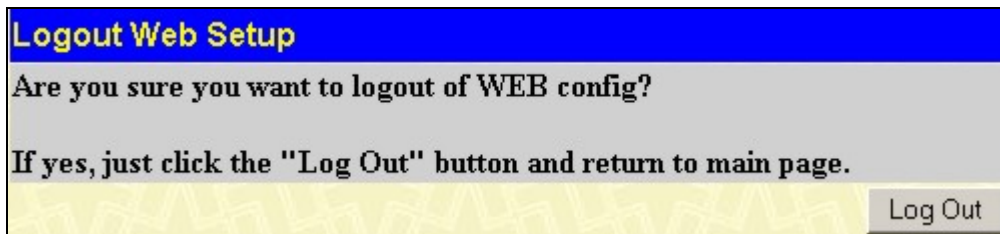


Figure 10- 10. Logout window

D-Link Single IP Management

Single IP Management (SIM) Overview

Topology

Firmware Upgrade

Configuration Backup/Restore

Single IP Management (SIM) Overview

Simply put, D-Link Single IP Management is a concept that will stack switches together over Ethernet instead of using stacking ports or modules. There are some advantages in implementing the "Single IP Management" feature:

1. SIM can simplify management of small workgroups or wiring closets while scaling the network to handle increased bandwidth demand.
2. SIM can reduce the number of IP address needed in your network.
3. SIM can eliminate any specialized cables for stacking connectivity and remove the distance barriers that typically limit your topology options when using other stacking technology.

Switches using D-Link Single IP Management (labeled here as SIM) must conform to the following rules:

- SIM is an optional feature on the Switch and can easily be enabled or disabled through the Command Line Interface or Web Interface. SIM grouping has no effect on the normal operation of the Switch in the user's network.
- There are three classifications for switches using SIM. The **Commander Switch (CS)**, which is the master switch of the group, **Member Switch (MS)**, which is a switch that is recognized by the CS as a member of a SIM group, and a **Candidate Switch (CaS)**, which is a Switch that has a physical link to the SIM group but has not been recognized by the CS as a member of the SIM group.
- A SIM group can only have one Commander Switch (CS).
- All switches in a particular SIM group must be in the same IP subnet (broadcast domain). Members of a SIM group cannot cross a router.
- A SIM group accepts up to 32 switches (numbered 0-31), including the Commander Switch (numbered 0).

There is no limit to the number of SIM groups in the same IP subnet (broadcast domain), however a single switch can only belong to one group.

If multiple VLANs are configured, the SIM group will only utilize the default VLAN on any switch.

SIM allows intermediate devices that do not support SIM. This enables the user to manage switches that are more than one hop away from the CS.

The SIM group is a group of switches that are managed as a single entity. The xStack® DES-6500 chassis switch may take on three different roles:

1. **Commander Switch (CS)** - This is a switch that has been manually configured as the controlling device for a group, and takes on the following characteristics:
 - It has an IP Address.
 - It is not a command switch or member switch of another Single IP group.
 - It is connected to the member switches through its management VLAN.
2. **Member Switch (MS)** - This is a switch that has joined a single IP group and is accessible from the CS, and it takes on the following characteristics:
 - It is not a CS or MS of another IP group.
 - It is connected to the CS through the CS management VLAN.
3. **Candidate Switch (CaS)** - This is a switch that is ready to join a SIM group but is not yet a member of the SIM group. The Candidate Switch may join the SIM group of the xStack® DES-6500 chassis switch by manually configuring it to be

a MS of a SIM group. A switch configured as a CaS is not a member of a SIM group and will take on the following characteristics:

- It is not a CS or MS of another Single IP group.
- It is connected to the CS through the CS management VLAN

The following rules also apply to the above roles:

- Each device begins in a Commander state.
- CS's must change their role to CaS and then to MS, to become a MS of a SIM group. Thus, the CS cannot directly be converted to a MS.
- The user can manually configure a CS to become a CaS.

A MS can become a CaS by:

- Being configured as a CaS through the CS.
- If report packets from the CS to the MS time out.
- The user can manually configure a CaS to become a CS
- The CaS can be configured through the CS to become a MS.

After configuring one switch to operate as the CS of a SIM group, additional xStack® DES-6500 chassis switch may join the group by manually configuring the Switch to be a MS. The CS will then serve as the in band entry point for access to the MS. The CS's IP address will become the path to all MS's of the group and the CS's Administrator's password, and/or authentication will control access to all MS's of the SIM group.

With SIM enabled, the applications in the CS will redirect the packet instead of executing the packets. The applications will decode the packet from the administrator, modify some data, then send it to the MS. After execution, the CS may receive a response packet from the MS, which it will encode and send it back to the administrator.

When a CS becomes a MS, it automatically becomes a member of the first SNMP community (include read/write and read only) to which the CS belongs. However, if a MS has its own IP address, it can belong to SNMP communities to which other switches in the group, including the CS, do not belong.

SIM Using the Web Interface

All xStack® DES-6500 chassis switch are set as Candidate (CaS) switches as their factory default configuration and Single IP Management will be disabled. To enable SIM for the Switch using the Web interface, go to the **Single IP Management** folder and click the **SIM Settings** link, revealing the following window.



Figure 11- 1. SIM Settings window (disabled)

Change the **SIM State** to *Enabled* using the pull down menu and click **Apply**. The user must then change the Role State of the Device to Commander. The screen will then refresh and the **SIM Settings** window will look like this:

Figure 11- 2. SIM Settings window (enabled)

The following parameters can be set:

Parameters	Description
SIM State	Use the pull down menu to either enable or disable the SIM state on the Switch. <i>Disabled</i> will render all SIM functions on the Switch inoperable.
Role State	Use the pull down menu to change the SIM role of the Switch. The two choices are: <ul style="list-style-type: none"> • <i>Candidate</i> - A Candidate Switch (CaS) is not the member of a SIM group but is connected to a Commander Switch. This is the default setting for the SIM role. • <i>Commander</i> - Choosing this parameter will make the Switch a Commander Switch (CS). The user may join other switches to this Switch, over Ethernet, to be part of its SIM group. Choosing this option will also enable the Switch to be configured for SIM.
Discovery Interval	The user may set the discovery protocol interval, in seconds that the Switch will send out discovery packets. Returning information to a Commander Switch will include information about other switches connected to it. (Ex. MS, CaS). The user may set the Discovery Interval from 30 to 90 seconds.
Holdtime	This parameter may be set for the time, in seconds the Switch will hold information sent to it from other switches, utilizing the Discovery Interval . The user may set the hold time from 100 to 255 seconds.

Click **Apply** to implement the settings changed.

After enabling the Switch to be a Commander Switch (CS), the **Single IP Management** folder will then contain three added links to aid the user in configuring SIM through the web, including **Topology**, **Firmware Upgrade** and **Configuration Backup/Restore**.

Topology

The **Topology** window will be used to configure and manage the Switch within the SIM group and requires Java script to function properly on your computer.

The Java Runtime Environment on your server should initiate and lead you to the topology window, as seen below.

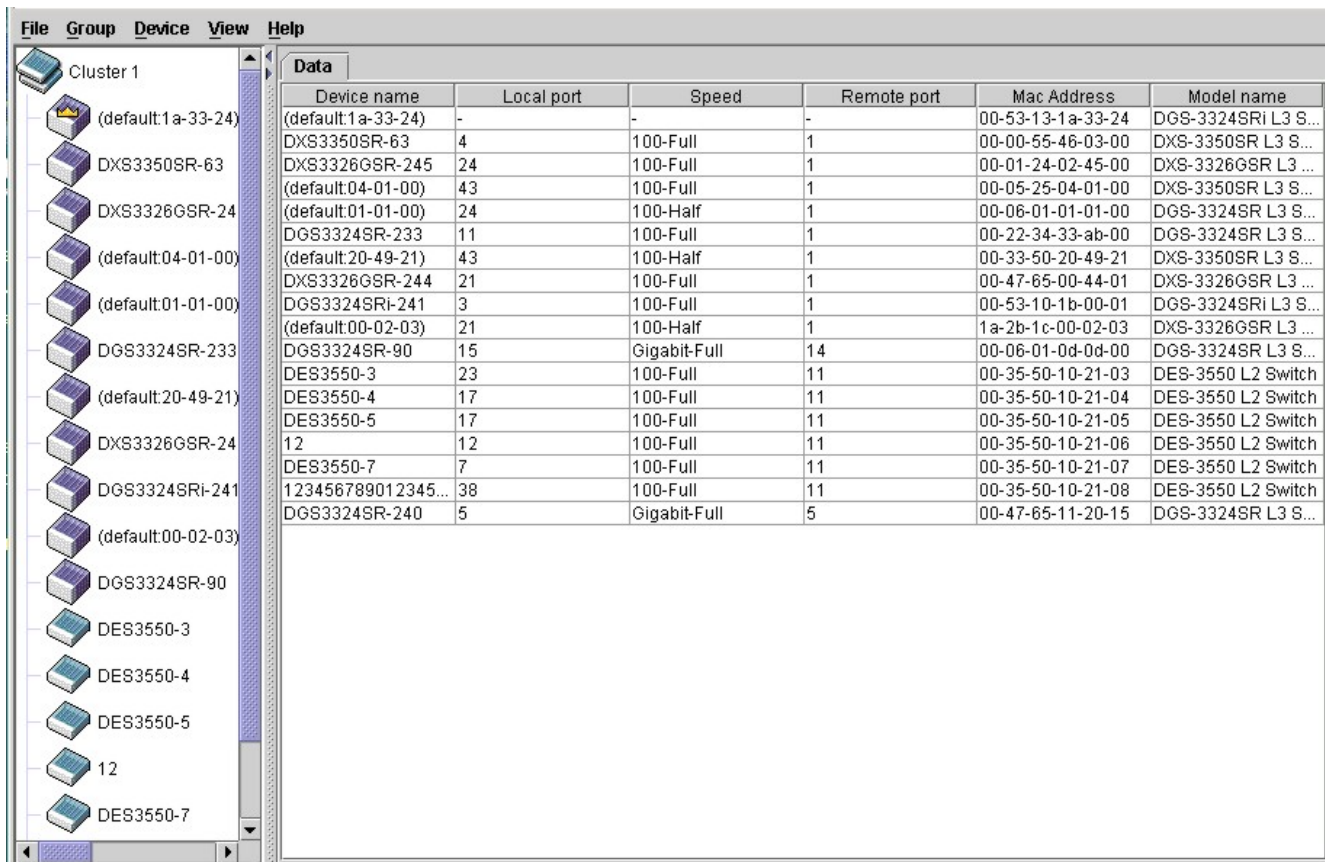


Figure 11- 3. Single IP Management window - Tree View

The Tree View window holds the following information under the Data tab:

Parameter	Description
Device Name	This field will display the Device Name of the switches in the SIM group configured by the user. If no Device Name is configured by the name, it will be given the name default and tagged with the last six digits of the MAC Address to identify it.
Local Port	Displays the number of the physical port on the CS that the MS or CaS is connected to. The CS will have no entry in this field.
Speed	Displays the connection speed between the CS and the MS or CaS.
Remote Port	Displays the number of the physical port on the MS or CaS that the CS is connected to. The CS will have no entry in this field.
MAC Address	Displays the MAC Address of the corresponding Switch.
Model Name	Displays the full Model Name of the corresponding Switch.

To view the **Topology Map**, click the View menu in the toolbar and then Topology, which will produce the following screen. The **Topology View** will refresh itself periodically (20 seconds by default).

