

# DXS-1210 Series LZ 10 GIGABIT ETHERNET SWITCH SERIES

Ver. 1.02



# Table of Contents

Table of Contents	i
About This Guide	1
Terms/Usage	1
Copyright and Trademarks	1
1 Product Introduction	2
	2
Front Panel	3
Rear Panel	3
DXS-1210-12TC	3
Front Panel	3
Rear Panel	4
DXS-1210-12SC	4
Front Panel	4
Rear Panel	4
2 Hardware Installation	5
Safety Cautions	
Step 1: Unpacking	
Step 2: Switch Installation	
Desktop or Shelf Installation	
Rack Installation	
Step 3 – Plugging in the AC Power Cord	
Power Failure	
3 Getting Started	
Management Options	
Using Web-based Management	
Supported Web Browsers	
Connecting to the Switch	
Login Web-based Management	
Smart Wizard	
Web-based Management	
4 Configuration	
Smart Wizard Configuration	
IPv4 Information	
SNMP Settings	. 10
User Accounts Settings	
Web-based Management	
Tool Bar > Save Menu	
Save Configuration	
Tool Bar > Tool Menu	
Firmware Information	. 13
Configuration Information	. 13
Firmware Upgrade & Backup > Firmware Upgrade from HTTP	
Firmware Upgrade & Backup > Firmware Upgrade from TFTP	
Firmware Backup to HTTP & Backup > Firmware Backup to HTTP	
Firmware Backup to HTTP & Backup > Firmware Backup to TFTP	
Configuration Upgrade & Backup > Configuration Restore from HTTP	
Configuration Upgrade & Backup > Configuration Restore from TFTP	

Configuration Upgrade & Backup > Configuration Backup to HTTP	
Configuration Upgrade & Backup > Configuration Backup to TFTP	
Log Backup > Log Backup to HTTP	. 15
Log Backup >Log Backup to TFTP	. 15
Ping	. 16
Reset	. 16
Reboot System	. 16
Tool Bar > Smart Wizard	. 16
Tool Bar > Online Help	. 16
Function Tree	-
Device Information	. 18
System > System Information	
System > Port Configuration > Port Settings	. 19
System > Port Configuration > Port Status	
System > Port Configuration > Error Disable Settings	. 20
System > Port Configuration > Jumbo Frame	. 21
System > System Log > System Log Settings	. 21
System > System Log > System Log Server Settings	. 21
System > System Log > System Log	. 22
System > Time and SNTP > Clock Settings	. 22
System > Time and SNTP > Time Zone Settings	
System > Time and SNTP > SNTP Settings	
System > Time Range	. 24
Management > User Accounts Settings	
Management > Password Encryption	
Management > SNMP > SNMP Global Settings	
Management > SNMP > SNMP View Table Settings	
Management > SNMP > SNMP Community Table Settings	
Management > SNMP > SNMP Group Table Settings	
Management > SNMP > SNMP Engine ID Local Settings	
Management > SNMP > SNMP User Table Settings	
Management > SNMP > SNMP Host Table Settings	
Management > RMON > RMON Global Settings	
Management > RMON > RMON Statistics Settings	. 30
Management > RMON > RMON History Settings	
Management > RMON > RMON Alarm Settings	
Management > RMON > RMON Event Settings	
Management > Telnet/Web	
Management > Session Timeout	
Management > D-Link Discover Protocol Settings	
L2 Features > FDB > Static FDB > Unicast Static FDB	
L2 Features > FDB > Static FDB > Multicast Static FDB	
L2 Features > FDB > MAC Address Table Settings	
L2 Features > FDB > MAC Address Table	
L2 Features > 802.1Q VLAN	
L2 Features > Asymmetric VLAN	
L2 Features > VLAN Interface	
L2 Features > STP > STP Global Settings	
L2 Features > STP > STP Port Settings	. 40

L2 Features > STP > MST Configuration Identification	. 41
L2 Features > STP > STP Instance	. 42
L2 Features > STP > MSTP Port Information	. 42
L2 Features > Loopback Detection	
L2 Features > Link Aggregation	
L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings	
L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Groups Settings	
L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Mrouter Settings	
L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Statistics Settings	
L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Setting	
L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Groups Setting	
L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Mrouter Settings	
L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Statistics Settings	
L2 Features > L2 Multicast Control > Multicast Filtering	
L2 Features > LLDP Slobal Settings	
L2 Features > LLDP > LLDP Port Settings	
L2 Features > LLDP > LLDP Management Address List	
L2 Features > LLDP > LLDP Basic TLVs Settings	
L2 Features > LLDP > LLDP Dot1 TLVs Settings	
L2 Features > LLDP > LLDP Dot3 TLVs Settings	
L2 Features > LLDP - MED Port Settings	
L2 Features > LLDP > LLDP Statistics Information	
L2 Features > LLDP > LLDP Local Port Information	
L2 Features > LLDP > LLDP Neighbor Port Information	
L3 Features > ARP > ARP Aging Time L3 Features > ARP > Static ARP	
L3 Features > ARP > Static ARP	
L3 Features > IPv4 Interface	
L3 Features > IPv4 Internace	
L3 Features > IPv4 Delault Route	
L3 Features > IPv6 Neighbor	
L3 Features > IPv6 Default Route	
QoS > Port Default CoS	
QoS > Port Scheduler Method	
QoS > Queue Settings	
QoS > CoS to Queue Mapping	
QoS > Port Rate Limiting	
QoS > Queue Rate Limiting	
QoS > Port Trust State	
QoS > DSCP CoS Mapping	
ACL > ACL Configuration Wizard	
ACL > ACL Access List	
ACL > ACL Interface Access Group	
Security > Port Security Global Settings	
Security > Port Security > Port Security Port Settings	
Security > Port Security > Port Security Address Entries	
Security > DHCP Server Screening > DHCP Server Screening Global Settings	
Security > DHCP Server Screening > DHCP Server Screening Port Settings	
Security > Safeguard Engine	

Convite Traffic Commentation Cattings	91
Security > Traffic Segmentation Settings	92
Security > Storm Control Settings	92
Security > DoS Attack Prevention Settings	93
Security > SSL > SSL Global Setting	94
Security > SSL > SSL Service Policy	94
OAM > Cable Diagnostics	95
Monitoring > Statistics > Port	96
Monitoring > Statistics > Port Counters	97
Monitoring > Statistics > Counters	97
Monitoring > Mirror Settings	98
Green > Power Saving	99
Green > EEE	100
5 Command Line Interface	101
To connect a switch via TELNET:	101
Logging on to the Command Line Interface:	101
CLI Commands:	101
?	102
config ipif	102
logout	103
ping	103
reboot	104
reset config	104
show ipif	
show ipv6	105
show switch	
config account username	106
save	107
boot image	107
debug info	108
debug show tech-support	
Appendix A - Technical Specifications	110
Hardware Specifications	
Key Components / Performance	110
Port Functions	110
Physical & Environment	110
Emission (EMI) Certifications	110
Safety Certifications	111
Features	111
L2 Features	
L3 Features	111
D-Link Green Technology	
VLAN	
	111
QoS (Quality of Service)	
QoS (Quality of Service) Security Management	111

# About This Guide

This guide provides installation and instructions for the D-Link 10 Gigabit Ethernet L2 Switch (DXS-1210-12TC/12SC/10TS),

1

**Note:** The model you have purchased may appear slightly different from the illustrations shown in the document. Refer to the Product Instruction and Technical Specification sections for detailed information about your switch, its components, network connections, and technical specifications.

This guide is divided into four parts:

- 1. Hardware Installation: Step-by-step hardware installation procedures.
- 2. Getting Started: A startup guide for basic switch installation and settings.
- 3. D-Link Network Assistant: An introduction to the central configuration utility.
- 4. Configuration: Information about the function descriptions and configuration settings.

# Terms/Usage

In this guide, the term "Switch" (first letter capitalized) refers to the DSX-1210 Series switch and "switch" (first letter lower case) refers to other Ethernet switches. Some technologies refer to terms "switch", "bridge" and "switching hubs" interchangeably, and both are commonly accepted for Ethernet switches.



A **NOTE** indicates important information that helps a better use of the device.

A **CAUTION** indicates potential property damage or personal injury.

# Copyright and Trademarks

Information in this document is subjected to change without notice.

© 2014 D-Link Corporation. All rights reserved.

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

Trademarks used in this text: D-Link and the D-LINK logo are trademarks of D-Link 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 Corporation disclaims any proprietary interest in trademarks and trade names other than its own.

# Product Introduction

Thank you and congratulations on your purchase of D-Link DXS-1210 Series Switch.

D-Link's latest generation L2 10 Gigabit Ethernet switch series blends plug-and-play simplicity with exceptional value and reliability for small and medium-sized business (SMB) networking. All models are housed in a new style rack-mount metal case with easy-to-view front panel diagnostic LEDs, and provides advance features including network security, traffic segmentation, QoS and versatile management.

*Flexible Port Configurations:* DXS-1210 Series is D-Link's latest 10G switch which provides 8 ports, 10 ports 10GBASE-T and 12 ports SFP+ models. DXS-1210 Series switches have advantage of ease-of-use, rich feature sets by utilizing the neat and simplified Web GUI allowing users to access and configure easily from everywhere via a web browser. 10GBASE-T provides the requisite backward compatibility that allows end users to transparently upgrade from 10/100/1000Mbps network by using cost effective Cat 6, 6A, 7 unshielded and shielded twisted-pairs copper. 10G SFP+ has advantages of lower power consumption, longer distance support, better latency performance. Provide a cost effective application by utilizing the Direct Attach Cable (DAC) feature.

**D-Link Green Technology:** D-Link Green devices are about providing eco-friendly alternatives without compromising performance. D-Link Green Technology includes a number of innovations to reduce energy consumption on DXS-1210 series such as reducing power when a port does not have a device attached, or adjusting the power usage according to the Ethernet cable connected to it.

*Extensive Layer 2 Features:* Implemented as complete L2 devices, these switches include functions such as IGMP snooping, port mirroring, Spanning Tree, 802.3ad LACP, SNTP, LLDP and Loopback Detection to enhance performance and network resiliency.

*Extensive Layer 3 Features:* These switches include functions such as IP interface, static route, IPv6 Static Route, and ARP to enhance performance and network resiliency.

**QoS:** The switches support bandwidth control and 802.1p priority queues, enabling users to run bandwidth-sensitive applications such as streaming multimedia by prioritizing that traffic in network. These functions allow switches to work seamlessly with VLAN and 802.1p traffic and IPv6 traffic class priority in the network.

*Network Security:* D-Link's innovative Safeguard Engine function protects the switches against traffic flooding caused by virus attacks. Additional features such as Storm Control can help to keep the network from being overwhelmed by abnormal traffic. Port Security is another simple but useful authentication method to maintain the network device integrity. Also supports DHCP Server Screening, SSL and IP-MAC-Port Binding features.

*Versatile Management:* The new generation of D-Link 10 Gigabit Ethernet Switches provide growing businesses with a simple and easy management of their network, using a Web-Based management interface that allows administrators to remotely control their network down to the port level.

Users can also access the switch via TELNET. Some basic tasks can be performed such as changing the Switch IP address, resetting the settings to factory defaults, setting the administrator password, rebooting the Switch, or upgrading the Switch firmware by using the Command Line Interface (CLI).

In addition, users can utilize the SNMP MIB (*Management Information Base*) to poll the switches for information about the status, or send out traps of abnormal events. SNMP support allows users to integrate the switches with other third-party devices for management in an SNMP-enabled environment. D-Link DXS-1210 Series also comes with the D-View plug-in module that works with D-View 6 SNMP Management Software, and provides easy-to-use graphic interface and facilitates the operation efficiency.

# DXS-1210-10TS

8-Port 10GBASE-T and 2-Port SFP + Fiber port L2 10 Gigabit Ethernet Switch.

# **Front Panel**



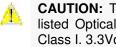
Figure 1.1 - DXS-1210-10TS Front Panel

**Power LED**<sup>(1)</sup>: The Power LED lights up when the Switch is connected to a power source.

**Fan error:** The Fan error LED lights up when the fan has runtime failure and is brought offline.

Reset: By pressing the Reset button, the Switch will change back to the default configuration and all changes will be lost.

Port Link/Act/Speed LED (1-8, 9F, 10F): The port LEDs indicate a network link through the corresponding port. Blinking indicates the Switch is either sending or receiving data to the port. When the port LED glows amber, it indicates the port is running at 100M or 1000M. When the port LED glows green, it is running at 10Gbps.



CAUTION: The MiniGBIC ports should use UL listed Optical Transceiver product, Rated Laser Class I. 3.3Vdc

#### **Rear Panel**



Figure 1.2 - DXS-1210-10TS Rear Panel

Power: Connect the AC power cord to this port.

# DXS-1210-12TC

8-port 10GBASE-T and 2-port 10G SFP+ also with additional 2-port 10GBASE-T/SFP+ combo port L2 10 Gigabit Ethernet Switch.