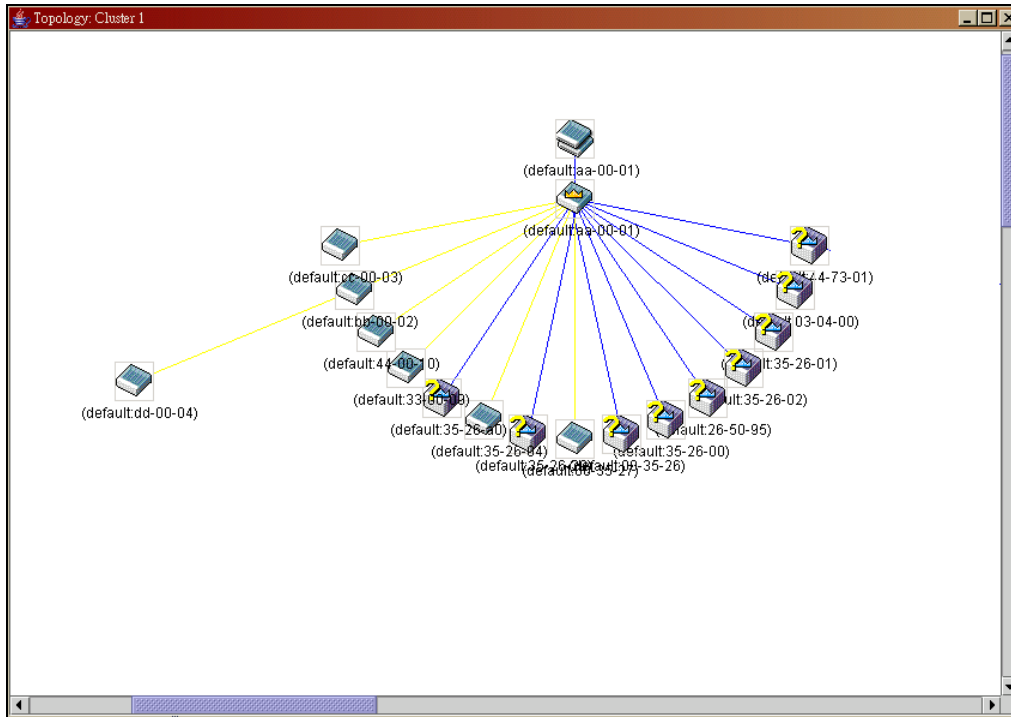













Figure 11- 4. Topology view

This screen will display how the devices within the Single IP Management Group are connected to other groups and devices. Possible icons in this screen are as follows:

Icon	Description
	Group
	Layer 2 commander switch
	Layer 3 commander switch
	Commander switch of other group
	Layer 2 member switch.
	Layer 3 member switch
	Member switch of other group
	Layer 2 candidate switch
	Layer 3 candidate switch
	Unknown device
	Non-SIM devices

Tool Tips

In the Topology view window, the mouse plays an important role in configuration and in viewing device information. Setting the mouse cursor over a specific device in the topology window (tool tip) will display the same information about a specific device as the Tree view does. See the window below for an example.

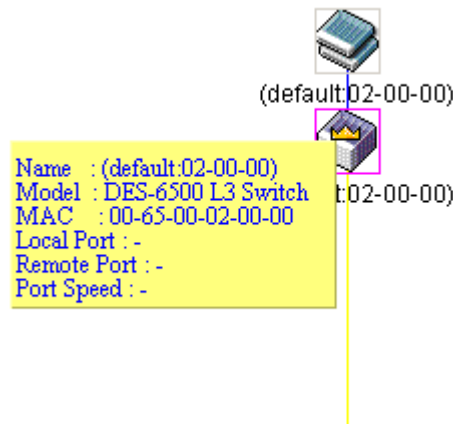


Figure 11- 5. Device Information Utilizing the Tool Tip

Setting the mouse cursor over a line between two devices will display the connection speed between the two devices, as shown below.

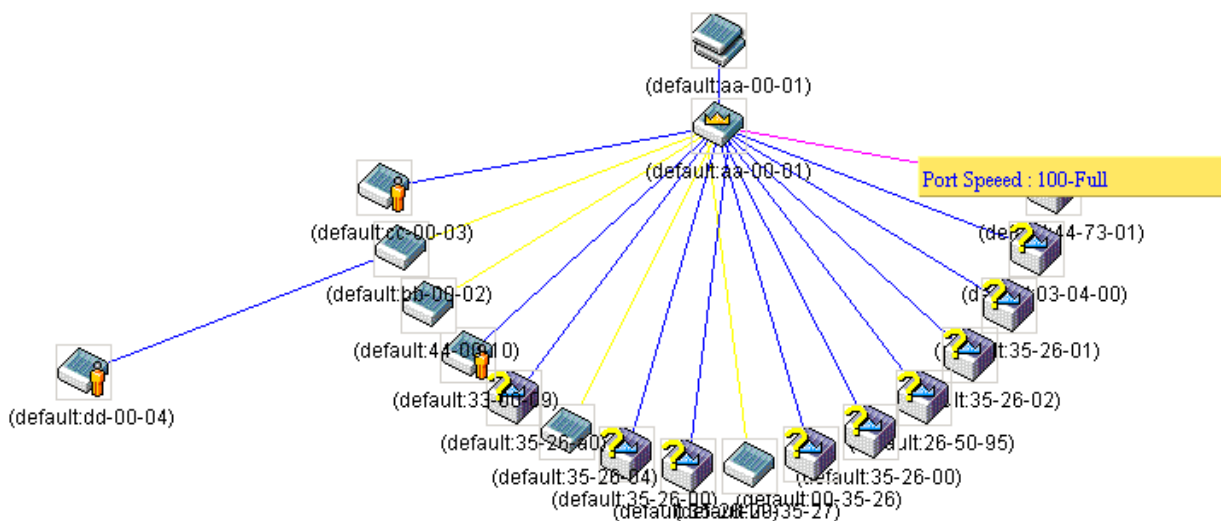


Figure 11- 6. Port Speed Utilizing the Tool Tip

Right Click

Right clicking on a device will allow the user to perform various functions, depending on the role of the Switch in the SIM group and the icon associated with it.

Group Icon

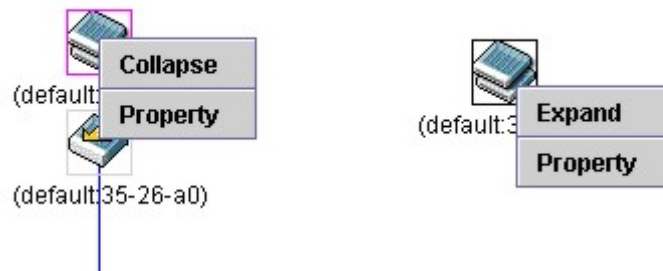


Figure 11- 7. Right Clicking a Group Icon

The following options may appear for the user to configure:

- **Collapse** - to collapse the group that will be represented by a single icon.
- **Expand** - to expand the SIM group, in detail.
- **Property** - to pop up a window to display the group information.

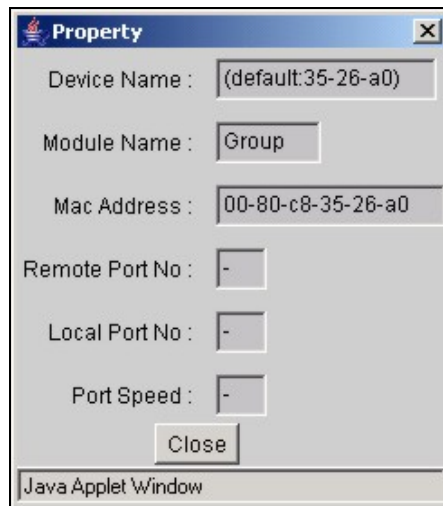


Figure 11- 8. Property window

Commander Switch Icon

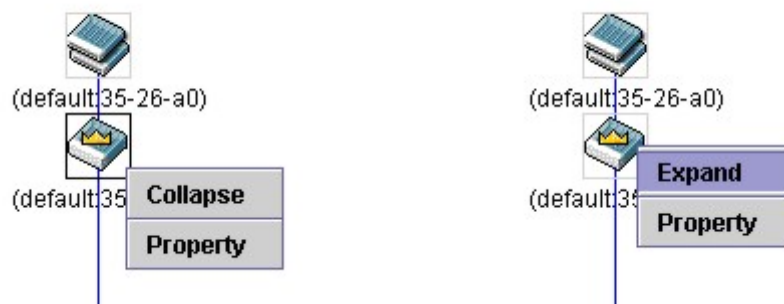


Figure 11- 9. Right Clicking a Commander Icon

The following options may appear for the user to configure:

- **Collapse** - to collapse the group that will be represented by a single icon.
- **Expand** - to expand the SIM group, in detail.
- **Property** - to pop up a window to display the group information.

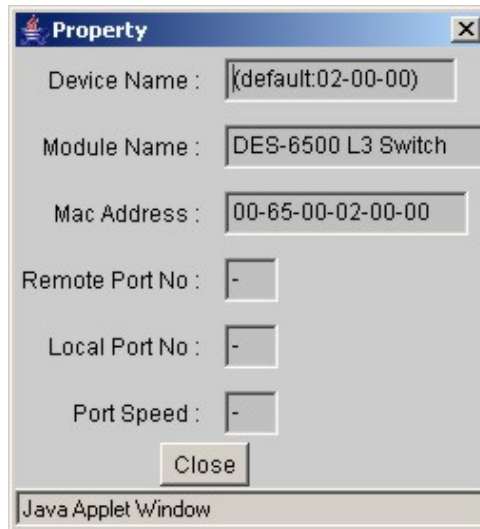


Figure 11- 10. Property window

Member Switch Icon

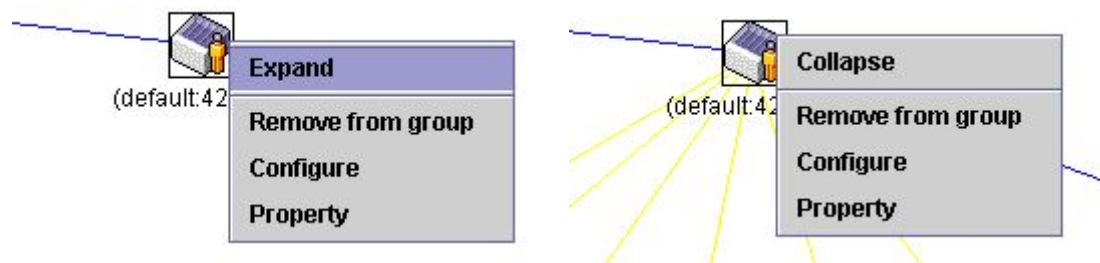


Figure 11- 11. Right Clicking a Member icon

The following options may appear for the user to configure:

- **Collapse** - to collapse the group that will be represented by a single icon.
- **Expand** - to expand the SIM group, in detail.
- **Remove from group** - remove a member from a group.
- **Configure** - launch the web management to configure the Switch.
- **Property** - to pop up a window to display the device information.

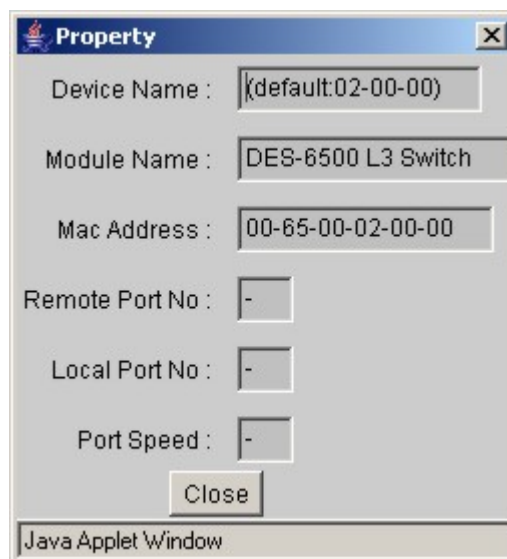


Figure 11- 12. Property window

Candidate Switch Icon

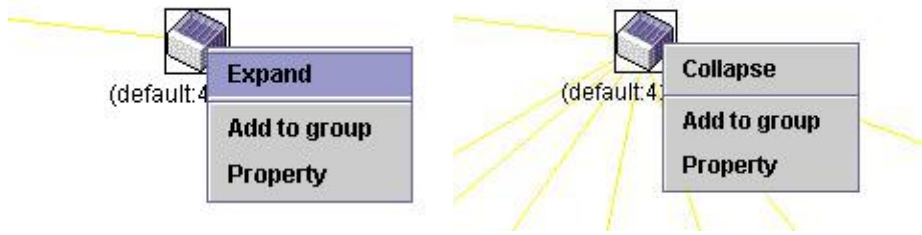


Figure 11- 13. Right Clicking a Candidate icon

The following options may appear for the user to configure:

- **Collapse** - to collapse the group that will be represented by a single icon.
- **Expand** - to expand the SIM group, in detail.
- **Add to group** - add a candidate to a group. Clicking this option will reveal the following screen for the user to enter a password for authentication from the Candidate Switch before being added to the SIM group. Click OK to enter the password or Cancel to exit the window.



Figure 11- 14. Input password window.

- **Property** - to pop up a window to display the device information, as shown below.

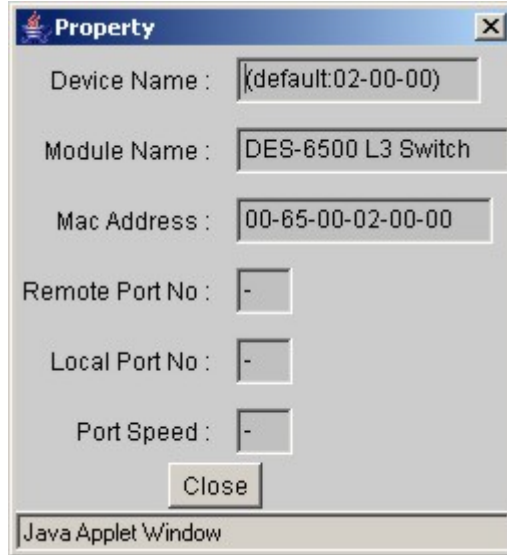


Figure 11- 15. Device Property window.

This window holds the following information:

Parameter	Description
Device Name	This field will display the Device Name of the switches in the SIM group configured by the user. If no Device Name is configured by the name, it will be given the name default and tagged with the last six digits of the MAC Address to identify it.
Module Name	Displays the full module name of the switch that was right-clicked.
MAC Address	Displays the MAC Address of the corresponding Switch.

Remote Port No.	Displays the number of the physical port on the MS or CaS that the CS is connected to. The CS will have no entry in this field.
Local Port No.	Displays the number of the physical port on the CS that the MS or CaS is connected to. The CS will have no entry in this field.
Port Speed	Displays the connection speed between the CS and the MS or CaS

Click **Close** to close the **Property** window.

Menu Bar

The **Single IP Management** window contains a menu bar for device configurations, as seen below.



Figure 11- 16. Menu Bar of the Topology View

The five menus on the menu bar are as follows.

File

- **Print Setup** - will view the image to be printed.
- **Print Topology** - will print the topology map.
- **Preference** - will set display properties, such as polling interval, and the views to open at SIM startup.

Group

- **Add to group** - add a candidate to a group. Clicking this option will reveal the following screen for the user to enter a password for authentication from the Candidate Switch before being added to the SIM group. Click OK to enter the password or Cancel to exit the window.



Figure 11- 17. Input password window.

- **Remove from Group** - remove an MS from the group.

Device

- **Configure** - will open the web manager for the specific device.

View

- **Refresh** - update the views with the latest status.
- **Topology** - display the Topology view.

Help

- **About** - Will display the SIM information, including the current SIM version.



NOTE: Upon this firmware release, some functions of the SIM can only be configured through the Command Line Interface. See the *xStack[®] DES-6500 Modular Layer 3 Chassis Ethernet Switch User CLI* for more information on SIM and its configurations.

Firmware Upgrade

This screen is used to upgrade firmware from the Commander Switch to the Member Switch. To access the following window, click **Single IP Management > Firmware Upgrade**. Member Switches will be listed in the table and will be specified by **Port** (port on the CS where the MS resides), **MAC Address**, **Model Name** and **Version**. To specify a certain Switch for firmware download, click its corresponding check box under the **Port** heading. To update the firmware, enter the **Server IP Address** where the firmware resides and enter the **Path/Filename** of the firmware. Click **Download** to initiate the file transfer.

Firmware Upgrade			
Port	MAC Address	Model Name	Version
Server IP Address	0	0	0
Path \ Filename			
			Download

Figure 11- 18. Firmware Upgrade window

Configuration File Backup/Restore

This screen is used to upgrade configuration files from the Commander Switch to the Member Switch using a TFTP server. Member Switches will be listed in the table and will be specified by **Port** (port on the CS where the MS resides), **MAC Address**, **Model Name** and **Version**. To specify a certain Switch for upgrading configuration files, click its corresponding radio button under the **Port** heading. To update the configuration file, enter the **Server IP Address** where the file resides and enter the **Path/Filename** of the configuration file. Click **Download** to initiate the file transfer from a TFTP server to the Switch. Click **Upload** to backup the configuration file to a TFTP server.

Configuration File Backup/Restore			
Port	MAC Address	Model Name	Version
Server IP Address	0	0	0
Path \ Filename			
			Upload
			Download

Figure 11- 19. Configuration File Backup/Restore window

Appendix A

General											
Standards	IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.1D Spanning Tree IEEE 802.1w Rapid Spanning Tree IEEE 802.1s Multiple Spanning Tree IEEE 802.1 P/Q VLAN IEEE 802.1p Priority Queues IEEE 802.1x Port and MAC Based Access Control IEEE 802.3ad Link Aggregation Control IEEE 802.3x Full-duplex Flow Control IEEE 802.3 Nway auto-negotiation										
Protocols	CSMA/CD										
Data Transfer Rates	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; text-align: center;">Half-duplex</td> <td style="width: 50%; text-align: center;">Full-duplex</td> </tr> <tr> <td style="padding-top: 10px;">Ethernet</td> <td style="padding-top: 10px;">10 Mbps 20Mbps</td> </tr> <tr> <td style="padding-top: 5px;">Fast Ethernet</td> <td style="padding-top: 5px;">100Mbps 200Mbps</td> </tr> <tr> <td style="padding-top: 5px;">Gigabit Ethernet</td> <td style="padding-top: 5px;">1000Mbps 2000Mbps</td> </tr> <tr> <td style="padding-top: 5px;">10G Ethernet</td> <td style="padding-top: 5px;">10Gbps 20Gbps</td> </tr> </table>	Half-duplex	Full-duplex	Ethernet	10 Mbps 20Mbps	Fast Ethernet	100Mbps 200Mbps	Gigabit Ethernet	1000Mbps 2000Mbps	10G Ethernet	10Gbps 20Gbps
Half-duplex	Full-duplex										
Ethernet	10 Mbps 20Mbps										
Fast Ethernet	100Mbps 200Mbps										
Gigabit Ethernet	1000Mbps 2000Mbps										
10G Ethernet	10Gbps 20Gbps										
Fiber Optic	<p>SFP (Mini GBIC) Support</p> IEEE 802.3z 1000BASE-LX (DEM-310GT Transceiver) IEEE 802.3z 1000BASE-SX (DEM-311GT Transceiver) IEEE 802.3z 1000BASE-LH (DEM-314GT Transceiver) IEEE 802.3z 1000BASE-ZX (DEM-315GT Transceiver) IEEE 802.3x 1000BASE-LX (DEM-330T Transceiver) IEEE 802.3x 1000BASE-LX (DEM-330R Transceiver) IEEE 802.3x 1000BASE-LX (DEM-331T Transceiver) IEEE 802.3x 1000BASE-LX (DEM-331R Transceiver)										
	<p>XFP (10G) Support</p> IEEE 802.3ae 10GBASE-ER (DEM-421XT Transceiver) IEEE 802.3ae 10GBASE-ER (DEM-422XT Transceiver) IEEE 802.3ae 10GBASE-ER (DEM-423XT Transceiver)										
Topology	Star										
Network Cables	UTP Cat.5, Cat.5 Enhanced for 1000Mbps UTP Cat.5 for 100Mbps UTP Cat.3, 4, 5 for 10Mbps EIA/TIA-568 100-ohm screened twisted-pair (STP)(100m)										

Physical And Environment

AC inputs & External Redundant Power Supply	100 - 240 VAC, 50/60 Hz (internal universal power supply)	
Power Consumption	Watts	Amps
	Chassis DES-6500: 30W maximum	Chassis DES-6500: 6.4A maximum
	Line Cards DES-6504: 30W maximum DES-6505: 18W maximum DES-6507: 35W maximum DES-6508: 27W maximum DES-6509: 20W maximum DES-6510: 28W maximum DES-6512: 21W maximum	Line Cards DES-6504: 8.8A maximum DES-6505: 4.8A maximum DES-6507: 9.92A maximum DES-6508: 7.9A maximum DES-6509: 5.82A maximum DES-6510: 8.1A maximum DES-6512: 6.28A maximum
	Power Supply DES-6511: 296W maximum	
DC fans	Four built-in 80 x 80 x 25 mm fans	
Operating Temperature	0 to 40 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	440 mm x 294 mm x 356 mm (1U), 19 inch rack-mount width Modules: 330mm x 281mm x 27.5mm	
Weight	13.16kg	
EMI	FCC Part 15 Class A/ ICES-003 Class (Canada) EN55022 Class A/ EN55024	
Safety	CSA International	

Performance

Transmission Method	Store-and-forward L3 Routing
RAM Buffer	256 MB per line card, 256MB for CPU Card
Filtering Address Table:	16 K MAC addresses per device 3K IP addresses per device
Packet Filtering/ Forwarding Rate:	Full-wire speed for all connections. 148,810 pps per port (for 100Mbps) 1,488,100 pps per port (for 1000Mbps)

MAC Address Learning	Automatic update
Forwarding Table Age Time:	Max age: 10 - 1000000 seconds Default = 300

Appendix B

Upgrading Instructions for Release 3 Firmware (R3.00.B33)

For firmware release R3.00-B33, certain guidelines must be followed for proper installation of line cards and their appropriate firmware. **Failing to follow these rules may result in inoperability of the switch or installed line cards.**

Line Card Firmware Compatibility

The xStack® DES-6500 chassis switch supports the following line cards:

- DES-6504 12-port 100BASE-FX (SFF) Fast Ethernet Switch module
- DES-6505 8-port 1000Base-SX SC Fiber Module
- DES-6506 Patch Panel for 24 port RJ45
- DES-6507 12-port 10BASE-T/100BASE-TX/1000BASE-T + Combo 2 SFP
- DES-6508 16-port 10/100M Base-T module
- DES-6509 12-port mini GBIC Fiber Module
- DES-6510 24-port 10/100M RJ21 Module
- DES-6512 2-port 10 GE XFP switch module

These line cards have various compatibilities with different CPU firmware runtime versions. See the following table for a better understanding.