#### Front Panel



Figure 1.3 – DXS-1210-12TC Front Panel

**Power LED**<sup>(1)</sup>: The Power LED lights up when the Switch is connected to a power source.

Fan error: The Fan error LED lights up when the fan has runtime failure and is brought offline.

Port Link/Act/Speed LED (1-8, 9F, 10F, 11F, 12F): The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When a port has an amber light, this indicates that the port is running at 100M or 1000M. When it has a green light it is running on 10Gbps.



Reset: By pressing the Reset button, the Switch will change back to the default configuration and all changes will be lost.

# Rear Panel



Power: Connect the AC power cord to this port.

# DXS-1210-12SC

10-Port 10G SFP+ fiber port and 2-port 10GBASE-T/SFP + combo port L2 10 Gigabit Ethernet Switch.

# Front Panel

D-Link	.00.		Aurola	
٥				
12				
BXS-1210-1220		ਿਊਜਿਨ		

Figure 1.5 – DXS-1210-12SC Front Panel

**Power LED**<sup>1</sup>: The Power LED lights up when the Switch is connected to a power source.

Fan error: The Fan error LED lights up when the fan has runtime failure and is brought offline.

**Port Link/Act/Speed LED (1-10, 11F, 12F):** The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When a port has an amber light, this indicates that the port is running on 100M or 1000M. When it has a green light it is running on 10Gbps.



**CAUTION:** The MiniGBIC ports should use UL listed Optical Transceiver product, Rated Laser Class I. 3.3Vdc.

**Reset:** By pressing the Reset button, the Switch will change back to the default configuration and all changes will be lost.

# Rear Panel



Figure 1.6 – DXS-1210-12SC Rear Panel

Power: Connect the AC power cord to this port.

# 2 Hardware Installation

This chapter provides unpacking and installation information for the D-Link DXS-1210 Series Switch.

# 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, 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.
- 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.

# Step 1: Unpacking

Open the shipping carton and carefully unpack its contents. Please consult the packing list located in the User Manual to make sure all items are present and undamaged. If any item is missing or damaged, please contact your local D-Link reseller for replacement.

- One D-Link DXS-1210 Series switch
- One Multilingual Getting Started Guide
- User Guide CD with DNA (D-Link Network Assistant) Program
- Power Cord and Power Cord Retainer
- Rack-mount kit and Rubber Feet

If any item is found missing or damaged, please contact the local reseller for replacement.

# Step 2: Switch Installation

For safe switch installation and operation, it is recommended that you:

- Visually inspect the power cord to see that it is secured fully to the AC power connector.
- Make sure that there is proper heat dissipation and adequate ventilation around the switch.
- Do not place heavy objects on the switch.

#### **Desktop or Shelf Installation**

When installing the switch on a desktop or shelf, the rubber feet included with the device must be attached on the bottom at each corner of the device's base. Allow enough ventilation space between the device and the objects around it.

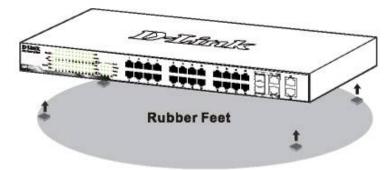


Figure 2.1 – Attach the adhesive rubber pads to the bottom

#### **Rack Installation**

The switch can be mounted in an EIA standard size 19-inch rack, which can be placed in a wiring closet with other equipment. To install, attach the mounting brackets to the switch's side panels (one on each side) and secure them with the screws provided (with 8 M3\*6.0 size screws).



Figure 2.2 – Attach the mounting brackets to the Switch

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

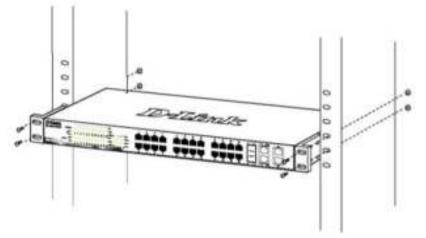


Figure 2.3 – Mount the Switch in the rack or chassis

# Step 3 – Plugging in the AC Power Cord

Users may now connect the AC power cord into the rear of the switch and to an electrical outlet (preferably one that is grounded and surge protected).

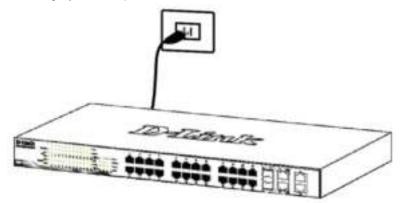


Figure 2.4 –Plugging the switch into an outlet

# **Power Failure**

As a precaution, the switch should be unplugged in case of power failure. When power is resumed, plug the switch back in.

# **3** Getting Started

This chapter introduces the management interface of D-Link DXS-1210 Series Switch.

# Management Options

The D-Link DXS-1210 Series. Switch can be managed through any port by using the Web-based Management, or through any PC using CLI commands.

Each switch must be assigned its own IP Address, which is used for communication with the Web-Based Management or a SNMP network manager. The PC should have an IP address in the same subnet as the switch. Each switch can allow up to four users to access the Web-Based Management concurrently.

Please refer to the following installation instructions for the Web-based Management.

# Using Web-based Management

After a successful physical installation, you can configure the Switch, monitor the network status, and display statistics using a web browser.

# Supported Web Browsers

The embedded Web-based Management currently supports the following web browsers:

- Internet Explorer 8 or later version
- Chrome
- Firefox
- Safari

# Connecting to the Switch

You will need the following equipment to begin the web configuration of your device:

- 1. A PC with a RJ-45 Ethernet connection
- 2. A standard Ethernet cable

Connect the Ethernet cable to any of the ports on the front panel of the switch and to the Ethernet port on the PC.

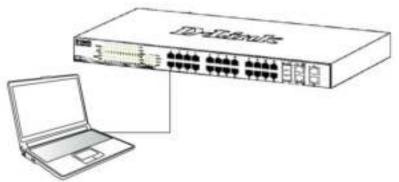
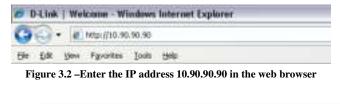


Figure 3.1 – Connected Ethernet cable

#### Login Web-based Management

In order to login and configure the switch via Web-based GUI, the PC must have an IP address in the same subnet as the switch. For example, if the switch has an IP address of **10.90.90.90**, the PC should have an IP address of **10.x.y.z** (where x/y is a number between  $0 \sim 254$  and z is a number between  $1 \sim 254$ ), and a subnet mask of **255.0.0.0**. There are two ways to launch the Web-based Management.



**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.

When the following login dialog box appears, enter the password and choose the language of the Webbased Management interface then click  $\mathbf{OK}$ .

The switch supports 10 languages including English, Traditional Chinese, Simplified Chinese, German, Spanish, French, Italian, Portuguese, Japanese and Russian. By default, the Username and Password are empty and the language is **English**.

Connect to 10.90	90.90	
Card I		
Enter your usen User Name Password	name and password	
Language	English	Logit Reset

Figure 3.3 – Login Dialog Box

#### Smart Wizard

After a successful login, the Smart Wizard will guide you through essential settings of the D-Link DXS-1210 Series Switch. Please refer to the Smart Wizard Configuration section for details.

#### Web-based Management

By clicking the **Exit** button in the Smart Wizard, you will enter the Web-based Management interface. Please refer to Chapter 4 <u>Configuration</u> for detailed instructions.

# **4** Configuration

The features and functions of the D-Link DXS-1210 Series Switch can be configured for optimum use through the Web-based Management Utility.

# Smart Wizard Configuration

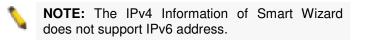
After a successful login, the Smart Wizard will guide you through essential settings of the D-Link DXS-1210 Series Switch. If you do not plan to change anything, click **Exit** to leave the Wizard and enter the Web Interface. You can also skip it by clicking **Don't show Smart Wizard next time** for the next time you logon to the Web-based Management.

# IPv4 Information

IPv4 Information will guide you to do basic configurations on 3 steps for the IP Information, access password, and SNMP. Select **Static**, to manually enter a new **IP Address**, **Netmask** and **Gateway** address, or select DHCP to automatically receive IP settings from a DHCP server. Click the **NEXT** button to enter the SNMP settings page The IP address is allowed for IPv4 and IPv6 address. If you are not changing the settings, click **Exit** button to go back to the main page. Or you can click on **Ignore the wizard** next time to skip wizard setting when the switch boots up.

Step 1 of 3 7 Coherenty System IP Internet	//14/11/1	114463	corrept	vie setilog	n Nir Bytt	het E al	1994455-29	itmasik, and
	DHOP							
W Address	INCOME.	90	31	90 1				
Gateroay	.0	D	.0	0				
iphone The rectard read							9	

Figure 4.1 – IPv4 Information in Smart Wizard



#### **SNMP Settings**

The SNMP Settings page allows you to quickly enable/disable the SNMP function. The default SNMP Setting is **Disabled**. Click **Enabled** and then click **Next**, then it will enter the **User Accounts Settings** page.

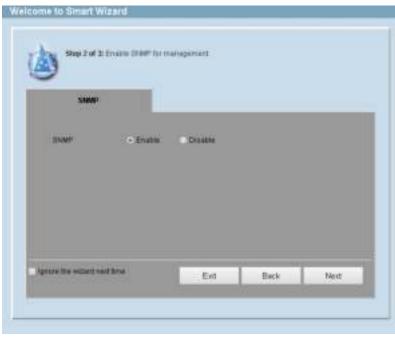


Figure 4.2 – SNMP Settings in Smart Wizard

#### **User Accounts Settings**

The User Accounts Settings page allows you to quickly specify the user account function. Enter the **User Name**, **Privilege**, **Password Type** and **Password**. Click **Apply & Save** to save the configuration.

liture Accounts Sell	inga		
Marrie Marrie	5		
Protege (1-15)			
Password Time	None	•	
Passwerg			

Figure 4.3 – User Accounts Setting in Smart Wizard

#### Web-based Management

After clicking the Exit button in the Smart Wizard you will see the screen below:

	In	Tool Bar		
( Local Street S	Devile recorder			and a second state of a
na Line (III: Avagene Line and State State State State State Function Tree	Alway a University of States Sector States Research Always Research Always Res	Hain Configuration Screen	RCCARENCE Induced State Sector	WL 22-00 (T 2/9-14 1-540 WL 20 URAA K WAAA WAAA WAAA AA WAAA AA AA WAAA AA WAAA AA WAAA AA WAAA AA WAAA AA WAAA AA WAAA AA WAAA AA AA WAAA AA WAAA AA WAAA AA WAAA AA WAAA AA AA AA WAAA AA AA AA WAAA AA

Figure 4.4 – Web-based Management

The above image is the Web-based Management screen. The three main areas are the **Tool Bar** on top, the **Function Tree**, and the **Main Configuration Screen**.

The **Tool Bar** provides a quick and convenient way for essential utility functions like firmware and configuration management.

By choosing different functions in the **Function Tree**, you can change all the settings in the **Main Configuration Screen**. The main configuration screen will show the current status of your Switch by clicking the model name on top of the function tree.

At the upper right corner of the screen the username and current IP address will be displayed.

Under the username is the **Logout** button. Click this to end this session.

**NOTE:** If you close the web browser without clicking the **Logout** button first, then it will be seen as an abnormal exit and the login session will still be occupied.

Click the D-Link logo at the upper-left corner of the screen to be redirected to the local D-Link website.

#### Tool Bar > Save Menu

The Save Menu provides Save Configuration and Save Log functions.



#### Save Configuration

Select to save the entire configuration changes you have made to the device to switch's non-volatile RAM.

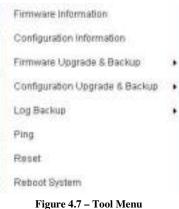
entration	Cartyt		of materials	
-----------	--------	--	--------------	--

Figure 4.6 – Save Configuration

**Destination:** Select the configuration destination to be saved. **Startup-config:** Check the box to enable the startup configuration function. Click the **Apply** button to save your settings.

# Tool Bar > Tool Menu

The Tool Menu offers global function controls such as Reset, Reboot Device, Configuration Backup and Restore, Firmware Backup and Upgrade.



#### **Firmware Information**

Display the firmware information for the 2-image ID.

an papakan				
-	Western	544 00	Caster litte	
111	V1.0.014	2146384	Apr/14.2211.6	doot Up
- I -	WI D.D14	2140203	AN 18 201X -	Boot Up

Figure 4.8 – Tool Menu > Firmware Information

#### **Configuration Information**

Display the configuration information on the Switch.