Runtime Code Version	Supported Line Card
R1.01.B37	DES-6507/DES-6509
R1.01.B40	DES-6505 /DES-6507/DES-6509
R1.20.B09	DES-6505/DES-6507/ DES-6508 /DES-6509/ DES-6510
R1.30.B02	DES-6504 /DES-6505/DES-6507/DES-6508/DES-6509/DES-6510
R1.40.B03	DES-6504/DES-6505/DES-6507/DES-6508/DES-6509/DES-6510
R2.00.B20	DES-6504/DES-6505/DES-6507/DES-6508/DES-6509/DES-6510
R2.50.B12	DES-6504/DES-6505/DES-6507/DES-6508/DES-6509/DES-6510/ DES-6512
R3.00.B33	DES-6504/DES-6505/DES-6507/DES-6508/DES-6509/DES-6510/DES-6512

In the previous table, the Runtime Code Version is the earliest firmware version that the corresponding cards listed in the Supported Line Card column can utilize. For example, the DES-6507 and the DES-6509 are listed for every firmware and therefore are compatible with every firmware release dating back to R1.01-B37. The DES-6505 starts with R1.01-B40 and is compatible with every firmware release dating back to R1.01-B40, and so on. **Installing a line card in the chassis containing unsupported firmware will result in a system boot-up failure for the chassis.** Line cards marked in bold denote recently added firmware support for these line cards with the corresponding listed firmware. **All installed line cards must be using the same firmware release runtime code as the chassis CPU, or compatibility problems will arise.**

Precautions for Adding New Line Cards to the Chassis

Certain guidelines must be followed when attempting to add a new line card to the chassis.

1. Ensure the firmware version of the chassis will support the new line cards and their corresponding firmware.
2. Remove line cards which cause a compatibility issue before adding the new line cards. See the next section for more information on line card compatibility.
3. Perform a system reset on the chassis before updating the firmware code of the new line cards. See the next section for more information regarding updating firmware for the chassis and the Switch.

Upgrading to R3.00-B33

For this firmware version, some procedures and implementations have changed since the previous firmware release. **Failure to follow these rules may lead to compatibility problems and inoperability of the Switch.** Please see the guide below for detailed information regarding the proper firmware upgrade procedure.

PROM Code

We strongly recommend that the user upgrade the PROM (Programmable Read Only Memory) code to R2.00-B20. Before upgrading the PROM code, the user **MUST** first upgrade the runtime firmware for both the CPU and any line cards set in the DES-6500 to R2.0 or later. These upgrades can be performed through a TFTP server application, yet the PROM code itself must be upgraded through the CLI interface only.

Firmware Filenames

For the xStack[®] DES-6500 chassis switch and associated line cards, there are two different Runtime Code filenames which must be correctly specified when upgrading either the CPU or the line cards. A capital **S** in the firmware filename (6500rS_3.00.B33.had) indicates the firmware is for the line card only, while a capital **U** (6500rU_3.00.B33.had) indicates the firmware is for the CPU card only. When downloading the firmware, be sure to specify in the CLI command or through the web, whether the firmware is for the CPU or the line card. Downloading the incorrect firmware will cause problems with the Switch.



Failing to follow this procedure will cause problems with the switch and the supported line cards. All Prom code versions (R0.00.B15, R0.00.B16, R1.50.B19 and R2.00.B20) are compatible with all firmware versions of the chassis and line cards. In addition, we strongly recommend that the user upgrade the PROM code to the latest release for maximum functionality of the chassis and the installed line cards.



Due to a backward compatibility issue, when a user upgrades to R3 firmware (3.00.B33), all settings previously configured for any ACL function (CPU ACL included) on the Switch will be lost. We recommend that the user save a configuration file of current settings before upgrading to R3 firmware.

Upgrading to R3.00-B33

To upgrade the firmware Runtime Code to R3.00.B33, follow the steps below to guide you through the firmware upgrading process. **Remember the CPU firmware runtime code must be downloaded to the Switch before the line card firmware Runtime code is downloaded.**

Step 1

Power on the chassis and check the Firmware version currently set in the Switch by entering the “**show switch**” command into the CLI interface, as shown below.

```

DES-6500:4#show switch
Command: show switch

Device Type           : DES-6500 Chassis Ethernet
Switch
MAC Address           : DA-10-21-00-00-01
IP Address             : 10.41.44.22 (Manual)
VLAN Name              : default
Subnet Mask            : 255.0.0.0
Default Gateway        : 0.0.0.0
Boot PROM Version     : Build 2.00-B23
Firmware Version       : Build 3.60-B02
Hardware Version       : 2A1
Device S/N            :
System Name            : DES-6500_#4
System Location        : 7th_flr_east_cabinet
System Contact         : Julius_Erving_212-555-6666
Spanning Tree          : Disabled
GVRP                   : Disabled
IGMP Snooping          : Disabled
802.1X                 : Disabled
Jumbo Frame            : Off
Clipaging              : Enabled
Port Mirror            : Disabled
SNTP                   : Disabled
Boot Relay             : Disabled
DNSR Status            : Disabled
VRRP                   : Disabled
DVMRP                  : Disabled
PIM-DM                 : Disabled
RIP                    : Disabled
OSPF                   : Disabled
TELNET                 : Enabled (TCP 23)
WEB                    : Enabled (TCP 80)
RMON                   : Enabled
HOL Prevention State   : Enabled
Syslog Global State    : Disabled

DES-6500:4#

```

Once you have verified your Firmware version, check the “**show stack_information**” command in the CLI interface to view the runtime codes of the line card modules set in the Switch.

```

DES-6500:4#show stack_information
Command: show stack_information

Box ID      Type      Exist  Prio- Prom   Runtime  H/W
          ID      Type      Exist  rity  version version version
-----
1      DES-6505  exist  16   0.00-B16 2.00-B20 0A1
2      DES-6507  exist  16   0.00-B16 2.00-B20 3A1
3      USR-NOT-CFG no
4      DES-6508  exist  16   1.50-B19 2.00-B20 0A1
5      DES-6508  exist  16   1.50-B19 2.00-B20 0A1
6      DES-6507  exist  16   1.50-B19 2.00-B20 2A1
7      DES-6504  exist  16   2.00-B20 2.00-B20 2A1
8      USR-NOT-CFG no
-----
Topology      :STAR
Current state :MASTER
Box Count     :6

DES-6500:4#

```

Step 2

Upgrade the CPU firmware R3.00-B33, as shown below.

```

DES-6500:4#download firmware_fromTFTP 10.48.74.121 c:/6500rU_3.00-
B33.had unit cpu
Command: download firmware_fromTFTP 10.48.74.121 c:/6500rU_3.00-B33.had
unit cpu

Connecting to server.....Done.
Download firmware.....Done. Do not power off!
Please wait, programming flash.....Done.
Saving current settings to NV-RAM.....Done.
Please wait, the switch is rebooting...

```

Step 3

Once rebooted, check the “**show switch**” command to verify that the firmware was downloaded correctly. The user can then upgrade the Runtime Version code for the inserted line cards using the following syntax in the CLI.

```

DES-6500:4#download firmware_fromTFTP 10.48.74.121 c:/6500rS_3.00-B33.had
unit all_line_card
Command: download firmware_fromTFTP 10.48.74.121 c:/6500rS_3.00-B33.had unit
all_line_card

Connecting to server..... Done.
Download firmware.....Done.
Connecting to slave.....Done.
Upload firmware.....Done.
Line card will automatically reboot after a few minutes. Please don't power
off!
Success.

DES-6500:4#

```

Step 5

Once the line cards have rebooted, check the “**show stack information**” command in the CLI to verify all line cards are now holding the same firmware version as the CPU. If there is a discrepancy in any line card, the user must again repeat the download firmware process for the line cards in question.

Step 6

After confirming all firmware runtime codes are the same, the user must download the PROM code through a TFTP server. Although the same PROM code is to be used for both line cards and the CPU, the user must download the PROM code to both the CPU and the line cards separately. This may be done in any order preferable to the user but two downloads must take place, as shown below.

```
DES-6500:4#download firmware_fromTFTP 10.48.74.121 c:/DES6500_PROM_B20.had unit
all_line_card
Command: download firmware_fromTFTP 10.48.74.121 c:/DES6500_PROM_B20.had unit
all_line_card

Connecting to server..... Done.
Download firmware.....Done.
Connecting to slave.....Done.
Upload firmware.....Done.
Line card will automatically reboot after a few minutes. Please don't power off!
Success.

DES-6500:4#
```

```
DES-6500:4#download firmware_fromTFTP 10.48.74.121 c:/DES6500_PROM_B20.had
unit cpu
Command: download firmware_fromTFTP 10.48.74.121 c:/DES6500_PROM_B20.had unit
cpu

Connecting to server..... Done.
Download firmware.....Done. Do not power off!
Please wait, programming flash.....Done.
Saving current settings to NV-RAM.....Done.
Please wait, the switch is rebooting..
```

Step 7

Once the whole system has been upgraded to R3.00-B33 with PROM code R2.00-B20, the user may verify all downloads have been successful by checking the “**show switch**” and “**show stack_information**” commands in the CLI one final time. These commands should look similar to the ones shown below.


```
DES-6500:4#show stack_information
```

```
Command: show stack_information
```

Box ID	Type	Exist	Prio- rity	Prom version	Runtime version	H/W version
1	DES-6505	exist	16	0.00-B16	2.00-B20	0A1
2	DES-6507	exist	16	0.00-B16	2.00-B20	3A1
3	USR-NOT-CFG	no				
4	DES-6508	exist	16	1.50-B19	2.00-B20	0A1
5	DES-6508	exist	16	1.50-B19	2.00-B20	0A1
6	DES-6507	exist	16	1.50-B19	2.00-B20	2A1
7	DES-6504	exist	16	2.00-B20	2.00-B20	2A1
8	USR-NOT-CFG	no				

```
-----  
Topology :STAR  
Current state :MASTER  
Box Count :6
```

```
DES-6500:4#
```

```
DES-6500:4#show switch
```

```
Command: show switch
```

```
Device Type : DES-6500 Chassis Ethernet  
Switch  
MAC Address : DA-10-21-00-00-01  
IP Address : 10.41.44.22 (Manual)  
VLAN Name : default  
Subnet Mask : 255.0.0.0  
Default Gateway : 0.0.0.0  
Boot PROM Version : Build 2.00-B20  
Firmware Version : Build 3.00-B33  
Hardware Version : 2A1  
System Name : DES-6500_#3  
System Location : 7th_flr_east_cabinet  
System Contact : Julius_Erving_212-555-6666  
Spanning Tree : Disabled  
GVRP : Disabled  
IGMP Snooping : Disabled  
802.1X : Disabled  
Jumbo Frame : Off  
Clipaging : Enabled  
Port Mirror : Disabled  
SNTP : Disabled  
DHCP Relay : Disabled  
DNSR Status : Disabled  
VRRP : Disabled  
DVMRP : Disabled  
PIM-DM : Disabled  
RIP : Disabled  
OSPF : Disabled  
TELNET : Enabled (TCP 23)  
WEB : Enabled (TCP 80)  
RMON : Enabled  
HOL Prevention State : Enabled  
Syslog Global State : Disabled
```

```
DES-6500:4#
```

Adding Runtime R1.01 DES-6505/DES-6507/DES-6509 Line Cards to the Runtime R1.3/1.4/2.0/2.5/3.0 Chassis

For owners of the xStack® DES-6500 chassis switch, certain software incongruencies have surfaced with the adding and removing new line cards in the chassis. If an xStack® DES-6500 chassis switch has been uploaded with R1.3 or later runtime code, and yet line cards DES-6505/DES-6507/DES-6509 are R1.01, line cards DES-6504/DES-6508/DES-6510/DES-6512 cannot be recognized by the chassis' CPU. To solve this problem, first remove the DES-6504/DES-6508/DES-6510/DES-6512 line cards from the chassis, upgrade the new DES-6505/DES-6507/DES-6509 to R1.30/1.4/2.0/2.5/3.0 and then re-insert the DES-6504/DES-6508/DES-6510/DES-6512 line cards into the chassis. The system should be recovered and the chassis should function normally. Follow the following steps to guide you through the process.