	Carrige share 0	Size (III	Undate Time		
-	*) r	0	4	Root in	
	1.1	0	*	Doort Up	

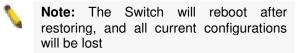
Figure 4.9 – Tool Menu > Configuration Information

#### Firmware Upgrade & Backup > Firmware Upgrade from HTTP

Allow existing firmware file to be uploaded to the Switch from HTTP.

enerware Opgrade en		
Personal Oppiado Disre III		
Source URL	Bitem	
Destrution UPG	inagi1 (*	
		Seatede

Figure 4.10 – Tool Menu > Firmware Upgrade & Backup > Firmware Upgrade from HTTP

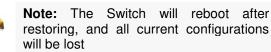


#### Firmware Upgrade & Backup > Firmware Upgrade from TFTP

Upgrade firmware by using TFTP. Enter the TFTP IP address, source URL, and select a Destination URL. Click **Upgrade**.

reenro Vagrado Born II			
F1F Darves #		= Pv4	
	÷1	1.114	
louite URL Sectorator URL	144Pmm		
Sector and a 1995	(maget		
			lograde

Figure 4.11 – Tool Menu > Firmware Upgrade & Backup > Firmware Upgrade from TFTP



#### Firmware Backup to HTTP & Backup > Firmware Backup to HTTP

To save a backup of the firmware, select the source URL and then click **Backup**.

Configuration Backup to HTTP	
Configuration Dechap to HTTP	
Backup Configuration Re	
	Balkin

Figure 4.12 – Tool Menu > Firmware Upgrade & Backup > Firmware Backup to HTTP

#### Firmware Backup to HTTP & Backup > Firmware Backup to TFTP

To save a backup of the firmware using TFTP, enter the TFTP server IP address, the source URL, and the destination URL. Click **Backup**.

Firmware Backup to triff Firmware Backup is 1719			
TETT Darver (*	-	C Pri	
Bouta Destination URL	mapit *	10.00	
Destination UFR.	Editoria	3	hathar
			For Mar

Figure 4.13 – Tool Menu > Firmware Upgrade & Backup > Firmware Backup to TFTP

#### Configuration Upgrade & Backup > Configuration Restore from HTTP

To restore the Switch from a saved configuration file, select a **Source URL**, configuration **Destination** and click **Restore**.

Configuration Restore	from H11P	_		
Baute (195, Destruition	[Cevig f	(Browns,	21 status-cento	
		TR.		fasture

Figure 4.14 – Tool Menu > Configuration Upgrade & Backup > Configuration Restore from HTTP

Startup-config: Check the box to enable the startup configuration function.

#### Configuration Upgrade & Backup > Configuration Restore from TFTP

To load the Switch's configuration from a saved configuration file using TFTP, enter the TFTP server IP address and source URL, then click **Restore**.

Configuration Restore	IGEN TETE	
Configuration Restaura from 11		
1917 Same P	# Pet	
Boursi (M),	remark 3	
		Restore

Figure 4.15 – Tool Menu > Configuration Upgrade & Backup > Configuration Restore from TFTP

#### Configuration Upgrade & Backup > Configuration Backup to HTTP

To save the current configuration to a file, click **Backup**.

Configuration	Backup to HTTP		
Smithe	[Config 1 •]	👻 startup config	Tarine

Figure 4.16 – Tool Menu > Configuration Upgrade & Backup > Configuration Backup to HTTP

# Configuration Upgrade & Backup > Configuration Backup to TFTP

To save the current configuration to a file using TFTP, click **Backup**.

TP Same P	1	# Pri	
100.0		· Statu-unity	
octonation 1,471.	Lis dans		

Figure 4.17 – Tool Menu > Configuration Upgrade & Backup > Configuration Backup to TFTP

TFTP Server IP: Select IPv4 or IPv6 and enter the IP address.

**Source:** Select the source configuration file.

Startup-config: when checking the box, only the current startup configuration file will be backed up which might be kept in "Config 1" or "Config 2" location.

Destination URL: Enter the destination URL.

# Log Backup > Log Backup to HTTP

To save the log to a file and click **Backup.** 

Log Backup to HTTP	
Dackup System Log Be	Backup

Figure 4.18 – Tool Menu > Log Backup > Log Backup to HTTP

# Log Backup >Log Backup to TFTP

To save the log to a file using TFTP, enter the TFPT server IP address and destination URL then click **Backup**.

Log Backup to TFT	Lii		
Log Bacher to 1717			
TF1P (server #		a Pel	
	-	0.84	
Decision URL	- the stand		Ballup
			L_Balkup

Figure 4.19 – Tool Menu > Log Backup > Log Backup to TFTP

**TFTP Server IP:** Select **IPv4** or **IPv6** and enter the IP address. **Destination URL:** Enter the destination URL.

# Ping

To ping a computer or device, enter either **Target IPv4 or IPv6 Address**, **Ping Times** and **Timeout**. Enter the required information, Tick the **Infinite** option, to disable the **Ping Times** feature and click **Apply**. The results will be displayed in the **Result** box.

10.02		
Evel Pring		
Tauget Pol Annesi	Contraction of the second	
Ping Times cl-2019	A 1000	
Timenal (1-19)		
		Apph
NE Ping		
Terpid Pull Address	120(5)	
Ping Timisa (5-200	Q 2545	
Tenend /1-NW	586	
		Apply

Figure 4.20 – Ping

# <u>Reset</u>

Select which reset option you want to perform and click Apply.

wat	
The Bwitch will be reset to its factory behaufts except IF address, and then will save, rebot.	
The Switch will be reset to its factory defaults including # address.	Apply

Figure 4.21 – Tool Menu > Reset

# Reboot System

Select to save your current settings and then click **Reboot** to restart the Switch.

Perioral System			
Do you want to new the bettergs ?	Uner internet		
Destription	Cevity U.	ie status-cong	
If you do not used the pathogs, at you	terioday reasons with a shain regra		Report

Figure 4.22 – Tool Menu > Reboot System

Destination: Select the configuration destination to be saved.

**Startup-config:** when checking the box, only the current startup configuration file will be backed up which might be kept in "Config 1" or "Config 2" location.

# Tool Bar > Smart Wizard

By clicking the **Smart Wizard** button, you can return to the Smart Wizard if you wish to make any changes.

# Tool Bar > Online Help

The Online Help provides two ways of online support: **D-link Support Site** will lead you to the D-Link website where you can find online resources such as updated firmware; **User Guide** can offer an immediate reference for the feature definition or configuration guide.



Figure 4.23 – Online Help

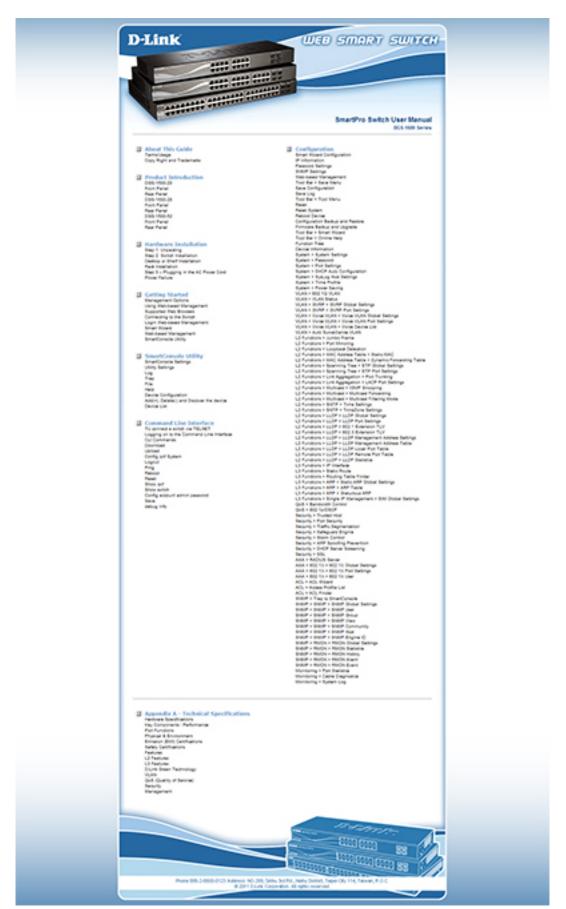


Figure 4.24 – User Guide Micro Site

# **Function Tree**

All configuration options on the switch are accessed through the Setup menu on the left side of the screen. Click on the setup item that you want to configure. The following sections provide more detailed description of each feature and function.



Figure 4.25 – Function Tree

# **Device Information**

The Device Information provides an overview of the switch, including essential information such as firmware & hardware information, and IP settings.

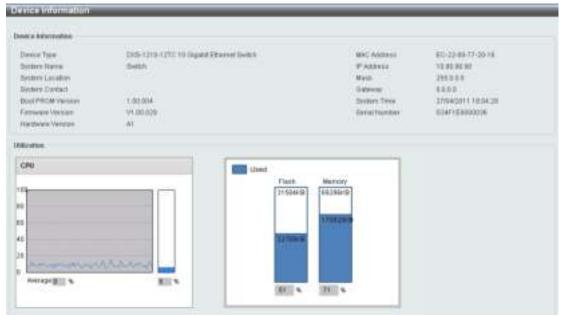


Figure 4.26 – Device Information

# System > System Information

The System Setting page allows you to configure basic system information.

#### System Information Settings: Enter a System Name, System Location and System Contact.

System Internation Settings	
Dyckers Name	
Nysters Lacatory	
Dyslers Curdad	40010

Figure 4.27 – System > System Information

#### System > Port Configuration > Port Settings

In the Port Settings page, the status of all ports can be monitored and adjusted for optimum configuration.

art Seltings			_					
net Settings								
From Funt whit /url • Dramm	To Put eth/201 • Spinet	Nette Conversion Constitute Advice Constitute Advice	dive.	elled •	Ado Dovergrade [Droabled •] Description	Plue Cost Of	•	
Auto •	Auto •	S.000 S.0			(Milting)		Apply	Petrest
Part	Lore Skatur	Slate	Same	Forcesse	Danto	Speed	Andre Disserange andre	Description
anitati .	. Ue	Example	ÚŃ.		Adv mater	Add Lawrence	Durani	l.
ABYDOD.	Daven	Excited	60	ंत	Aldo-Dahei	NATI-LOWED	Deabed	
and Gris	Q0w0	Exural.	0f	50	Public during	Auto-spans	Destas	
140(1/0+4	.Cowt	-Diverse	OM.	OF.	Auto-Ratio	Allenant	Distant	
attribut.	Crun	Statet.	101	08	Auto-mains		-Dusses	
ath title	Cost	Expend	108	Cf.	Automation	indo-spand	Driating	
####10V	Circl	25ares	OK .	CW.	Auto-Matter	Adversed	Dutted	
49108	Open.	Expend	598	- 68	Aph digtes	ABINDED	Doabort	
wite143-9471	Cowe.	Evaluet	04	C.E.	Auto digiting	Adversed.	Dashed	
(461/07102)	Cower	Ecutors	OR .	OF	N/N-IEADO	ALE-10701	Department	
(00TFFTTDD)	Cown	Course	1/1	¢.e	Auto-Highten	A2+1210	Distant	
attraction (	(Down	Course)	08	08:	Auto-digene	ALBOTTOPOS	Doption	
0811012023	Open	Chamad	318	1.68	Auto-paper	PLE> 00000	Destant	
********	Cost	Enstred.	18	C#	App-Duble	4.0-12405	. Dested	

Figure 4.28 – System > Port Configuration > Port Settings

From Port / To Port: Select the appropriate port range to be configured.

State: Enable or disable the physical port.

**Auto Downgrade:** To enable or disable automatically downgrading advertised speed in case a link cannot be established at the available speed.

**Flow Control:** Select **On** or **Off**. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use back-pressure flow control, and Auto ports use an automatic selection of the two.

Duplex: Select the duplex mode used. Options to choose from are Auto and Full.

**Speed:** Select the speed for the ports. The speed values are **Auto**, **100M**, **1000M**, **1000M Master**, **1000M Slave**, and **10G**. The Switch allows you to configure two types of Gigabit connections; **1000M Master** and **1000M Slave** which refer to connections running a 1000BASE-T cable for connection between the Switch port and another device capable of a Gigabit connection. The master setting (1000M Master) 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 (1000M Slave) uses loop timing, where the timing comes from a data stream received from the master. If one connection is set for 1000M Master, the other side of the connection must be set for 1000M Slave. Any other configuration will result in a link down status for both ports.

Capability Advertised: When the Speed is set to Auto, these capabilities are advertised during autonegotiation.

**Description:** Enter a 64 characters description for the corresponding port.

Click **Apply** button to save your settings.

Click the **Refresh** button to refresh the display table.

#### System > Port Configuration > Port Status

The Port Settings page allows you to view the Switch's physical port status and settings. The table will display the Port, Status, MAC Address, VLAN, Flow Control Operator, Duplex, Speed and Type.

Tallah .							
Part	00000	MAC Automa	VIAN	Parent Star	manual Disperciption	Dama	(Carried Street
1 1245	1000	NVN, FALSTINE	100	See 1	Neutre	0.00	Second Second
10001020	Crimeland	EC-03-85/01.20/07	0.800	(10 <b>9</b> )	UR	Pulli FLB	A& 12110
#01100E	SUPCOMMENT.	#C-25-85-77-85-18		100	08	1445	444
49(1003	1404 Contracted	EC-23-45-77 (5-19	10411	UR .	201	4,61	100
##15%=	AbhComaded	EC-35-45-77-33-14	1	- 12	18	440	4,00
-481102	TEN Constant	80.02.80 TT 23.10	1	114	舗	4,05	-
am1008	164-Cerescher	80-40-80-77-30-90		08	ÚŤ	Aste	144
481107	PARA CONTRACTOR	80 40 77 30 40	0.000	0.0	OK.	Aple	1475
atvine	HIFOUVERNI .	20-22-40-77-25-HE		101	DR .	Age	645
##15.57	Tol-Coveraged	EC-03-89-75-09-10	10.000	11	UR	Apre	100
1010107071	Not-Converted	EC 03 89-77 29-21	1	117	0ft	440	100
-8110210123	It if Corrected	10.03148-0149-01		100	100	Auto	144
ercul(11F)	FBIE-GREWING	80.2289-17.0011	1	119	101	April	140
white-to-to-	Tell-Consumed .	2003239277-25-23	4		10f	Auto	144
am tort(F)	tairConsites	#C-33-46-17 (0-13		110	108	9,01	NaME 1

Figure 4.29 – System > Port Configuration > Port Status

#### System > Port Configuration > Error Disable Settings

The Error Disable Settings page allows you to configure the sending of SNMP notifications for error disable state.

nar Dhudan Trigi Bathaga				
usefed Doabled				
Deated Deathed				
Software Rose of States			Apply	
na Daatie Recency Settings				
ExClosely Cause Al R State Dealed R	Internal.(2-80405)	(	Serv.	
Entheaters Cause	510%	Substrat (Sec)		
Pat lecuto	Olugied.	302		
Item Dekil	Crowney.	30		
ARP Rate	Diateled	300		
Brits Max Provider	Distant	.308		
DHCP Rule	Dutter	303		
Local and Denet	Driver	30		
Interfaces that will be recovered at the react takeout :				
	En Douter Course	Targe with Direct		

Figure 4.30 – System > Port Configuration > Error Disable Settings

#### **Error Disable Trap Settings:**

**Asserted:** Select to enable or disable the notifications when entering into the error disabled state. **Cleared:** Select to enable or disable the notifications when exiting from the error disabled state. **Notification Rate (0-1000):** Enter the number of traps per minute. The packets that exceed the rate will be dropped. The value is between 0 and 1000.

Click the **Apply** button to save your settings.

#### **Error Disable Recovery Settings:**

ErrDisable Cause: Specify the error disable causes. Options to choose from are All, Port Security, Storm Control, ARP Rate, BPDU Protect Protection, DHCP Rate and Loopback Detect.

**State:** Select to enable or disable the auto-recovery for an error port caused by the specified cause. **Interval (5-586400):** Enter the time interval. The values are between 5 and 586400 seconds.

Click the **Apply** button to save your settings.

#### System > Port Configuration > Jumbo Frame

The Jumbo Frame page allows you to view and configure the Jumbo Frame size and settings. Jumbo frames are Ethernet frames with more than 1,518 bytes of payload. The Switch supports jumbo frames with a maximum frame size of up to 9216 bytes.

Jumbo Frame Settings		
Autou Prane From Post To Post (whit6/1 •) (whit6/1 •)	Maarinam Raccom France Star (1918-5216) [1526 ] Intro	Apply
	Maximum Resolve Frame Star (byles)	
#8.15/1	1636	
WALKEE	(134	
¥8:101	1614	
46.104	1121	
48158	1128	
481128	1136	
wents/1	109	
/ #8168	1038	
20100	11.00	
abit/decid	1136	
110110	1138	
Verticit2	11.28	

Figure 4.31 –System > Port Configuration > Jumbo Frame

#### System > System Log > System Log Settings

The System Log Settings page allows you to view and configure the system's log settings.

System Log Settings		_			
Claimal State					
Strate Interface State	Enabled	•			
Tope.	VUM	•	100 (1-6098)	1	Adulty
Dothe Log Settings					
Puter Lig Des	Enabled				
Diretty	4(Warnings)				
WHEN DATAS (D-858245)	100	141	() ( definition		Apply

Figure 4.32 – System > System Log > System Log Settings

#### Global State:

Source Interface State: Select to enable or disable the source interface's global state.

Type: Select the type of interface that will be used. The default option is VLAN.

VID (1-4094): Specifies the VLAN ID. The possible range is 1 - 4094,

Click the **Apply** button to save your settings.

#### Buffer Log Settings:

Buffer Log State: Select to enable or disable the buffer log state. The options are Enable, Disable and Default.

**Severity:** Select the severity value of the type of information that will be logged. The values are 0 (Emergencies), 1 (Alerts), 2 (Critical), 3 (Errors), 4 (Warnings), 5 (Notifications), 6 (Informational), and 7 (Debugging).

Write Delay (0-65535): Enter the interval for periodic writing of the logging buffer to Flash. The value is between 0 and 65535 seconds. And default is 300 seconds. Tick the Infinite option, to disable the write delay feature.

Click the **Apply** button to save your settings.

#### System > System Log > System Log Server Settings

The System Log Server Settings page allows you to view and configure the system log's server settings.

ag Serar				
a Ifri Abbass		- Pri Astern	and the second s	
JCP Pad (114 or 1824-68820)	114	Saveth	4(Wareega)	•
with	(0 +)			
				Aboly
otal Embres : 2				
Server #	Serverty	Factory	UEP Part	
	and in the local sector of	101 - Contract 10	-914	
182,140,10,10	marings			Celeta

Figure 4.33 – System > System Log > System Log Server Settings

IP Address: Select and enter the IPv4 address or IPv6 Address.

**UDP Port (514 or 1024-65535):** Enter the system log server's UDP port number. This value must be 514 or between 1024 and 65535. The default value is 514.

Severity: Select the severity value of the type of information that will be logged. Options to choose from are 0 (Emergencies), 1 (Alerts), 2 (Critical), 3 (Errors), 4 (Warnings), 5 (Notifications), 6 (Informational), and 7 (Debugging).

Facility: Select the facility value. The values must be between 0 and 23.

Click the **Apply** button to save your settings.

#### System > System Log > System Log

The System Log page displays the system logs on the Switch.

danstag			
			Clear Lo
and Databas 8	Time	Lord .	

Figure 4.34 – System > System Log > System Log

#### System > Time and SNTP > Clock Settings

The Clock Settings page allows you to configure the time settings for the Switch.

Clock Settings Occupies		
Turve (Hert Mill 53) Deale (2004/9911)	20 60/07 36/12/2012	Apply

Figure 4.35 – System > Time and SNTP > Clock Settings

**Time (HH:MM:SS):** Enter the current time in hours, minutes, and seconds. **Data (DD/MM/YY):** Enter the current day, month, and year to update the system clock.

Click the Apply button to save your settings.

#### System > Time and SNTP > Time Zone Settings

The Time Zone Settings page allows you to configure time zones and Daylight Saving Time settings for SNTP.

Duration Title Talle	Doubled .		
Time Zone	(+ • [00 • [00 •]		
lacarity failing			
Form Planet, of the Humble	(Las: •)		
Nore. Day of the Weste	Lise. •		
Fore Mode	Liev		
Films: Tirke 2-4-5MM	(a) • (a)	•	
To three of the Words			
To Day of the Week	50. *		
Te Marth	1 in		
Tarrie (FIFFMAC	(0) + (0)		
ottual	70		
late Settings			
Sore: Eade of the Month	(iii · · )		
NORT MONTH	Ú., .		
hdrichtear			
ROTU. THINK BIRGEMOND	£co • 100	•]	
to: Data office No.effi	514 · · ·		
Ta: Manth:	(Jac. +		
To Take	11		
a Tave permit	Em + Hua	•1	
Mut	(C)	2.6	

Figure 4.36 – System > Time and SNTP > Time Zone Settings

Summer Time State: Select Summer Time State setting. Options to choose from are Disabled, Recurring Setting, and Date Setting.

Time Zone Offset: Select the local time zone's offset from Coordinated Universal Time (UTC).

The Recurring Setting can be configured below:

From:Week of the Month – Select week of the month that daylight saving time will start.

From:Day of the Week - Select day of the week that daylight saving time will start.

From:Month – Select the month that daylight time will start.

From:Time in HH MM – Select the time of the day that daylight saving time will start.

To:Week of the Month – Select week of the month that daylight saving time will end.

To:Day of the Week – Specify day of the week that daylight saving time will end.

**To:Month** – Select the month that daylight saving time will end.

To:Time In HH MM – Select the time of the day that daylight saving time will end.

**Offset** – Enter the number of minutes to add during daylight saving time. The default value is 60. The range of this offset is 30, 60, 90 and 120.

The **Date Setting** can be configured below:

From:Date of the Month - Select date of the month that daylight saving time will start.

**From:Month** – Select the month that daylight saving time will start.

From:Year – Select the year that the daylight saving time will start.

From:Time In HH MM – Select the time of the day that daylight saving time will start.

To:Date of the Month – Select the date of the month that daylight saving time will end.

**To:Month** – Select the month that daylight saving time will end.

To:Year - Select the year that the daylight saving time will end.

To:Time In HH MM – Select the time of the day that daylight time will end.

**Offset** – Select the number of minutes to add during daylight saving time. The default value is 60. The range of this offset is 30, 60, 90 and 120.

Click the **Apply** button to save your settings.

# System > Time and SNTP > SNTP Settings

The SNTP Settings page allows you to configure the time settings for the Switch.

ivTP Settings				
ATP Galax Sattlege				
Current Take Dource	Seitern Cikula			
SNIP State	Dustied +			
Pot interval (28 million)	720 846			Apply
ATT? Server Setting				
er thvé Address		O Pvi Assess	Contra de la contr	
				Apply
Total Entries 12				
SHOP METHOD	Station	Merculan	Losi Pacana	the second second second
19210810110	100 C		111 A.	Dewte
2014.2				Delate

Figure 4.37 – System > Time and SNTP > SNTP Settings

#### **SNTP Global Settings:**

SNTP State: Select to enable or disable the SNTP state.

**Poll Interval (30-99999):** Enter the poll interval. The value is from 30 to 99999 seconds. The default interval is 720 seconds.

Click the Apply button to save your settings.

#### **SNTP Server Setting:**

**IPv4 Address:** Enter the IPv4 address of the SNTP server which provides the clock synchronization. **IPv6 Address:** Enter the IPv6 address of the SNTP server which provides the clock synchronization. Click the **Apply** button to add the SNTP server.

#### System > Time Range

The Time Range page allows you to view and configure the time range settings for the Switch.

Range Harse		(Delt)		
From Week	SUN .	Tiz Week	SUN . U End Waveday	
From Time (H+1996)	00 * 00 *	Tiz Tana (Hirida)	00 + 100 +	Apply
Range Memor Initial Entrine 11	E me			- Pot
	-Barrie		End manifest	ENTRE U
		Page1/1 First Page		t Page Page of

Figure 4.38 – System > Time Range

Range Name: Enter a name for the time range. The name can be up to 32 characters long.

**From Week** / **To Week:** Select the starting and ending days of the week that will be used for this time range. Tick the **Daily** option to use this time range for every day of the week. Tick the **End Week Day** option to use this time range from the starting day of the week until the end of the week, which is Sunday.

From Time (HH:MM) / To Time (HH:MM): Select the starting and ending time of the day that will be used for this time range. The first drop-down menu selects the hour and the second drop-down menu selects the minute.

Click the **Apply** button to save your settings.

Click the **Find** button to locate a specific entry based on the information entered.

#### Management > User Accounts Settings

The User Accounts Settings page allows you to create and configure user accounts. Active user account sessions can be viewed. By default, there is no user account created on the Switch.

The pre-defined user account privilege levels supported by this switch are:

- Basic User Privilege Level1. This user account level has the lowest priority of the user accounts. The purpose of this type of user account level is for basic system checking.
- Operator Privilege Level 12. This user account level is used to grant system configuration information for users who need to change or monitor system configuration, except for security related information such as user accounts and SNMP account settings.
- Administrator Privilege Level 15. This administrator user account level can monitor all system information and change any of the system configuration settings expressed in this guide.

User Management Settings	Sexsion Table		
Etter Accounts			
Lier Transe	Privilego (1.1%)		
watered Type Hand	<ul> <li>Persvert</li> </ul>		Apply.
al Extrino ( T			
Unitiers	filmps .	Parawint	

Figure 4.39 – Management > User Accounts Settings

User Name: Enter the name of the user name. The name can be up to 32 characters long.

Privilege (1-15): Select the privilege level for this account. The value is between 1 and 15.

Password Type: Select a password type for this user account. The options are None, Plain Text, and Encrypted.

**Password:** If you selected either **Plain Text** or **Encrypted** for the password type, please enter a password for this user account.

Click the **Apply** button to save your settings.

Click the **Delete** button to remove the specified user account entry.

After clicking the **Session Table** tab, the following page will appear:

User Morogerent Sottings	Sossen Takle			
lutal Cottoes : 2				
Tax	Unior Numer	Postage	Logan Tenas	ST Address
Garraie	ang my misute	- 18	10	

Figure 4.40 – Management > User Accounts Settings – Session Table

#### Management > Password Encryption

The Password Encryption page allows you to enable or disable password encryption.

anneed Georgeticer Gettings			
servere Exception (Balo	0.004	nut	Apple .