Step 1

Execute the “show switch” command to confirm the CPU firmware status currently set on the chassis.

```
DES-6500:4#show switch
Command: show switch

Device Type           : DES-6500 Chassis Ethernet
Switch
MAC Address           : DA-10-21-00-00-01
IP Address            : 10.41.44.22 (Manual)
VLAN Name             : default
Subnet Mask           : 255.0.0.0
Default Gateway       : 0.0.0.0
Boot PROM Version     : Build 2.00-B20
Firmware Version      : Build 3.00-B33
Hardware Version      : 2A1
System Name           : DES-6500_#3
System Location       : 7th_flr_east_cabinet
System Contact        : Julius_Erving_212-555-6666
Spanning Tree         : Disabled
GVRP                  : Disabled
IGMP Snooping        : Disabled
802.1X                : Disabled
Jumbo Frame           : Off
Clipaging             : Enabled
Port Mirror           : Disabled
SNTP                  : Disabled
DHCP Relay            : Disabled
DNSR Status           : Disabled
VRRP                  : Disabled
DVMRP                 : Disabled
PIM-DM                : Disabled
RIP                   : Disabled
OSPF                  : Disabled
TELNET                : Enabled (TCP 23)
WEB                   : Enabled (TCP 80)
RMON                  : Enabled
HOL Prevention State : Enabled
Syslog Global State   : Disabled

DES-6500:4#
```

Step 2

Remove all DES-6504/DES-6508/DES-6510/DES-6512 line cards from the slots in the chassis switch. Next enter the “**reset system**” command and the whole system should reboot with stacking in tact. Enter the “**show stack_information**” command to verify that the switch has completely removed the line card from the chassis.

```
DES-6500:4#reset system
Command: reset system

Are you sure you want to proceed with the system reset? (y/n)
(reset all, save, reboot) y
Reboot & Load Factory Default Configuration.....
Saving all configurations to NV-RAM.....Done
```

```
DES-6500:4#show stack_information
Command: show stack_information

Box ID      Type          Exist rity  Prio- Prom   Runtime  H/W
          version  version    rity  version  version  version
-----
1  DES-6505  exist      16   2.00-B20 3.00-B33 0A1
2  DES-6507  exist      16   2.00-B20 3.00-B33 3A1
3  USR-NOT-CFG no
4  USR-NOT-CFG no
5  USR-NOT-CFG no
6  USR-NOT-CFG no
7  USR-NOT-CFG no
8  USR-NOT-CFG no
-----
Topology      :STAR
Current state :MASTER
Box Count     :2

DES-6500:4#
```

Step 3

After removing the DES-6504/DES-6508/DES-6510/DES-6512 line cards from the switch, enter the new DES-6505/DES-6507/DES-6509 into the chassis. Check the “**show stack_information**” command again to see if the new line card(s) are recognized by the switch.

```
DES-6500:4#show stack_information
Command: show stack_information

Box ID      Type          Exist  Prio- Prom   Runtime  H/W
          Type          Exist rity version version version
-----
1  DES-6505    exist  16   2.00-B20 3.00-B33 0A1
2  DES-6507    exist  16   2.00-B20 3.00-B33 3A1
3  USR-NOT-CFG no
4  USR-NOT-CFG no
5  USR-NOT-CFG no
6  DES-6507    exist  16   0.00-B16 1.01-B37 2A1
7  USR-NOT-CFG no
8  USR-NOT-CFG no
-----
Topology      :STAR
Current state :MASTER
Box Count     :3

DES-6500:4#
```

Step 4

Download the Runtime Version Code (R3.00-B33 for this example) to the new line card in the chassis.

```
DES-6500:4#download firmware_fromTFTP 10.48.74.121 c:/6500rS_3.00-
B33.had unit 6
Command: download firmware_fromTFTP 10.48.74.121 c:/6500rS_3.00-
B33.had unit 6

Connecting to server..... Done.
Download firmware.....Done.
Connecting to slave.....Done.
Upload firmware .....Done.
Line card will automatically reboot after a few minutes. Please don't
power off!
Success.

DES-6500:4#
```

Step 5

Check the upgrade result with the “show stack_information” command.

```
DES-6500:4#show stack_information
Command: show stack_information

Box ID      Type          Exist  Prio- Prom   Runtime  H/W
          Type          rity  rity  version version version
-----
1  DES-6505    exist  16   2.00-B20 3.00-B33 0A1
2  DES-6507    exist  16   2.00-B20 3.00-B33 3A1
3  USR-NOT-CFG no
4  USR-NOT-CFG no
5  USR-NOT-CFG no
6  DES-6507    exist  16   0.00-B16 3.00-B33 2A1
7  USR-NOT-CFG no
8  USR-NOT-CFG no

-----
Topology      :STAR
Current state  :MASTER
Box Count     :3

DES-6500:4#
```

Step 6

Re-insert the DES-6504/DES-6508/DES-6510/DES-6512 line card(s) into the chassis and check the “show stack_information” one more time. All line cards should now be recognized by the Switch and they should all be showing the same firmware Runtime Version.

```
DES-6500:4#show stack_information
Command: show stack_information

Box ID      Type          Exist  Prio- Prom   Runtime  H/W
          Type          rity  rity  version version version
-----
1  DES-6505    exist  16   2.00-B20 3.00-B33 0A1
2  DES-6507    exist  16   2.00-B20 3.00-B33 3A1
3  DES-6510    exist  16   2.00-B20 3.00-B33 2A1
4  USR-NOT-CFG no
5  DES-6508    exist  16   2.00-B20 3.00-B33 2A1
6  DES-6507    exist  16   0.00-B16 3.00-B33 2A1
7  DES-6504    exist  16   2.00-B20 3.00-B33 2A1
8  DES-6512    exist  16   2.00-B20 3.00-B33 1A1

-----
Topology      :STAR
Current state  :MASTER
Box Count     :7

DES-6500:4#
```

Firmware Downgrade Procedure

For users wishing to downgrade their firmware versions for the chassis CPU and corresponding line cards, there are certain guidelines and steps that need to be followed to ensure optimum functionality of the chassis and supported line cards. Failing to follow these rules may result in inoperability of the chassis and installed line cards. Please see the explanation below for more information regarding this subject.

Procedure Overview

1. **Before commencing with the firmware downgrade, the administrator must remove all line cards not supported for that firmware release.** (ex. If the user is downgrading to R1.20-B09, the DES-6504 line card must be removed from the chassis before beginning the firmware downgrade). See the **Line Card Firmware Compatibility** table at the beginning of this section for more information on line cards and their supported firmware versions.
2. After removing the unsupported line card, the user must execute the “**reset system**” command in the CLI interface. This will clear the configurations of the unsupported line card in the chassis.
3. Once the “reset System” command is executed and the removal is a success, the user may then download the lower version runtime code into the chassis CPU. **Remember to downgrade the installed line cards firmware before downgrading the chassis’ CPU firmware.** This downgrade order **MUST** be followed or compatibility issues will arise with the chassis and the line cards and may render your chassis inoperable.
4. Finally, the user must once again execute the “**reset system**” command into the CLI interface.

Downgrade Example

This downgrade example will refer to the downgrade procedure from R2.00-B20 to R1.20-B09 but is universal to all firmware downgrade procedures for the xStack[®] DES-6500 chassis switch.

Step1

Power on the chassis and once it has booted completely, enter the “**show switch**” command into the CLI interface to view the firmware version of the CPU runtime code currently employed in the chassis.

```
DES-6500:4#show switch
Command: show switch

Device Type           : DES-6500 Chassis Ethernet
Switch
MAC Address           : DA-10-21-00-00-01
IP Address            : 10.41.44.22 (Manual)
VLAN Name             : default
Subnet Mask           : 255.0.0.0
Default Gateway       : 0.0.0.0
Boot PROM Version     : Build 2.00-B20
Firmware Version      : Build 2.00-B20
Hardware Version      : 2A1
Device S/N           :
System Name           : DES-6500_#3
System Location       : 7th_flr_east_cabinet
System Contact        : Julius_Erving_212-555-6666
Spanning Tree         : Disabled
GVRP                  : Disabled
IGMP Snooping        : Disabled
802.1X                : Disabled
Jumbo Frame           : Off
Clipaging             : Enabled
Port Mirror           : Disabled
SNTP                  : Disabled
Boot Relay            : Disabled
DNSR Status           : Disabled
VRRP                  : Disabled
DVMRP                 : Disabled
PIM-DM               : Disabled
RIP                   : Disabled
OSPF                  : Disabled
TELNET                : Enabled (TCP 23)
WEB                   : Enabled (TCP 80)
RMON                  : Enabled
HOL Prevention State  : Enabled
Syslog Global State   : Disabled

DES-6500:4#
```


Step 2

Next enter the “**show stack_information**” command into the CLI to display the Runtime Version Code of the line cards currently set in the chassis.

```
DES-6500:4#show stack_information
Command: show stack_information

Box ID      Type          Exist  Prio- Prom   Runtime  H/W
          Type          Exist rity version version version
-----
1  DES-6505  exist    16   2.00-B20 2.00-B20 0A1
2  DES-6507  exist    16   2.00-B20 2.00-B20 2A1
3  DES-6510  exist    16   2.00-B20 2.00-B20 0A1
4  USR-NOT-CFG no
5  DES-6508  exist    16   2.00-B20 2.00-B20 0A1
6  DES-6507  exist    16   2.00-B20 2.00-B20 2A1
7  DES-6504  exist    16   2.00-B20 2.00-B20 0A1
8  USR-NOT-CFG no
-----
Topology      :STAR
Current state  :MASTER
Box Count     :6

DES-6500:4#
```

Step 3

Remove unsupported line cards from the chassis (in this case, the DES-6504 line card for downgrade to 1.20-B09). Next enter the “**reset system**” command and the whole system should reboot with stacking in tact. Enter the “**show stack_information**” command again to verify that the switch has completely removed the line card from the chassis.

```
DES-6500:4#show stack_information
Command: show stack_information

Box ID      Type          Exist  Prio- Prom   Runtime  H/W
          Type          Exist rity version version version
-----
1  DES-6505  exist    16   2.00-B20 2.00-B20 0A1
2  DES-6507  exist    16   2.00-B20 2.00-B20 2A1
3  DES-6510  exist    16   2.00-B20 2.00-B20 0A1
4  USR-NOT-CFG no
5  DES-6508  exist    16   2.00-B20 2.00-B20 0A1
6  DES-6507  exist    16   2.00-B20 2.00-B20 2A1
7  DES-6504  no
8  USR-NOT-CFG no
-----
Topology      :STAR
Current state  :MASTER
Box Count     :5

DES-6500:4#
```

```
DES-6500:4#reset system
Command: reset system

Are you sure you want to proceed with the system reset?(y/n)
(reset all, save, reboot) y
Reboot & Load Factory Default Configuration...
Saving all configurations to NV-RAM.....Done
```

```
DES-6500:4#show stack_information
Command: show stack_information

Box ID      Type      Exist  Prio- Prom   Runtime  H/W
          ID      Type      Exist  rity  version version  version
-----
1      DES-6505  exist  16    2.00-B20 2.00-B20 0A1
2      DES-6507  exist  16    2.00-B20 2.00-B20 2A1
3      DES-6510  exist  16    2.00-B20 2.00-B20 0A1
4      USR-NOT-CFG no
5      DES-6508  exist  16    2.00-B20 2.00-B20 0A1
6      DES-6507  exist  16    2.00-B20 2.00-B20 2A1
7      USR-NOT-CFG no
8      USR-NOT-CFG no
-----
Topology      :STAR
Current state :MASTER
Box Count     :5

DES-6500:4#
```

Step 4

Download the line card Runtime Code Version R1.20-B09 to the available line cards in the chassis.

```
DES-6500:4#download firmware_fromTFTP 10.48.74.121 c:/6500rS_1.20-B09.had unit
all_line_card
Command: download firmware_fromTFTP 10.48.74.121 c:/6500rS_1.20-B09.had unit
all_line_card

Connecting to server..... Done.
Download firmware.....Done.
Connecting to slave.....Done.
Upload firmware.....Done.
Line card will automatically reboot after a few minutes. Please don't power
off!
Success.
```

Step 5

After the chassis reboots and returns to normal operation and stacking configuration, download Runtime Code Version R1.20-B09 to the chassis CPU.

```
DES-6500:4#download firmware_fromTFTP 10.48.74.121 c:/6500rU_1.20-B09.had unit cpu
Command: download firmware_fromTFTP 10.48.74.121 c:/6500rU_1.20-B09.had unit cpu

Connecting to server..... Done.
Download firmware.....Done.
Connecting to slave.....Done.
Upload firmware.....Done.
Line card will automatically reboot after a few minutes. Please don't power off!
Success.

DES-6500:4#
```


Step 6

Once the CPU and all line cards have been downgraded, the user may verify that all downloads have been successfully completed by entering the “show switch” command and the “show stack_information” command.

```
DES-6500:4#show stack_information
Command: show stack_information

Box ID      Type          Exist  Prio- Prom   Runtime  H/W
          Type          rity   rity  version version version
-----
1    DES-6505    exist  16    2.00-B20  1.20-B09  0A1
2    DES-6507    exist  16    2.00-B20  1.20-B09  2A1
3    DES-6510    exist  16    2.00-B20  1.20-B09  0A1
4    USR-NOT-CFG  no
5    DES-6508    exist  16    2.00-B20  1.20-B09  0A1
6    DES-6507    exist  16    2.00-B20  1.20-B09  2A1
7    USR-NOT-CFG  no
8    USR-NOT-CFG  no
-----
Topology      :STAR
Current state :MASTER
Box Count     :5

DES-6500:4#
```



```
DES-6500:4#show switch
Command: show switch

Device Type           : DES-6500 Chassis Ethernet
Switch
MAC Address           : DA-10-21-00-00-01
IP Address             : 10.41.44.22 (Manual)
VLAN Name              : default
Subnet Mask            : 255.0.0.0
Default Gateway        : 0.0.0.0
Boot PROM Version     : Build 2.00-B20
Firmware Version       : Build 1.20-B09
Hardware Version       : 2A1
Device S/N            :
System Name            : DES-6500_#3
System Location        : 7th_flr_east_cabinet
System Contact         : Julius_Erving_212-555-6666
Spanning Tree          : Disabled
GVRP                   : Disabled
IGMP Snooping          : Disabled
802.1X                 : Disabled
Jumbo Frame            : Off
Clipaging              : Enabled
Port Mirror            : Disabled
SNTP                   : Disabled
Boot Relay             : Disabled
DNSR Status            : Disabled
VRRP                   : Disabled
DVMRP                  : Disabled
PIM-DM                 : Disabled
RIP                    : Disabled
OSPF                   : Disabled
TELNET                 : Enabled (TCP 23)
WEB                    : Enabled (TCP 80)
RMON                   : Enabled
HOL Prevention State   : Enabled
Syslog Global State    : Disabled

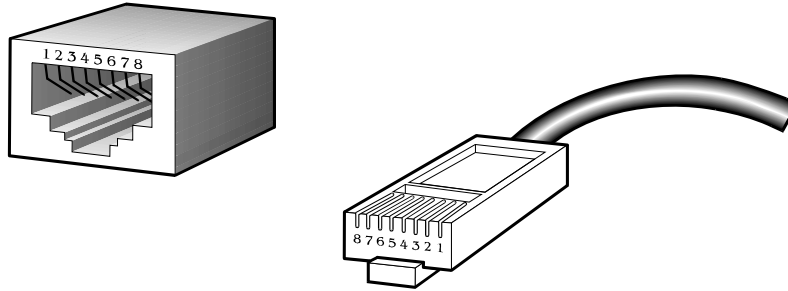
DES-6500:4#
```

Appendix C

Cables and Connectors

When connecting the Switch to another switch, a bridge or hub, a normal cable is necessary. Please review these products for matching cable pin assignment.

The following diagrams and tables show the standard RJ-45 receptacle/connector and their pin assignments.



Appendix 1- 1. The standard RJ-45 port and connector

RJ-45 Pin Assignments		
Contact	MDI-X Port	MDI-II Port
1	BI-DB+	BI-DA+
2	BI-DB-	BI-DA-
3	BI-DA+	BI-DB+
4	BI-DD+	BI-DC+
5	BI-DD-	BI-DC-
6	BI-DA-	BI-DB-
7	BI-DC+	BI-DD+
8	BI-DC-	BI-DD+

Appendix 1- 2. The standard RJ-45 pin assignments

Appendix D

Cable Lengths

Use the following table to as a guide for the maximum cable lengths.

Standard	Media Type	Maximum Distance
Mini-GBIC	1000BASE-LX, Single-mode fiber module	10km
	1000BASE-SX, Multi-mode fiber module	550m
	1000BASE-LHX, Single-mode fiber module	40km
	1000BASE-ZX, Single-mode fiber module	80km
1000BASE-T	Category 5e UTP Cable	100m
	Category 5 UTP Cable (1000 Mbps)	
100BASE-TX	Category 5 UTP Cable (100 Mbps)	100m
10BASE-T	Category 3 UTP Cable (10 Mbps)	100m

Glossary

1000BASE-LX: A short laser wavelength on multimode fiber optic cable for a maximum length of 550 meters

1000BASE-SX: A long wavelength for a "long haul" fiber optic cable for a maximum length of 10 kilometers

100BASE-FX: 100Mbps Ethernet implementation over fiber.

100BASE-TX: 100Mbps Ethernet implementation over Category 5 and Type 1 Twisted Pair cabling.

10BASE-T: The IEEE 802.3 specification for Ethernet over Unshielded Twisted Pair (UTP) cabling.

ageing: The automatic removal of dynamic entries from the Switch Database which have timed-out and are no longer valid.

ATM: Asynchronous Transfer Mode. A connection oriented transmission protocol based on fixed length cells (packets). ATM is designed to carry a complete range of user traffic, including voice, data and video signals.

auto-negotiation: A feature on a port which allows it to advertise its capabilities for speed, duplex and flow control. When connected to an end station that also supports auto-negotiation, the link can self-detect its optimum operating setup.

backbone port: A port which does not learn device addresses, and which receives all frames with an unknown address. Backbone ports are normally used to connect the Switch to the backbone of your network. Note that backbone ports were formerly known as designated downlink ports.

backbone: The part of a network used as the primary path for transporting traffic between network segments.

bandwidth: Information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10Mbps, the bandwidth of Fast Ethernet is 100Mbps.

baud rate: The switching speed of a line. Also known as line speed between network segments.

BOOTP: The BOOTP protocol allows you to automatically map an IP address to a given MAC address each time a device is started. In addition, the protocol can assign the subnet mask and default gateway to a device.

bridge: A device that interconnects local or remote networks no matter what higher level protocols are involved. Bridges form a single logical network, centralizing network administration.

broadcast: A message sent to all destination devices on the network.

broadcast storm: Multiple simultaneous broadcasts that typically absorb available network bandwidth and can cause network failure.

console port: The port on the Switch accepting a terminal or modem connector. It changes the parallel arrangement of data within computers to the serial form used on data transmission links. This port is most often used for dedicated local management.

CSMA/CD: Channel access method used by Ethernet and IEEE 802.3 standards in which devices transmit only after finding the data channel clear for some period of time. When two devices transmit simultaneously, a collision occurs and the colliding devices delay their retransmissions for a random amount of time.

data center switching: The point of aggregation within a corporate network where a switch provides high-performance access to server farms, a high-speed backbone connection and a control point for network management and security.

Ethernet: A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks operate at 10Mbps using CSMA/CD to run over cabling.

Fast Ethernet: 100Mbps technology based on the Ethernet/CD network access method.

Flow Control: (IEEE 802.3z) A means of holding packets back at the transmit port of the connected end station. Prevents packet loss at a congested switch port.

forwarding: The process of sending a packet toward its destination by an internetworking device.

full duplex: A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.

half duplex: A system that allows packets to be transmitted and received, but not at the same time. Contrast with full duplex.

IP address: Internet Protocol address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with full-stops (periods), and is made up of a network section, an optional subnet section and a host section.

IPX: Internetwork Packet Exchange. A protocol allowing communication in a NetWare network.

LAN - Local Area Network: A network of connected computing resources (such as PCs, printers, servers) covering a relatively small geographic area (usually not larger than a floor or building). Characterized by high data rates and low error rates.

latency: The delay between the time a device receives a packet and the time the packet is forwarded out of the destination port.

line speed: See baud rate.

main port: The port in a resilient link that carries data traffic in normal operating conditions.

MDI - Medium Dependent Interface: An Ethernet port connection where the transmitter of one device is connected to the receiver of another device.

MDI-X - Medium Dependent Interface Cross-over: An Ethernet port connection where the internal transmit and receive lines are crossed.

MIB - Management Information Base: Stores a device's management characteristics and parameters. MIBs are used by the Simple Network Management Protocol (SNMP) to contain attributes of their managed systems. The Switch contains its own internal MIB.

multicast: Single packets copied to a specific subset of network addresses. These addresses are specified in the destination-address field of the packet.

protocol: A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.

resilient link: A pair of ports that can be configured so that one will take over data transmission should the other fail. See also main port and standby port.

RJ-45: Standard 8-wire connectors for IEEE 802.3 10BASE-T networks.

RMON: Remote Monitoring. A subset of SNMP MIB II that allows monitoring and management capabilities by addressing up to ten different groups of information.

RPS - Redundant Power System: A device that provides a backup source of power when connected to the Switch.

server farm: A cluster of servers in a centralized location serving a large user population.

SLIP - Serial Line Internet Protocol: A protocol which allows IP to run over a serial line connection.

SNMP - Simple Network Management Protocol: A protocol originally designed to be used in managing TCP/IP internets. SNMP is presently implemented on a wide range of computers and networking equipment and may be used to manage many aspects of network and end station operation.

Spanning Tree Protocol (STP): A bridge-based system for providing fault tolerance on networks. STP works by allowing you to implement parallel paths for network traffic, and ensure that redundant paths are disabled when the main paths are operational and enabled if the main paths fail.

stack: A group of network devices that are integrated to form a single logical device.

standby port: The port in a resilient link that will take over data transmission if the main port in the link fails.

switch: A device which filters, forwards and floods packets based on the packet's destination address. The switch learns the addresses associated with each switch port and builds tables based on this information to be used for the switching decision.

TCP/IP: A layered set of communications protocols providing Telnet terminal emulation, FTP file transfer, and other services for communication among a wide range of computer equipment.

telnet: A TCP/IP application protocol that provides virtual terminal service, letting a user log in to another computer system and access a host as if the user were connected directly to the host.

TFTP - Trivial File Transfer Protocol: Allows you to transfer files (such as software upgrades) from a remote device using your switch's local management capabilities.

UDP - User Datagram Protocol: An Internet standard protocol that allows an application program on one device to send a datagram to an application program on another device.

VLAN - Virtual LAN: A group of location- and topology-independent devices that communicate as if they are on a common physical LAN.

VLT - Virtual LAN Trunk: A Switch-to-Switch link which carries traffic for all the VLANs on each Switch.

VT100: A type of terminal that uses ASCII characters. VT100 screens have a text-based appearance.