Figure 4.41 – Management > Password Encryption

**Password Encryption State:** Specify to enable or disable the password encryption. Click the **Apply** button to save your settings.

#### Management > SNMP > SNMP Global Settings

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) protocol 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 on the Switch or your local 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 default SNMP global state is disabled. Select **Enable** and then select **Trap Settings**. Click **Apply** to enable the SNMP function.

SNMF Global Settings		
SIBIP Global Settings		
SNMP Grosul Blate SNMP Response Broadcast Request SNMP (UCP Port (0-85515)	Enabled      Enabled     Enabled     Enabled     Enabled     Enabled	
Trap Gource Interfacer	stant	
Trop Settings		
Trap Olohal Bate	Enabled      Disabled	Αρρίγ

Figure 4.42 – Management > SNMP > SNMP Global Settings

#### SNMP Global Settings:

**SNMP Global State:** Select to enable or disable the SNMP feature.

**SNMP Response Broadcast Request:** Select to enable or disable the server to response to broadcast SNMP GetRequest packets.

SNMP UDP Port (0-65535): Enter the SNMP UDP port number. The value is between 0 and 65535.

**Trap Source Interface:** Specify the interface whose IP address will be used as the source address for sending the SNMP trap packet.

#### Trap Settings:

Trap Global State: Select to enable or disable the sending of all or specific SNMP notifications.

**SNMP Authentication Trap:** Tick this option to control the sending of SNMP authentication failure notifications. An authenticationFailuretrap is generated when the device receives an SNMP message that is not properly authenticated. The authentication method depends on the version of SNMP being used. For SNMPv1 or SNMPv2c, authentication failure occurs if packets are formed with an incorrect community string. For SNMPv3, authentication failure occurs if packets are formed with an incorrect SHA/MD5 authentication key.

**Port Link Up:** Tick this option to control the port link up notifications.

Port Link Down: Tick this option to control the port link down notifications.

**Coldstart:** Tick this option to control the sending of SNMP coldStart notifications.

Warmstart: Tick this option to control the sending of SNMP warmStart notifications.

Click the **Apply** button to save your settings.

#### Management > SNMP > SNMP View Table Settings

The SNMP View page allows you to maintain SNMP views to community strings that define the MIB objects which can be accessed by a remote SNMP manager.

where	Titolan	1		
Instant (IC)	lini a	1		
forer Taxos	Included .	ŧ		
a grant and the state	(Processing )			
				-
etal Letrics : 0				
View R	and the second	Salation CRD	Allow Type	-
webb	36.	7.285271	" heathedent	Deteta
	2.52	0.343,2131	The Lot of	Real and
10181	10.5			Dehte
10.00		LEBIASINET	in An altered	Deleta
	98			
14.00	948 543	LEBIASHIEF	in/habel	Coluta
inits mits	98 51 54	CARTACHURY CARTACHURY	installed installed	Celeta Deleta
incide model model	na ing Wé Wény	CARTACHURY CARTACHURY	included included included	Calata Delata Delata

Figure 4.43 – Management > SNMP > SNMP View Table Settings

View Name: Create a name of the view, up to 32 characters.

**Subtree OID:** 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 the configured OID is Included or Excluded that a SNMP manager can access.

Click Add to create a new view or Delete to remove an existing view.

#### Management > SNMP > SNMP Community Table Settings

The SNMP Community page allows you to maintain the SNMP community string of the switch. SNMP managers using the same community string are permitted to gain access to the Switch's SNMP agent.

BE Convenienty Table Setti					
view Trape	Plan Test				
Community Name	Trime				
lew liane	14 Hours				
kamas Hegel	Read Only				
P Access Lightene	1. store				
					Add
letal Extrino : 2					
Concernently Nam		Water Martial	Access Sales	B"Access. Carl Name	
Town:		Conversite/line	Hyse Drs		Delete
anata -		ZammustiAare	Pear With:		Delate

Figure 4.44 – Management > SNMP > SNMP Community Table Settings

Key Type: Select the key type for the SNMP community. Select either Plain Text or Encrypted.

**Community Name:** Select 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:** Enter 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: Select the user's access rights from the drop-down menu:

**Read Only** - SNMP community members using the community string created can only read the contents of the MIBs on the Switch.

**Read Write** - SNMP community members using the community string created can read from, and write to the contents of the MIBs on the Switch.

IP Access-List Name: Enter the name of the standard access list to control the user to use this community

string to access to the SNMP agent.

Click Add to a new entry based on the information entered or **Delete** to remove the specified entry.

#### Management > SNMP > SNMP Group Table Settings

The SNMP Group page allows you to assign SNMP Users into SNMP Groups. SNMPv3 can control access and security policies on a per group basis.

0P Group Setting								
www.hate		(1 - e		. Fee	d view have	1.000	1	
list-based Decart	WMMH.	SMMP	6	990	v Vere Daries	Coloney .		
and delated		Balan	nden	Not	WWWTiate	TI CLER !		
PASSweb-Listia	ne i	U-T-m						
Another Calif.								400
obsi Corces : 5								400
	Read View N		Wetter View Harts	Roldy Uson Rame	Siccurfy Madel	SecurityLowe	P Address Lat News	401
ntar Extres : 5		ate .	With Vest Bates	Notify Union Houses	Security Madel	Second planet	IP Address Lat Name	Add Delete
olar Cornes : 5 Giorge Martin	Real Vew H	atta New	Welfar Views Ruesse	Weddy Verm Harred	Security Market	and the second se	# <sup>1</sup> Address List Name	
da taroes : 5 Gerginares gans	Real Veel H	atta New Tree	Wattle View Burns	Anothy Univer Maximu	et	Baldrafter.	P'Address Lat Norm	Deate
nta Corres : 5 Corregenses paint paint	Correction	arta Non	Welle Vew Hand	Auduly Value Massa Community/www	er. Ot	HARFS FOR	P Address Lat Norm	Delete

Figure 4.45 – Management > SNMP > SNMP Group Table Settings

Group Name: Enter the SNMP user group of up to 32 characters.

User-based Security Model: Select the SNMP security model.

**SNMPv1 -** SNMPv1 does not support any security features.

**SNMPv2c** - SNMPv2 supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.

**SNMPv3 -** SNMPv3 provides secure access to devices through a combination of authentication and encrypting packets over the network.

Security Level: This function is only available when you select SNMPv3 security level.

**NoAuthNoPriv** - No authorization and no encryption for packets sent between the Switch and SNMP manager.

AuthNoPriv - Authorization is required, but no encryption for packets sent between the Switch and SNMP manager.

**AuthPriv** – Both authorization and encryption are required for packets sent between the Switch and SNMP manger.

#### IP Address-List Name:

**Read View Name:** Enter a SNMP group name for users that are allowed SNMP read privileges to the Switch's SNMP agent.

Write View Name: Enter a SNMP group name for users that are allowed SNMP write privileges to the Switch's SNMP agent.

**Notify View Name:** Enter a SNMP group name for users that can receive SNMP trap messages generated by the Switch's SNMP agent.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove the specified entry.

#### Management > SNMP > SNMP Engine ID Local Settings

The Engine ID is a unique identifier used to identify the SNMPv3 engine on the Switch.

Input the Engine ID then click **Apply** to apply the changes or click **Default** to change back to the default value.

SVMP Englise ID Local Settings		
Eight D	8000081c044953	Default Acitiv
Fingers ID length is 34. The screption character is from 0 to F		

Figure 4.46 – Management > SNMP > SNMP Engine ID Local Settings

#### Management > SNMP > SNMP User Table Settings

The SNMP User Table Settings page allows you to maintain the SNMP user table for the use of SNMPv3. SNMPv3 allows or restricts users using the MIB OID, and encrypts the SNMP messages sent out between users and Switch.

and the Take Settings							
UserNave 1	10	nn -					
Genus Mana	111	1.6.0					
DHMP VALUE.	1		+				
SAMP VS Encoder	Ner	-					
Add Transitive Testover	(NO	4	•	Parametric (S-16 mont)	08	11	
Pro-Potenti în Parevent	- Dar		•	Patternet (1) 16 shared		11	
Audio-Produced by Filey	[isp	9		Hay D2 share		141	
File Protocal to Has	110			Here (32 charte)	E		
# Address-Cat Netwo	91	free .					
							Add
Tatal Estries : 1					a		
that Name Group!	1000	Saran By Manhail	Advantica	Distance Dynamics	Disgree D	F Add mo-Livi Name	
. 14541		+1-	7.00		#3000Ex#2300cu+a/1927500		Deteta

Figure 4.47 – Management > SNMP > SNMP User Table Settings

User Name: Enter a SNMP user name of up to 32 characters.

Group Name: Enter the SNMP group of the SNMP user.

SNMP Version: Select the SNMP version of the user. The options to choose are v1, v2c and v3.

**SNMP V3 Encryption:** When selecting **v3** in the **SNMP Version** drop-down list, this option is available. Options to choose from are **None**, **Password**, and **Key**.

**Auth-Protocol by Password:** Select either **MD5** or **SHA** to be the authentication protocol. Enter a password for SNMPv3 encryption in the right column.

**MD5** – Select to use the HMAC-MD5-96 authentication level. This field will require the user to enter a password.

**SHA** - Select that the HMAC-SHA authentication protocol will be used. This field will require the user to enter a password.

**Priv-Protocol by Password:** Select either **None** or **DES56** and then enter a password for SNMPv3 encryption in the right column.

None – Select to not use any authorization.

**DES56** – Select to use DES 56-bit encryption, based on the CBC-DES (DES-56) standard. This field will require you to enter a password.

Auth-Protocol by Key: Select either MD5 or SHA to be the authentication protocol. Enter a key for SNMPv3 encryption in the right column.

**MD5** – Select to use the HMAC-MD5-96 authentication level. This field will require the user to enter a key.

SHA – Select to use the HMAC-SHA authentication protocol. This field will require you to enter a key. **Priv-Protocol by Key:** Select either **None** or **DES56** and then enter a password for SNMPv3 encryption in the right column.

**None** – Select to not use any authorization.

**DES56** – Select to use DES 56-bit encryption, based on the CBC-DES (DES-56) standard. This field will require the user to enter a key.

**IP Address-List Name:** Enter the standard IP access control list (ACL) to associate with the user.

Click Add to create a new SNMP user account or click Delete to remove any existing data.

#### Management > SNMP > SNMP Host Table Settings

The SNMP Host Table Settings page allows you to configure the SNMP trap recipients.

BMP skast Settings				
e Hattifyi Addess				
Hout Pv6 Addresse				
permanent (privaly Model	SNAME			
incurte Level	Industriation -			
OP FUE (E-65535)	143			
	1117001			Add
promunity (Bring): (INMPs) (Ine Trans-	Contraction of the second s			
incompany Change (1999-1) like frame-				
	SMR <sup>1</sup> Versee	 UDP Part	Commanity Sining : Sillet V/1 (Just Rame	
ot ar Extrines : 2		UD# Pat	Cornelly Solids ( SIRPA1 Har Barra User menu, Tarli	Calata

Figure 4.48 – Management > SNMP > SNMP Host Table Settings

Host IPv4/IPv6 Address: Select IPv4 or IPv6 and specify the IP address of SNMP management host.

**User-based Security Model:** Specify the SNMP version to be used to the management host. The options are **SNMPv1**, **SNMPv2C** and **SNMPv3**.

Security Level: When selecting SNMPv3 in the User-based Security Model drop-down list, this option is available.

**NoAuthNoPriv** – Select to have no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.

**AuthNoPriv** – Select to require authorization, but with no encryption of packets sent between the Switch and a remote SNMP manager.

**AuthPriv** – Select to require authorization, and packets sent between the Switch and a remote SNMP manger will be encrypted.

**UDP Port (0-65535):** Enter the UDP port number. The default trap UDP port number is 162. The range of **UDP port numbers is from 0 to 65535. Some port numbers may conflict with other protocols.** 

Community String / SNMPv3 User Name: Enter the community string to be sent with the notification packet.

Click Add to create a new SNMP host, Delete to remove an existing host.

#### Management > RMON > RMON Global Settings

You can enable and disable remote monitoring (RMON) status for the SNMP function on the Switch. In addition, RMON Rising and Falling Alarm Traps can be enabled and disabled. Click **Apply** to save your settings.

MOR Glassal Sattlenge		
TIMON THIS IS A NOT THE	Contract of Document	
Recto Falling Marry Trap	() Evalued + Disasted	Apply

Figure 4.49 – Management > RMON > RMON Global Settings

#### Management > RMON > RMON Statistics Settings

The RMON Statistics Settings page displays RMON Ethernet Statistics and allows you to configure the settings.

BROM STREETS	Samage						
Page -		100400 (T-210530).*		Owner			
eth1/0/1 +	<	1					Add
Sector Sector	Field		Trans.				_
	1011010	(	Dones, Tostt		 Delvite	Show Detail	
I WHERE I	UPO DITE:		Instant, Total		Delete 1	Show Detail	

Figure 4.50 – Management > RMON > RMON Statistics Settings

The RMON Ethernet Statistics Configuration contains the following fields:

Port: Select the port from which the RMON information was taken.