Limited Warranty (USA Only)

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. ("D-Link") provides this Limited Warranty:

- Only to the person or entity that originally purchased the product from D-Link or its authorized reseller or distributor, and
- Only for products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, or addresses with an APO or FPO.

Limited Warranty: D-Link warrants that the hardware portion of the D-Link product described below ("Hardware") will be free from material defects in workmanship and materials under normal use from the date of original retail purchase of the product, for the period set forth below ("Warranty Period"), except as otherwise stated herein.

Limited Lifetime Warranty for the product is defined as follows:

- Hardware: For as long as the original customer/end user owns the product, or five (5) years after product discontinuance, whichever occurs first (excluding power supplies and fans)
- Power supplies and fans: Three (3) Year
- Spare parts and spare kits: Ninety (90) days

The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund the actual purchase price paid. Any repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement hardware need not be new or have an identical make, model or part. D-Link may, at its option, replace the defective Hardware or any part thereof with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer, and is subject to the same limitations and exclusions. If a material defect is incapable of correction, or if D-Link determines that it is not practical to repair or replace the defective Hardware, the actual price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware or part thereof that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty: D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days ("Software Warranty Period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Software Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund the portion of the actual purchase price paid that is attributable to the Software. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Replacement Software will be warranted for the remainder of the original Warranty Period and is subject to the same limitations and exclusions. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

Non-Applicability of Warranty: The Limited Warranty provided hereunder for Hardware and Software portions of D-Link's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

Submitting A Claim: The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.
- The customer must obtain a Case ID Number from D-Link Technical Support at 1-877-453-5465, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at <https://rma.dlink.com/>.
- 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. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.
- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to **D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708**. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping

charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer.

D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

What Is Not Covered: The Limited Warranty provided herein by D-Link does not cover: Products that, in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; and Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product. While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited Warranty.

Disclaimer of Other Warranties: EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability: TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY.

Governing Law. This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This Limited Warranty provides specific legal rights and you may also have other rights which vary from state to state.

Trademarks: D-Link is a registered trademark of D-Link Systems, Inc. Other trademarks or registered trademarks are the property of their respective owners.

Copyright Statement: No part of this publication or documentation accompanying this product 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 and any amendments thereto. Contents are subject to change without prior notice. Copyright 2008 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

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

FCC Statement: 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 in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. Operation of this equipment in a residential environment is likely to cause harmful interference to radio or television reception. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

For detailed warranty information applicable to products purchased outside the United States, please contact the corresponding local D-Link office.

Product Registration

Register your D-Link product online at <http://support.dlink.com/register/>

Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.



D-Link Europe Limited Lifetime Warranty

Dear Customer,

Please read below to understand the details of the warranty coverage you have.

Warranty terms for D-LINK xStack® products:

All D-Link xStack® products* are supplied with a 5 year warranty as standard. To enable the Limited Lifetime Warranty on this product you must register the product, within the first three months of purchase**, on the following website: <http://www.dlink.biz/productregistration/>

D-Link will then provide you with a Limited Lifetime Warranty reference number for this product. Please retain your original dated proof of purchase with a note of the serial number, and Limited Lifetime Warranty reference number together with this warranty statement and place each document in a safe location. When you make a warranty claim on a defective product, you may be asked to provide this information.

Nothing in this Limited Lifetime Warranty affects your statutory rights as a consumer. The following are special terms applicable to your Limited Lifetime hardware warranty.

Warranty beneficiary

The warranty beneficiary is the original end user. The original end user is defined as the person that purchases the product as the first owner.

Duration of Limited Lifetime Warranty

As long as the original end-user continues to own or use the product with the following conditions:

- fan and power supplies are limited to a five (5) year warranty only
- in the event of discontinuance of product manufacture, D-Link warranty support is limited to five (5) years from the announcement of discontinuance. If a product is no longer available for replacement, D-Link will issue a product comparable or better to the one originally purchased.

Replacement, Repair or Refund Procedure for Hardware

D-Link or its service center will use commercially reasonable efforts to ship a replacement part within ten (10) working days after receipt of the RMA request. Actual delivery times may vary depending on customer location. D-Link reserves the right to refund the purchase price as its exclusive warranty remedy.

To Receive a Return Materials Authorization (RMA) Number, please visit: <http://service.dlink.biz> and for Italy and Spain, please use: <http://rma.dlink.es> or <http://rma.dlink.it>.



D-Link Limited Lifetime Warranty

Hardware: D-Link warrants the D-Link hardware named above against defects in materials and workmanship for the period specified above. If D-Link receives notice of such defects during the warranty period, D-Link will, at its option, either repair or replace products proving to be defective. Replacement products may be either new or like-new.

Software. D-Link warrants that D-Link software will not fail to execute its programming instructions, for the period specified above, due to defects in material and workmanship when properly installed and used. If D-Link receives notice of such defects during the warranty period, D-Link will replace software media that does not execute its programming instructions due to such defects.

Warranty exclusions

This warranty does not apply if the software, product or any other equipment upon which the software is authorized to be used (a) has been altered, except by D-Link or its authorized representative, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by D-Link (improper use or improper maintenance), (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident; (d) is licensed, for beta, evaluation, testing or demonstration purposes for which D-Link does not charge a purchase price or license fee or (e) defects are caused by force majeure (lightning, floods, war, etc.), soiling, by extraordinary environmental influences or by other circumstances of which D-Link is not responsible.

Disclaimer of warranty

Please note, some countries do not allow the disclaimer of implied terms in contracts with consumers and the disclaimer below may not apply to you.

To the extent allowed by local law, the above warranties are exclusive and no other warranty, condition or other term, whether written or oral, is expressed or implied. D-Link specifically disclaims any implied warranties, conditions and terms of merchantability, satisfactory quality, and fitness for a particular purpose.

To the extent allowed by local law, the remedies in this warranty statement are customer's sole and exclusive remedies. Except as indicated above, in no event will D-Link or its suppliers be liable for loss of data or for indirect, special, incidental, consequential (including lost profit or data), or other damage, whether based in a contract, tort, or otherwise.

To the extent local law mandatorily requires a definition of "Lifetime Warranty" different from that provided here, then the local law definition will supersede and take precedence.

Valid law

The warranty is subject to the valid laws in the country of purchase and is to be interpreted in the warranty terms with the said laws. You may have additional legal rights that are not restricted by this warranty. Nothing in this Limited Lifetime Warranty affects your statutory rights as a consumer.

* DES-6500 series is excluded from the Limited Lifetime Warranty offering and will be supplied with a standard 5 year warranty.

** Failure to register this product within the first three months of purchase [by the first user only] will invalidate the Limited Lifetime Warranty.

LIMITED WARRANTY

D-Link provides this limited warranty for its product only to the person or entity who originally purchased the product from D-Link or its authorized reseller or distributor. D-Link would fulfill the warranty obligation according to the local warranty policy in which you purchased our products.

Limited Hardware Warranty: D-Link warrants that the hardware portion of the D-Link products described below ("Hardware") will be free from material defects in workmanship and materials from the date of original retail purchase of the Hardware, for the period set forth below applicable to the product type ("Warranty Period") if the Hardware is used and serviced in accordance with applicable documentation; provided that a completed Registration Card is returned to an Authorized D-Link Service Office within ninety (90) days after the date of original retail purchase of the Hardware. If a completed Registration Card is not received by an authorized D-Link Service Office within such ninety (90) period, then the Warranty Period shall be ninety (90) days from the date of purchase.

<i>Product Type</i>	<i>Warranty Period</i>
Product (including Power Supplies and Fans)	One (1) Year
Spare parts and pare kits	Ninety (90) days

D-Link's sole obligation shall be to repair or replace the defective Hardware at no charge to the original owner. Such repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement Hardware need not be new or of an identical make, model or part; D-Link may in its discretion may replace the defective Hardware (or any part thereof) with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. The Warranty Period shall extend for an additional ninety (90) days after any repaired or replaced Hardware is delivered. If a material defect is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to repair or replace the defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware (or part thereof) that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty: D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original delivery of the Software for a period of ninety (90) days ("Warranty Period"), if the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. D-Link's sole obligation shall be to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. The Warranty Period shall extend for an additional ninety (90) days after any replacement Software is delivered. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

What You Must Do For Warranty Service:

Registration Card. The Registration Card provided at the back of this manual must be completed and returned to an Authorized D-Link Service Office for each D-Link product within ninety (90) days after the product is purchased and/or licensed. The addresses/telephone/fax list of the nearest Authorized D-Link Service Office is provided in the back of this manual. FAILURE TO PROPERLY COMPLETE AND TIMELY RETURN THE REGISTRATION CARD MAY AFFECT THE WARRANTY FOR THIS PRODUCT.

Submitting A Claim. Any claim under this limited warranty must be submitted in writing before the end of the Warranty Period to an Authorized D-Link Service Office. The claim must include a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same. The original product owner must obtain a Return Material Authorization (RMA) number from the Authorized D-Link Service Office and, if requested, provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided. 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 packaged product shall be insured and shipped to Authorized D-Link Service Office with all shipping costs prepaid. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

What Is Not Covered:

This limited warranty provided by D-Link does not cover:

Products that have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed;

Initial installation, installation and removal of the product for repair, and shipping costs;

Operational adjustments covered in the operating manual for the product, and normal maintenance;

Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage;
and

Any hardware, software, firmware or other products or services provided by anyone other than D-Link.

Disclaimer of Other Warranties: EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability: TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY,

EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT.

GOVERNING LAW: This Limited Warranty shall be governed by the laws of the state of California.

Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This limited warranty provides specific legal rights and the product owner may also have other rights which vary from state to state.

Trademarks

Copyright 2008 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.

Tech Support

Technical Support

You can find software updates and user documentation on the D-Link website.

D-Link provides free technical support for customers within the United States and within Canada for the duration of the service period, and warranty confirmation service, during the warranty period on this product. U.S. and Canadian customers can contact D-Link technical support through our website, or by phone.

Tech Support for customers within the United States:

D-Link Technical Support over the Telephone:

(877) 354-6555

Monday to Friday 8:00am to 5:00pm PST

D-Link Technical Support over the Internet:

<http://support.dlink.com>

email: support@dlink.com

Tech Support for customers within Canada:

D-Link Technical Support over the Telephone:

1-800-361-5265

Monday to Friday 7:30am to 9:00pm EST

D-Link Technical Support over the Internet:

<http://support.dlink.com>

email: support@dlink.ca



Technical Support

United Kingdom (Mon-Fri)

Home Wireless/Broadband 0871 873 3000 (9.00am–06.00pm, Sat 10.00am-02.00pm)
Managed, Smart, & Wireless Switches, or Firewalls 0871 873 0909 (09.00am – 05.30pm)
(BT 10ppm, other carriers may vary.)

Ireland (Mon-Fri)

All Products 1890 886 899 (09.00am-06.00pm, Sat 10.00am-02.00pm)
€ 0.05ppm peak, €0.045ppm off peak Times

Internet

<http://www.dlink.co.uk>
<ftp://ftp.dlink.co.uk>

Technische Unterstützung

Deutschland: Web: <http://www.dlink.de>
E-Mail: support@dlink.de
Telefon: +49(0)1805 2787 0,14 € pro Minute
Zeiten: Mo. –Fr. 09:00 – 17:30 Uhr

Österreich: Web: <http://www.dlink.at>
E-Mail: support@dlink.at
Telefon: +43(0)820 480084 0,116 € pro Minute
Zeiten: Mo. –Fr. 09:00 – 17:30 Uhr

Schweiz: Web: <http://www.dlink.ch>
E-Mail: support@dlink.ch
Telefon: +41(0)848 331100 0,08 CHF pro Minute
Zeiten: Mo. –Fr. 09:00 – 17:30 Uhr

* Gebühren aus Mobilnetzen und von anderen Providern können abweichen.