Index (1 - 65535): Indicates the RMON Ethernet Statistics entry number.

**Owner:** Displays the RMON station or user that requested the RMON information.

Click Add to activate your entry or click to renew the details collected and displayed.

#### Management > RMON > RMON History Settings

The RMON History Settings page contains information about samples of data taken from ports. For example, the samples may include interface definitions or polling periods.

CH HILIYY	Tellings						
wi*		Index (1-83235).*	Buckets Nav	rber (1-58)	Internal (1-3000 units)	Owner	
eth1/0/1		22	40		1883		
	1000				the second se		
			the clubber				Appile
	Field	Backets Respected	Harbett fa artest	Edulud	Owner		Appile
-	_			Rentand Table		Delete	Apple

Figure 4.51 – Management > RMON > RMON History Settings

The History Control Configuration contains the following fields:

Port: Select the port from which the RMON information was taken.

Index (1 - 65535): Indicates the history control entry number.

Buckets Requested (1 ~ 50): Enter the number of buckets that the device saves.

**Interval (1** ~ **3600 secs):** Indicates in seconds the time period that samplings are taken from the ports. The field range is *1-3600*. The default is *1800* seconds (equal to 30 minutes).

**Owner:** Displays the RMON station or user that requested the RMON information.

Click **Apply** to activate your entry.

#### Management > RMON > RMON Alarm Settings

The RMON Alarm Settings page allows you to configure the network alarms. Network alarms occur when a network problem or event is detected.

NON.	Al June	Seltings									
NUMBER OF STREET	anna Sant	ings -									
	i Demoka	a (p-249-1) Ma (r-49512)					14-1 aucces) and (9-2*34-4) augus (1-445634)	Absolut	e value		Acoly
Teta En	nies:2										
		Verteiler	her	Last Value	Hong Territeld	Failing) Threadacht	Hung fund	Falling Frend Ma	Slate Auro	Course .	
	100	556121222397	Aug.m.du		2000				.mangar Falma		Delete
***12	200	928121221383	401111	- 18	993	- 100	- F.	.0	Runger Falling		Deleta
									900 1000		internet in the

Figure 4.52 – Management > RMON > RMON Alarm Settings

The configuration contains the following fields:

Index (1 - 65535): Enter a specific alarm.

Variable: Select the selected MIB variable value.

**Rising Threshold (0 ~ 2^31-1):** Displays the rising counter value that triggers the rising threshold alarm.

**Rising Event Index (1**  $\sim$  65535): Displays the event that triggers the specific alarm. The possible field values are user defined RMON events.

**Owner:** Displays the device or user that defined the alarm.

Interval (1 ~ 2^31-1): Defines the alarm interval time in seconds.

**Sample type:** Defines the sampling method for the selected variable and comparing the value against the thresholds. The possible field values are:

**Delta value** – Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.

Absolute value - Compares the values directly with the thresholds at the end of the sampling interval.

Falling Threshold (0 ~ 2^31-1): Displays the falling counter value that triggers the falling threshold alarm.

Falling Event Index (1 ~ 65535): Displays the event that triggers the specific alarm. The possible field values are user defined RMON events.

Click Apply to activate your alarm entry.

### Management > RMON > RMON Event Settings

The RMON Event Settings page contains fields for defining, modifying and viewing RMON event statistics.

STORES	ana seranga					_	_
FOR COLUMN	Settings						
-mana (1-6)	otexa		1				
Description							
Description Type		Nens	•				
Corrected	6						
Corverant Owner							
							AM
Tetal Dette							
Sec.	Description	Centrality	Event Treasure	Owine	Last Titger taxe		
1.4	Descoutes_Tell1	10.04		Owner Taxett	0-days 000x EDec (8da	Delete	Vere Logi
81126	Detroistine_Text)	Leg		Demonster Texati	O days the thrubbe	Coleta	Wew Loos

Figure 4.53 – Management > RMON > RMON Event Settings

The RMON Events Page contains the following fields:

Index (1~ 65535): Enter the event index.

Description: Enter an event description.

**Type:** Select the event type. The possible values are:

None – Indicates that no event occurred.

**Log** – Indicates that the event is a log entry.

**SNMP Trap** – Indicates that the event is a trap.

Log and Trap – Indicates that the event is both a log entry and a trap.

**Community:** Enter the community to which the event belongs.

**Owner:** Enter the time that the event occurred.

Click Add to add a new RMON event.

#### Management > Telnet/Web

The Telnet/Web page allows you to configure Telnet and Web settings on the Switch.

TeinebWeb Teinet Rettings		
Tvitret Date Fon ci 60000	in Enabled	Apply
Wein Settings		
Web Diale Port in -emilials	n Enisted C Dreatest	Apply

Figure 4.54 – Management > Telnet/Web

#### **Telnet Settings:**

**Telnet State:** Select to enable or disable the configuration through Telnet.

**Port (1-65535):** Enter the TCP port number used for Telnet management of the Switch. The "well-known" TCP port for the Telnet protocol is 23.

Click **Apply** to save your settings.

#### Web Settings:

Web State: Select to enable or disable Web-based configuration.

**Port (1-65535):** Enter the TCP port number used for Telnet management of the Switch. The "well-known" TCP port for the Telnet protocol is 80.

Click the **Apply** button to save your settings.

### Management > Session Timeout

The Session Timeout page allows you to configure the session timeout on the Switch.

Session Timeout				
Seculte Tenedat				
Web Serieum Timscod (59-38080)	100	- fam	Devoit (	
Twent Second Tenool (0 1478)	50	100	iet Dortault	Apply

Figure 4.55 – Management > Session Timeout

Web Session Timeout (60-36000): Enter the time in seconds of the web session timeout. Tick the Default check box.

**Telnet Session Timeout (0-1439):** Enter the time in minutes of the Telnet session timeout. Tick the **Default** check box to return to the default setting. The value is from 0 to 1439 minutes. 0 means never timeout. The default value is 3 minutes.

Click the **Apply** button to save your settings.

# Management > D-Link Discover Protocol Settings

The D-Link Discover Protocol Settings page allows you to configure and display D-Link Discovery Protocol (DDP).

D Link Discovery Protocol DDP Gislan Settings				
D-Less Discovery Protocol State	· English			
Report Timer	Herer	• 3.000		Apply
00P Part Settings				
Frenchet etht/01-	Tarton	eth/16/1 •	Bahar Ersebiet •	Apply
Patt			Status.	_
-401.081			. Enabled	
- MYTERS			- England	
			Enabled	
100103			( Distant	
entrois.			Enabled	
entries			(Instant	
			Deadlood	
			Engine	
etri99			Rhatsert	
#8110718			Distant	
			Destant	
ani/ortz			- thereit	

Figure 4.56 – Management > D-Link Discover Protocol Settings

D-Link Discovery Protocol State: Enter the enable or disable the D-Link Discovery Protocol state.

**Report Timer:** Specify the interval in seconds between two consecutive DDP report messages. Options to choose from are **30**, **60**, **90**,**120**, and **Never**.

### **DDP Port Settings:**

**From Port** / **To Port:** Enter the appropriate port range used for the configuration. **State:** Select to enable or disable the DDP port state.

Click the Apply button to save your settings.

### L2 Features > FDB > Static FDB > Unicast Static FDB

The Unicast Static FDB page allows you to view and configure the static unicast forwarding settings on the Switch.

Neuerl Statts 100			
Past • attribut •	VID-0-4946	MAC ADDVIS (19. 14 19. 19. 1	Apply
Total Entrine : 2			Delate All
WI.	BAC AARONE	Even /	and the second se
	0.0000000000000000	48.105	Delate
- K	65-65-95-88-95-83	481537	Deate

Figure 4.57 – L2 Features > FDB > Static FDB > Unicast Static FDB

**Port** / **Drop:** Allows the selection of the port number on which the MAC address entered resides. This option could also drop the MAC address from the unicast static FDB. When selecting **Port**, select the switch unit and port number.

VID (1-4094): Enter the VLAN ID on which the associated unicast MAC address resides.

**MAC Address:** Enter the MAC address to which packets will be statically forwarded or dropped. This must be a unicast MAC address.

Click the **Apply** button to save your settings or click the **Delete All** button to delete all the entries found in the display table.

Enter a page number and click the Go button to navigate to a specific page when multiple pages exist.

### L2 Features > FDB > Static FDB > Multicast Static FDB

The Multicast Static FDB page allows you to view and configure the static multicast forwarding settings on the Switch.

fullicast Static	non					
Fight Furt		To Field	VID (1-40H)	MAC Address		
eth18/1	•	#85.5X1 *		01-05-08-03-03-02-02		Appin
Intal Entries 13						Celeta Al
1	1000	100	C Address	Egrave Polls		
	1	31.85	48.83.86 M	ann robit ann 100mg	54	ety.
	9.0	07-00	00-00-00-41	with:53/WS-with(1/018	De	ete .
					111	1

Figure 4.58 – L2 Features > FDB > Static FDB > Multicast Static FDB

From Port / To Port: Enter the appropriate port range used for the configuration.

VID (1-4094): Enter the VLAN ID of the VLAN the corresponding MAC address belongs to.

**MAC Address:** Enter the static destination MAC address of the multicast packets. This must be a multicast MAC address. The format of the destination MAC address is 01-XX-XX-XX-XX.

Click the **Apply** button to save your settings. And click the **Delete All** button to remove all the entries. Click the **Delete** button to remove the specific entry.

Enter a page number and click the Go button to navigate to a specific page when multiple pages exist.

#### L2 Features > FDB > MAC Address Table Settings

The **MAC Address Table Settings** page allows you to view and configure the MAC address table's global settings.

AAC ADDINES TEDIE Setting			
Global Setting	MAC Address Loursing		
Aprily Time (8, 10-1000008)	200	last.	
Aging Certification Hit	Evaluat + D		Apprix

Figure 4.59 – L2 Features > FDB > MAC Address Table Settings – Global Setting

**Aging Time:** Enter the MAC address table's aging time value. This value must be between 10 and 1000000 seconds. Entering 0 will disable MAC address aging. By default, this value is 300 seconds. **Aging Destination Hit:** Select to enable or disable the aging destination hit function.

Click the **Apply** button to save your settings.

After clicking the MAC Address Learning tab, the following page will appear.

<b>Globul Setting</b>	MAC Address Louising	
(enthick	To Piet Uses	
est/01. •	ettiliter +	Apply
_	Port	Marin
	481.07	Enabled
	481.002	tranker 1
	C0184	Evabled
	VEEDA	Desking
	#8105	Enables
	48508	English
	707/198	Enabled
	48.000	Evaluation .
	48.150	Erabiet
	danarie .	Enablight
	48:0011	Erakee
	wei-18/2	Instead

Figure 4.60 - L2 Features > FDB > MAC Address Table Settings - MAC Address Learning

**From Port** / **To Port:** Enter the range of ports that will be used for this configuration. **State:** Select to enable or disable the MAC address learning function on the specified ports.

Click the **Apply** button to save your settings.

#### L2 Features > FDB > MAC Address Table

The MAC Address Table page allows you to view the entries listed in the MAC address table.

AC Address Table				_	
MAC Robbies Table					
Port	[ath(10/1 • )	1	Clear Baturnic by Port	Find	
VID-01-40140		9	Dear Dynamic by VLAN	Red	
MAC ADDISS	The dia set out its dia.	98	Clear Dyname by NAC	Find	
Total Entries : 3			Cear M	View All	
	NAC Address	Ture .		97	
2 <b>*</b>	100-00-00-00-00-00	10.001	(8)	entor:	
1 II	85-00-03-00-35-A7	3141	48.5		
	- 85 CD-85 CD-05 A4	Oynames	171	0001	

Figure 4.61 – L2 Features > FDB > MAC Address Table

Port: Select the port that will be used for this configuration.

VID (1-4094): Enter the VLAN ID that will be used for this configuration.

MAC Address: Enter the MAC address that will be used for this configuration

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear Dynamic by Port** button to clear the dynamic MAC address listed on the corresponding port. Click the **Clear Dynamic by VLAN** button to clear the dynamic MAC address listed on the corresponding VLAN.

Click the Clear Dynamic by MAC button to clear the dynamic MAC address entered.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Clear All** button to clear all dynamic MAC addresses.

Click the View All button to display all the MAC addresses recorded in the MAC address table.

#### L2 Features > 802.1Q VLAN

The 802.1Q VLAN page allows you to view and configure the VLAN settings on this switch.

BOS TO VEAR	-				
882.10 YLAH					
VID Link	1023				Apply Deteta
Tierd Vol. AM					
90.04090		1			Find View All
Telal Entries /	t.				
180	VEAN Barrer	Enggera Mercatare Party-	Unitagged Statement Ports	VEAR THREE	for any second s
1.1	diftant.		em1005-em15012		THE DATE OF

Figure 4.62 – L2 Features > 802.1Q VLAN

### 802.1Q VLAN:

**VID List:** Enter the VLAN ID list that will be created. Click the **Apply** button to save your settings. Click the **Delete** button to remove the specific entry.

#### Find VLAN:

**VID (1-4094):** Enter the VLAN ID to be displayed. Click the **Find** button to locate a specific entry based on the information entered. Click the **View All** button to locate all the entries.

Click the **Edit** button to re-configure the specific entry.

Enter a page number and click the Go button to navigate to a specific page when multiple pages exist.

### L2 Features > Asymmetric VLAN

The Asymmetric VLAN page allows you to configure the asymmetric VLAN function on this switch.

Asymmetric VLAH Asymmetric VLAH		
Anymmettic VLAN State	🗇 Evaluet + Disatine	Apple

Figure 4.63 – L2 Features > Asymmetric VLAN

**Asymmetric VLAN State:** Select to enable or disable the Asymmetric VLAN function. Click the **Apply** button to save your settings.

### L2 Features > VLAN Interface

The VLAN Interface page allows you to view and configure the VLAN interface settings on this switch.

Interface -					
Part	TALANI Multir	Ingross Classes	Acceptable frame Type		
1011021	Hybrid	England	Autor) Mi	Van Detail	18.
#11103	Holand	E144Emel	Appendix A.E	Wan Datal	Edd
eti 195	Altest	Enided	Amethi	Vian Dytail	Diff.
HIIITH.	ALLER.	ENERG	Activities	Var Detail	Ede.
#1105	Hotel	Ensteine	ArtistAt	Vien Owneil	517
stitte.	Pytoni	Ernitine	Amerida	Vian Detail	Edit
YOUNH	Hybrid	Enter	Autorid All	Man Detail	EDE
akriste 🗌	Hybrid	Dright Bud	AutoritAt	Viac Detail	Edg
etinas	ingent	Evited	AstronAst	vian perail	Hat
0193870	HY400	Ender	ArmetAl	Wan Detail	Edd.
010011	412415	Fraking	Armonike	vian Detail	ER
entrol (	AATTS .	Ensted	Autorit Ad	Van Detai	E.dx

Figure 4.64 – L2 Features > VLAN Interface

**Unit:** Select the switch unit that will be used for this configuration.

Click the **VLAN Detail** button to view more detailed information about the VLAN on the specific interface. Click the **Edit** button to re-configure the specific entry.

All Infortion Information		
Hur.	apprixity	
CAN MILLION	hesese	
Victory Victory	1	
Harris Chevrola	Disater .	
NUMBER Prants Type	Autorit Add	

After clicking the VLAN Detail button, the following page will appear:

Figure 4.65 – L2 Features > VLAN Interface – VLAN Detail

After clicking the **Edit** button, the following window will appear. This is a dynamic window that will change when a different **VLAN Mode** is selected. When **Access** was selected as the **VLAN Mode**, the following page will appear.

anfigura VLNI kesetace		
toe.	49(10)1	
KARINGR	Access *	
Acceptable Frank Type	Admit Al .	
Hamos Checking	C Evaluent (E Crossiend	
4D-(1-40M0		
		Back Appl

Figure 4.66 – L2 Features > VLAN Interface – VLAN Detail

**Port:** Display the VLAN port number.

VLAN Mode: Select the VLAN mode option. Options to choose from are Access, Hybrid, and Trunk.

Acceptable Frame Type: Select the acceptable frame type behavior option. Options to choose from are Tagged Only, Untagged Only, and Admit All.

**Ingress Checking:** Select to enable or disable the ingress checking function.

VID (1-4094): Enter the VLAN ID used for this configuration. This value must be between 1 and 4094.

Click the **Apply** button to save your settings.

Click the **Back** button to return to the previous page.

### L2 Features > STP > STP Global Settings

The Switch implements three versions of the Spanning Tree Protocol, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1w specification, a version compatible with the IEEE 802.1D STP and the Multiple Spanning Tree Protocol (MSTP) as defined by the IEEE802.1 specification. 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. 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.

The IEEE 802.1 Multiple Spanning Tree (MSTP) provides various load balancing scenarios by allowing multiple VLANs to be mapped to a single spanning tree instance, providing multiple pathways across the network. For example, while port A is blocked in one STP instance, the same port can be placed in the Forwarding state in another STP instance.

By default, Rapid Spanning Tree is disabled. If enabled, the Switch will listen for BPDU packets and its accompanying Hello packet. BPDU packets are sent even if a BPDU 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.

By default Multiple Spanning Tree is enabled. It will tag BPDU packets to receiving devices and distinguish spanning tree instances, spanning tree regions and the VLANs associated with them.

After enabling STP, configure the STP Global Settings. (shown below)

STP Clobal Seminge	_	_	_				
839 State							
UTP-Dates	- Date:	÷ Disabat					Acch
STP Traps							
STP New Root Trap STP Teachage Charge Trap		e Doated					Apple
STP Made							
61P Mode	MSTP						Apph
Stitheoly							
Priority (0-81 840)	32768						Apply
101P Configuration							
Dricya MacAge (5-40)	20 15 2		(account)	Delago Holia Tana (1-2)	2	940	
Dridge Forward Time (#-30)	15		344	TO Hold Court (1-10)	в	Banes.	
MacHons (1-40)	2		besei				Apple

Figure 4.67 – L2 Features > STP > STP Global Settings

**STP State:** Select the Spanning Tree Protocol to be enabled or disabled. Click the **Apply** button to save your settings.

### STP Traps:

**STP New Root Trap:** Select to enable or disable the STP new root trap option.

**STP Topology Change Trap:** Select to enable or disable the STP topology change trap option. Click the **Apply** button to save your settings.

**STP Mode:** Select the STP mode. The options to choose from are MSTP, RSTP and STP. Click the **Apply** button to save your settings.

### **STP Priority:**

**STP (0-61440):** Enter the STP priority value. This value is between 0 and 61440. By default, this value is 32768. The lower the value, the higher the priority.

Click the **Apply** button to save your settings.

### STP Configuration:

**Bridge Max Age (6-40):** Enter the bridge's maximum age value here. This value must be between 6 and 40 seconds. By default, this value is 20 seconds. The maximum age value 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.

**Bridge Forward Time (4-30):** Enter the bridge's forwarding time value. This value must be between 4 and 30 seconds. By default, this value is 15 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 (1-40):** Enter the maximum number of hops that are allowed. This value must be between 1 and 40 hops. By default, this value is 20 hops. This value is 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 BDPU packet and the information held for the port will age out.

**Bridge Hello Time (0-2):** After selecting **RSTP/STP** as the **STP Mode**, this parameter will be available. Enter the bridge's hello time value here. This value must be between 1 and 2 seconds. By default, this value is 2 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.

**TX Hop Count (1-10):** Enter the transmit hold count value. This value must be between 1 and 10 times. By default, this value is 6 times. This value is used to set the maximum number of Hello packets transmitted per interval.

Click the **Apply** button to save your settings.

### L2 Features > STP > STP Port Settings

STP can be set up on a port per port basis. 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 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.

P Part Sattes											
10.000											
Hees Part		eth.1.671	1.	Taber.	ethi						
Contin-2		0		Sinte .	End	in the	COMMER	ket 17	Dead	Med : .	*
Live Type		Adu		Patriani	Tigty	* #	TON FIL		Dist	bled .	
IPDU Purvan	1	Deatled	•	Preve	CH	•	PAULT TO	10 D W	1		1281
			-		100						Appliv
					_						T. Al-As
E Stat	A SUMP	Cont	Sard Red	STATES OF THE OWNER	ac i	Alteri Passi	<b>EXAPRO</b>	HERE FO	10.01	Description	HINE STOL
#81.00	Erstähne	eronanna.	(tin ainia it	Availab	Ares	AdditionE	friendsing : :	(Disa)	84	120	-1-
17100	TIMET	ACTORNES .	Doartes.	4(8,07)	1111	Antesa	Doorsend.	Otiat	44	121	1
2215/	Builden	242000303	Dourse	Autoritie	ALC: N	Adatasi E.	Dustried	Diat	84	101	10
12154	COMPLEX.	- FILLER	Dearer	443-424		ABRIDE	[] Distances []	0144	44	128	12
201/58	Distant	8410000	Dasied	Actuality	200	ABUND-5	Detected	Disa	84	128	3
yanna :	TYNAM	1010000	Dyaned.	453000	init??	ADMINE	Siddows :	Driat	¥6	1000	1237
49157	Ender	-02000	Doutest.	Aug. 121	wee:	Addition	(Distant)	Cent	11	136	3
eriles .	Courses of	NUTRING .	Treased.	Ava-		Antesd.	(Deater))	DHOD	44	128	1.20
101.61	Dutter	ALLERANS	Doubled.	ALM/TO	inter.	Autoritant	(Dopind)	Dejug	nd.	.128	2
ettiliili	Distant	RECORDER OF	Dourse.	ALS	ALC: NO	April 1	Dagood	Dear		326	1.3
WEIRITE	- Erstellent	NOTESEE	Disaved	A,bith	494	Assisted	Drugsmit	Uscan	45	7.26	
##110312	Transa .	POR BAR	Distantian.	Palation	area .	Andrea	Disalited 1	Diam		156	000312

Figure 4.68 – L2 Features > STP > STP Port Settings

From Port/To Port: Enter a consecutive group of ports to be configured starting with the selected port.

**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).

**0 (auto)** - 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.

**Value 1-200000000 -** 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.

**State:** Select to enable or disable STP by per-port based. It will be selectable after the global STP is enabled. **Guard Root:** Select to enable or disable the guard root function.

Link Type: Select the link type option. The options to choose from are Auto, P2P, and Shared. A full-duplex port is considered to have a point-to-point (P2P) connection. On the opposite, a half-duplex port is

considered to have a **Shared** connection .The port cannot transit into the forwarding state rapidly by setting the link type to **Shared**. By default this option is **Auto**.

**Port Fast:** Select the port fast option. The options to choose from are **Network**, **Disabled**, and **Edge**. In the **Network** mode the port will remain in the non-port-fast state for three seconds. The port will change to the port-fast state if no BPDU is received and changes to the forwarding state. If the port received the BPDU later, it will change to the non-port-fast state. In the **Disable** mode, the port will always be in the non-port-fast state. It will always wait for the forward-time delay to change to the forwarding state. In the **Edge** mode, the port will directly change to the spanning-tree forwarding state when a link-up occurs without waiting for the forward-time delay. If the interface receives a BPDU later, its operation state changes to the non-port-fast state. By default, this option is **Network**.

**TCN Filter:** Select to enable or disable the TCN filter option. Enabling TC filtering on a port is useful for an ISP to prevent the external bridge to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator. When a port is set to the TCN filter mode, the TC event received by the port will be ignored. By default, this option is disabled.

**BPDU Forward:** Bridges use Bridge Protocol Data Units (BPDU) to provide spanning tree information. STP BPDUs filtering is useful when a bridge interconnects two regions; each region needing a separate spanning tree. BPDU filtering functions only when STP is disabled either globally or on a single interface. The possible field values are:

**Disabled** – BPDU filtering is enabled on the port.

Enabled - BPDU forwarding is enabled on the port (if STP is disabled).

**Priority:** Select the priority of each port. Selectable range is from 0 to 240, and the default setting is 128. The lower the number, the greater the probability the port will be chosen as a root port.

**Hello Time:** The interval between two transmissions of BPDU packets sent by the Root Bridge to indicate to all other switches that it is indeed the Root Bridge. The default value is 2.

Click **Apply** button to save your settings.

#### <u>L2 Features > STP > MST Configuration Identification</u>

Multiple Spanning Tree (MSTP) provides various load balancing scenarios by allowing multiple VLANs to be mapped to a single spanning tree instance, providing multiple pathways across the network. For example, while port A is blocked in one STP instance, the same port can be placed in the Forwarding state in another STP instance.

The MST Configuration Identification page is for defining global MSTP settings, including region names, MSTP revision level.

fill Configuration MemoRication		
Configuration Name	IEEO 44/FT 35 79	
Revision Level (0-45525)	0	
Digasi	000000000000000000000000000000000000000	Apple
where to Settings		
Noteron ID (2-16)	[]	
Aidori	Add VID .	
Alton VID List	Amage .	Apply
Tolai Entres : 1		
bittance ID	VLML100	
CHER	Y-#33#	6.00 ( Seator )

Figure 4.69 – L2 Features > STP > MST Configuration Identification

### **MST Configuration Identification:**

**Configuration Name:** Enter a name set on the switch to uniquely identify the MSTI (multiple spanning tree instance). If a configuration name is not set, this field shows the MAC address of the device running MSTP.

**Revision Level(0 - 65535):** This value, together with the configuration name and identical VLANs mapped for STP instance IDs identifies the MST region configured on the switch.

Click **Apply** to define the configuration name and revision level.

# **Instance ID Settings:**

**Instance ID (1 - 64):** Enter the MSTI ID associated with the VID List. The possible field range is 1-64. **Action:** The possible values are:

Add VID - Indicates that the edit type is add.