Assistance technique

Assistance technique D-Link par téléphone : 0 820 0803 03
0,12 €/min la minute : Lundi – Vendredi de 9h à 13h et de 14h à 19h
Samedi 9h à 13h et de 14h à 16h
Assistance technique D-Link sur internet :
<http://www.dlink.fr>

Asistencia Técnica

Asistencia Técnica Telefónica de D-Link: +34 902 30 45 45
0,067 €/min
De Lunes a Viernes de 9:00 a 14:00 y de 15:00 a 18:00
<http://www.dlink.es>

Supporto tecnico

Supporto Tecnico dal lunedì al venerdì dalle ore 9.00 alle ore 19.00 con orario continuato
Telefono: 199400057
<http://www.dlink.it/support>

Technical Support

Tech Support for customers within the Netherlands:

0900 501 2007 / www.dlink.nl / €0.15ppm anytime.

Tech Support for customers within Belgium:

070 66 06 40 / www.dlink.be / €0.175ppm peak, €0.0875ppm off peak

Tech Support for customers within Luxemburg:

+32 70 66 06 40 / www.dlink.be

Pomoc techniczna

Telefoniczna pomoc techniczna firmy D-Link: 0 801 022 021

Pomoc techniczna firmy D-Link świadczona przez Internet:

URL: <http://www.dlink.pl>

e-mail: serwis@dlink.pl

Technická podpora

Web: <http://www.dlink.cz/support/>

E-mail: support@dlink.cz

Telefon: 225 281 553

Telefonická podpora je v provozu: PO- PÁ od 09.00 do 17.00

Land Line 1,78 CZK/min - Mobile 5.40 CZK/min

Technikai Támogatás

Tel. : 06 1 461-3001

Fax : 06 1 461-3004

Land Line 14,99 HUF/min - Mobile 49.99,HUF/min

email : support@dlink.hu

URL : <http://www.dlink.hu>

Teknisk Support

D-Link Teknisk telefon Support: 820 00 755
(Hverdager 08:00-20:00)

D-Link Teknisk Support over Internett: <http://www.dlink.no>

Teknisk Support

D-Link teknisk support over telefonen: Tlf. 7026 9040

Åbningstider: kl. 08:00 – 20:00

D-Link teknisk support på Internettet: <http://www.dlink.dk>

Teknistä tukea asiakkaille Suomessa:

Arkisin klo. 9 - 21
numerosta : **06001 5557**
Internetin kautta : <http://www.dlink.fi>

Teknisk Support

D-Link Teknisk Support via telefon: 0900-100 77 00
Vardagar 08.00-20.00
D-Link Teknisk Support via Internet: <http://www.dlink.se>

Assistência Técnica

Assistência Técnica da D-Link na Internet:
<http://www.dlink.pt>
e-mail: soporte@dlink.es

Τεχνική Υποστήριξη

D-Link Hellas Support Center
Κεφαλληνίας 64, 11251 Αθήνα,
Τηλ: 210 86 11 114 (Δευτέρα- Παρασκευή 09:00-17:00)
Φαξ: 210 8611114
<http://www.dlink.gr/support>

Tehnička podrška

Hvala vam na odabiru D-Link proizvoda. Za dodatne informacije, podršku i upute za korištenje uređaja, molimo vas da posjetite D-Link internetsku stranicu na www.dlink.eu

www.dlink.biz/hr

Tehnična podpora

Zahvaljujemo se vam, ker ste izbrali D-Link proizvod. Za vse nadaljnje informacije, podpora ter navodila za uporabo prosimo obiščite D-Link - ovo spletno stran www.dlink.eu

www.dlink.biz/sl

Suport tehnica

Vă mulțumim pentru alegerea produselor D-Link. Pentru mai multe informații, suport și manuale ale produselor vă rugăm să vizitați site-ul D-Link www.dlink.eu

www.dlink.ro

Technical Support

You can find software updates and user documentations on the D-Link website.

Tech Support for customers in

Australia:

Tel: 1300-766-868

24/7(24Hrs, 7days a week) technical support

<http://www.dlink.com.au>

e-mail: support@dlink.com.au

India:

Tel: 1800-222-002

9.00 AM to 9.00 PM. All days

<http://www.dlink.co.in/support/productsupport.aspx>

Indonesia, Malaysia, Singapore and Thailand:

Tel: +62-21-5731610 (Indonesia)

Tel: 1800-882-880 (Malaysia)

Tel: +65 66229355 (Singapore)

Tel: +66-2-719-8978/9 (Thailand)

24/7, for English Support Only

<http://www.dlink.com.sg/support/>

e-mail: support@dlink.com.sg

Korea:

Tel: +82-2-2028-1815

Monday to Friday 9:00am to 6:00pm

<http://www.d-link.co.kr>

e-mail: arthur@d-link.co.kr

New Zealand:

Tel: 0800-900-900

24/7(24Hrs, 7days a week) technical support

<http://www.dlink.co.nz>

e-mail: support@dlink.co.nz

D-Link®
Building Networks for People

Technical Support

You can find software updates and user documentation on the D-Link website.

Tech Support for customers in

Egypt:

Tel: +202-2919035 or +202-2919047
Sunday to Thursday 9:00am to 5:00pm
<http://support.dlink-me.com>
Email: support.eg@dlink-me.com

Iran:

Te: +98-21-88880918,19
Saturday to Thursday 9:00am to 5:00pm
<http://support.dlink-me.com>
Email : support.ir@dlink-me.com & support@dlink.ir

Israel:

Magshimim 20 St., Matalon center,
Petach Tikva, Israel 49348
Consumer support line: 03-9212886
Business support line: 03-9212608

Pakistan:

Tel: +92-21-4548158 or +92-21-4548310
Monday to Friday 10:00am to 6:00pm
<http://support.dlink-me.com>
E-mail: zkashif@dlink-me.com

South Africa and Sub Sahara Region:

Tel: +27-12-665-2165
08600 DLINK (for South Africa only)
Monday to Friday 8:30am to 9:00pm South Africa Time
<http://www.d-link.co.za>

Turkey:

Tel: +90-212-2895659
Monday to Friday 9:00am to 6:00pm
<http://www.dlink.com.tr>
e-mail: turkiye@dlink-me.com
e-mail: support@d-link.co.za

U.A.E and North Africa:

Tel: +971-4-4278127 (U.A.E)
Sunday to Thursday 9.00AM to 6.00PM GMT+4
Web: <http://www.dlink-me.com>
E-mail: support.me@dlink-me.com

Saudi ARABIA (KSA):

Telephone : +966 01 217 0008
Facsimile : +966 01 217 0009
e-mail: Support.sa@dlink-me.com
Saturday to Wednesday 9.30AM to 6.30PM
Thursdays 9.30AM to 2.00 PM

D-Link®
Building Networks for People

Техническая поддержка

Обновления программного обеспечения и документация доступны на Интернет-сайте D-Link.

D-Link предоставляет бесплатную поддержку для клиентов в течение гарантийного срока.

Клиенты могут обратиться в группу технической поддержки D-Link по телефону или через Интернет.

Техническая поддержка D-Link:

+7(495) 744-00-99

Техническая поддержка через Интернет

<http://www.dlink.ru>

e-mail: support@dlink.ru



SOPORTE TÉCNICO

Usted puede encontrar actualizaciones de softwares o firmwares y documentación para usuarios a través de nuestro sitio www.dlinkla.com

SOPORTE TÉCNICO PARA USUARIOS EN LATINO AMERICA

Soporte técnico a través de los siguientes teléfonos de D-Link

PAIS	NUMERO	HORARIO
Argentina	0800 - 12235465	Lunes a Viernes 08:00am a 21:00pm
Chile	800 - 835465 ó (02) 5941520	Lunes a Viernes 08:00am a 21:00pm
Colombia	01800 - 9525465	Lunes a Viernes 06:00am a 19:00pm
Costa Rica	0800 - 0521478	Lunes a Viernes 05:00am a 18:00pm
Ecuador	1800 - 035465	Lunes a Viernes 06:00am a 19:00pm
El Salvador	800 - 6335	Lunes a Viernes 05:00am a 18:00pm
Guatemala	1800 - 8350255	Lunes a Viernes 05:00am a 18:00pm
México	01800 - 1233201	Lunes a Viernes 06:00am a 19:00pm
Panamá	011 008000525465	Lunes a Viernes 05:00am a 18:00pm
Perú	0800 - 00968	Lunes a Viernes 06:00am a 19:00pm
República Dominicana	18887515478	Lunes a Viernes 05:00am a 18:00pm
Venezuela	0800 - 1005767	Lunes a Viernes 06:30am a 19:30pm

Soporte Técnico de D-Link a través de Internet

www.dlinkla.com

e-mail: soporte@dlinkla.com & consultas@dlinkla.com



Suporte Técnico

Você pode encontrar atualizações de software e documentação de usuário no site da D-Link Brasil.

A D-Link fornece suporte técnico gratuito para clientes no Brasil durante o período de vigência da garantia deste produto.

Suporte Técnico para clientes no Brasil:

Telefone

São Paulo +11-2185-9301

Segunda à sexta

Das 8h30 às 18h30

Demais Regiões do Brasil 0800 70 24 104

E-mail:

e-mail: suporte@dlinkbrasil.com.br



D-Link 友訊科技 台灣分公司 技術支援資訊

如果您還有任何本使用手冊無法協助您解決的產品相關問題，台灣地區用戶可以透過我們的網站、電子郵件或電話等方式與D-Link台灣地區技術支援工程師聯絡。

D-Link 免付費技術諮詢專線

0800-002-615

服務時間：週一至週五，早上8:30到晚上9:00

(不含周六、日及國定假日)

網 站：<http://www.dlink.com.tw>

電子郵件：dssqa_service@dlink.com.tw

如果您是台灣地區以外的用戶，請參考D-Link網站全球各地分公司的聯絡資訊以取得相關支援服務。

產品保固期限、台灣區維修據點查詢，請參考以下網頁說明：

<http://www.dlink.com.tw>

產品維修：

使用者可直接送至全省聯強直營維修站或請洽您的原購買經銷商。

D-Link[®]
Building Networks for People

Dukungan Teknis

Update perangkat lunak dan dokumentasi pengguna dapat diperoleh pada situs web D-Link.

Dukungan Teknis untuk pelanggan:

Dukungan Teknis D-Link melalui telepon:

Tel: +62-21-5731610

Dukungan Teknis D-Link melalui Internet:

Email : support@dlink.co.id

Website : <http://support.dlink.co.id>



Technical Support

この度は弊社製品をお買い上げいただき、誠にありがとうございます。
ございます。

下記弊社 Web サイトからユーザ登録及び新製品登録を行っていただくと、ダウンロードサービスにてサポート情報、ファームウェア、ユーザマニュアルをダウンロードすることができます。

ディーリンクジャパン Web サイト

URL:<http://www.dlink-jp.com>

D-Link®
Building Networks for People

技术支持

您可以在 D-Link 的官方网站找到产品的软件升级和使用手册

办公地址：北京市东城区北三环东路 36 号 环球贸易中心 B 座 26F 02-05 室 邮编: 100013

技术支持中心电话：8008296688/ (028)66052968

技术支持中心传真：(028)85176948

维修中心地址：北京市东城区北三环东路 36 号 环球贸易中心 B 座 26F 02-05 室 邮编: 100013

维修中心电话：(010) 58257789

维修中心传真：(010) 58257790

网址：<http://www.dlink.com.cn>

办公时间：周一到周五，早09:00到晚18:00

D-Link[®]
Building Networks for People