**Remove VID -** Indicates that the edit type is removed.

**VID List:** Enter the VID range from configured VLANs set on the Switch.

Click **Apply** button to save your settings.

Click Edit to modify the setting of VID or click Delete to remove it.

# L2 Features > STP > STP Instance

The STP Instance Settings page display MSTIs currently set on the Switch and allows users to change the Priority of the MSTPs.

Without 1			
Belleven.	Instance State	keetanca Provity	
CHET	Epitead Anti	3,2764	ER.
		Austance C	mawbord.
	Brass Agrees	10+045	11-22-110
	100 State of the residence of the	A4 10 30 1	0100-00-00-0
Deng	DERTFORTATIONS (PERMI)	00-68-00-6	
	n die Charl Address (Provin Maai Deropa Address (Provin	A1 10-03 0	

Figure 4.70 – L2 Features > STP > STP Instance

Click the **Edit** button to re-configure the specific entry.

# L2 Features > STP > MSTP Port Information

The MSTP Port Information page allows you to configure the MSTP Interface settings.

Photodos					
e att10/1	•			Ciner Deta	ected Protocol Find
es 50-1 Settings					
	Cast	Printy	States .	Res	

Figure 4.71 – L2 Features > STP > MSTP Port Information

**Port:** Enter the port to find.

Click the **Clear Detected Protocol** button to clear the detected protocol settings for the port selected. Click **Find** to search the MSTP port information.

Click the **Edit** button to re-configure the specific entry.

### L2 Features > Loopback Detection

The Loopback Detection function is used to detect the loop created by a specific port while Spanning Tree Protocol (STP) is not enabled in the network, especially when the down links are hubs or unmanaged switches. The Switch will automatically shutdown the port and sends a log to the administrator. The Loopback Detection port will be unlocked when the Loopback Detection **Recover Time** times out. The Loopback Detection function can be implemented on a range of ports at a time. You may enable or disable this function using the pull-down menu.

mathack Detection Galax Settle					
Longeback Datastron State	(Desident +)			Port-based +	ĺ.
Example VL/H (D)Ltd	10	100	enal (3-32767)	2	]
Trae Dista	Disabled •		tori	Sha-down •	Appin
ingelants Detection Part Setting					
FremFint	TIPH.	28 da 1			
* 100.6%	eth16712 *	Deabled			Acuthy
Plat	Langers (	AND IN THE	_	NAME OF TAXABLE	Time Laff (seec)
eth1031	Da	stied		Hatta	1
20106	DA	0.0101		Marriel	
.atr1023	-Da	ative		Manual -	
401104	10	49-9-1		Horner .	
ue109	20	ating .		Mitrial	1
0811020		49.94		tigene	
sets1027	Da	40.01		Harry	
ait1001	De	10.01		Harnel	1
-00109	Du	apping and a		Notial	
#91/\$118	: (Da	all		Hornal	1
10101	De	striet.		norral	1
		APRIL 1		Manager and Control of	

Figure 4.72 – L2 Features > Loopback Detection Settings

Loopback Detection State: Enable or disable loopback detection. The default is disabled.

Mode: Select either Port-based or VLAN-based.

**Enabled VLAN ID List:** Enter the VLAN ID for loop detection. This only takes effect when the **VLAN-based** is selected in the **Mode** drop-down list.

Interval (1-32767): Set a Loop Detection Interval between 1 and 32767 seconds. The default is 2 seconds.

Trap State: Select to enable or disable the loopback detection trap state.

Action: Select Shut-down or None for the loopback detection.

**From Port** / **To Port:** Enter a consecutive group of ports to be configured starting with the selected port. **State:** Use the drop-down menu to toggle between *Enabled* and *Disabled*. Default is *disabled*. Click **Apply** to save your settings.

### L2 Features > Link Aggregation

The Link Aggregation page allows you to view and configure the link aggregation settings.

(eners Pearly (1-80)	1260	12768			
cold Dataset Agenth		Source MAC			
(vren D		10788,85-65-44-77-9	5.79		Apply
havened Carring Reference	-				
Dam Fint	To Post	Orner D			
41110/1 *	(081/071	•	On		Add Delete Hember Par
arkit, G/1 •	(001/07)	THE REAL PROPERTY AND INCOMENTATION OF A DESCRIPTION OF A			Add 1 Delete Hender Par
the second s	(001/07)	THE REAL PROPERTY AND INCOMENTATION OF A DESCRIPTION OF A			Add Collector Nember Par
Harter Sach Chartoni (	(001/07)	THE REAL PROPERTY AND INCOMENTATION OF A DESCRIPTION OF A			Add Dalata Hender Par
Neter Earl Charnel ( Neter Getries : 2	(etit.01 Pola naontriat	a Directorian parts	On		Sector Care
Hadas: Elacti Channel I Natal Galaine : 2 Colonial Galaine	(eth)/01 Proce maximiti ce f	Harbets	Directory Network	E Restor fueto	Sector Care

Figure 4.73 – L2 Features > Link Aggregation

**System Priority (1-65535):** Enter the system's priority value you want to use. This value must be between 1 and 65535. By default, this value is 32768. The system priority determines which ports can join a port-channel and which ports are put in the stand-alone mode. The lower value has a higher priority. If two or more ports have the same priority, the port number determines the priority

Load Balance Algorithm: Specify the load balancing algorithm that will be used. Options to choose from are Source MAC, Destination MAC, Source Destination MAC, Source IP, Destination IP, and Source

**Destination IP**. By default, this option is **Source MAC**. **System ID:** The **System ID** information.

Click the **Apply** button to save your settings.

# Channel Group Information:

From Port / To Port: Select the appropriate port range used for the configuration.

**Group ID:** Enter the channel group number. This value must be between 1 and 32. The system will automatically create the port-channel when a physical port first joins a channel group. An interface can only join one channel-group.

**Mode:** Select either **On**, **Active**, or **Passive**. If you selected **On**, the channel group type is static. If **Active** or **Passive** is selected, the channel group type is LACP. A channel group can only consist of either static members or LACP members. Once the type of channel group has been determined, other types of interfaces cannot join the channel group.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete Member Port** button to remove the specific member port.

Click the **Delete Channel** button to remove the specific entry.

Click the **Channel Detail** button to view more detailed information about the channel.

# L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings

With Internet Group Management Protocol (IGMP) snooping, the DXS-1210 Series Switch can make intelligent multicast forwarding decisions by examining the contents of each frame's Layer 2 MAC header.

IGMP snooping can help reduce cluttered traffic on the LAN. With IGMP snooping enabled globally, the DXS-1210 Series Switch will forward multicast traffic only to connections that have group members attached. The settings of IGMP snooping is set by each VLAN individually.

IMP Snooping Settings	_			
Global Settings				
Occura their		() Evene * Divated		Apply
A AM Watan Settings				
MD (1-4994) [		U Dreated		Apple
20P Security Table				
10 (1-4096 [				Find Print M
Textual Contralment: IN				
100		10 AM Marrie	Scalar.	
1.0		arbot .	Distances	lihow Detail 691

Figure 4.74 – L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings

# Global Settings:

**Global State:** Select to enable or disable the IGMP Snooping global state. Click the **Apply** button to save your settings.

# VLAN Status Settings:

**VID (1-4094):** Enter the VLAN ID and select to enable or disable the IGMP snooping on the VLAN. Click the **Apply** button to save your settings.

# IGMP Snooping Table:

VID (1-4094): Enter the VLAN ID between 1 and 4094.

Click the **Find** button to display a specific entry based on the information entered.

Click the **Find All** button to display all the entries.

Click the **Show Detail** button to display the detail information of the specified VLAN.

Click the **Edit** button to re-configure the specific entry.

Enter a page number and click the Go button to navigate to a specific page when multiple pages exist.

After clicking the Show Detail button, the following window will appear:

MP Sasoping VLAH Paramatara VID Status	1 Densitied
FactLeove Guerter State	Disabled
Guevy Version	43
Gruery Interval	125 seconds
Max Response Tene Risbustness Value	10 sacondo 2
Last Merriser Duery Warval	2 seconds
	Modify

Figure 4.75 – L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping – Show Detail Click the **Modify** button to edit the information in the following window:

Guary Interval (1-31744)     125     146       Max Response Term (5-21)     10     546       Modulmanic Visitar (5-21)     12     546       Last Member Quary Interval (5-21)     12     546	VIC (1-4084) Blakes Fast Loove Gearler Blake Gearly Version	Constant and	Dualses Deables Deables	
Probustmence Value (7-7) [2 ]	Geory Interval (1-31744)	125	886	
	Mail Response Time (3-25)	(10)	884.	
	Hobumens Value (1-7)	1		
Apply	Last Member Query Interval (1-25)	2	141	
			1	Δρρίγ

Figure 4.76 L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping – Modify

#### The following parameters can be configured:

Fast Leave: Select to enable or disable the IGMP snooping fast leave function.

Querier State: Select to enable or disable the querier state.

Query Version: Select the general query packet version sent by the IGMP snooping querier.

**Query Interval (1-31744):** Enter the interval at which the IGMP snooping querier sends IGMP general query messages periodically.

Max. Response Time (1-25): Enter the maximum response time. The range is between 1 and 25 seconds.

Robustness Value (1-7): Enter the robustness variable used in IGMP snooping.

Last Member Query Interval (1-25): Enter the interval at which the IGMP snooping querier sends IGMP group-specific or group-source-specific query messages.

Click the **Apply** button to save your settings.

### L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Groups Settings

The IGMP snooping Groups Settings page allows you to configure and view the IGMP snooping static group, and view IGMP snooping group.

VID (1-4094)	Oroug Address	Provi Pat	Turter (eh101 •	Apply Dalate
VD 0-47941	Group Address.			Pend Pend all
Tutal Entries ( 2				
1.M		Excep Antrees		Parte
1 P.		man		101103
		2343.8.5		x81/6/2
				11 64
139 <sup>2</sup> Second Groups Tabl				
MD (1-4094) = [	Group Address			Find Rid M
Tatal Entries 18				
UP UP	forme Ammens	Searce Address	Eqasel1	Patra
the stress of the second		_ + = Tarter	ANALY CONTRACTOR	

Figure 4.77 – L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Group Settings

VID (1-4094): Enter the VLAN ID.

Group Address: Enter the IP multicast group address.

From Port / To Port: Select the range of ports to be configured.

Click the **Apply** button to save your settings.

Click the **Delete** button to remove the specified entry.

Click the **Find** button to locate a specific entry based on the information entered.

Click the Find All button to view all the entries.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

The fields that can be configured for **IGMP Snooping Groups Table** are described below:

### IGMP Snooping Group Table:

VID (1-4094): Specify the VLAN ID.

Group Address: Click the radio button and enter an IP multicast group address.

Click the **Find** button to locate a specific entry based on the information entered. Click the **Find All** button to view all the entries.

### L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Mrouter Settings

The IGMP Snooping Mrouter Settings page allows you to configure the specified interface(s) as the multicast router ports or as forbidden to be multicast router ports on the Switch.

W? Sanayang Minuts	a Safaraya			
(A014-010)	Contiguestor	From Part	Tarfort	
	Purt	ath10/1 *	#81.0/1 *	Apply Delete
(D. (s-wijsk)		( and the second		Find Produet
ito (s-wiski) [	e Table			Find Find at
0 (s-week [	e Table		Parts :	Find

Figure 4.78 – L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Mrouter Settings

VID (1-4094): Enter the VLAN ID and the range is between 1 and 4094.

**Configuration:** Select the port configuration type.

Port: Select to have the configured ports to be static multicast router ports.

**Forbidden Port** – Select to have the configured ports not to be multicast router ports.

From Port / To Port: Select the range of ports to be configured.

Click the **Apply** button to save your settings. Click the **Delete** button to remove the specified entry.

The IGMP Snooping Mrouter Table is showed as below: **VID (1-4094):** Enter the VLAN ID to be searched.

Click the Find button to locate a specific entry based on the information entered.

Click the Find All button to view all the entries.

Enter a page number and click the Go button to navigate to a specific page when multiple pages exist.

#### L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Statistics Settings

The IGMP Snooping Statistics Settings page allows you to clear and display the IGMP snooping related statistics.

10.00	n Seffrage				
District	VID-01-42340				
(A) +	and the second s				Clear
AP Suspen Subah	ca Table				
First Type	VID 01-403H0				
VLAN				Fini	Find All
Terhall Emblore = 10					
Torial Emblos : 0	KOMPLE	434	842	CAMP	41
Total Extrem =0	KANIWI IN	424 637	140 18	elater HN	43 18

Figure 4.79 – L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Statistics Settings

Statistics: Select the interface to be cleared. The options are All and VLAN. VID (1-4094): Enter the VLAN ID.

Click the **Clear** button to clear the IGMP snooping related statistics.

The fields that can be configured for **IGMP Snooping Statistics Table** are listed below: **Find Type:** Select the interface to be searched. The options are **VLAN** and **Port**. **VID (1-4094):** Enter the VLAN ID.

Click the **Find** button to locate a specific entry based on the information entered. Click the **Find All** button to view all the entries.

### L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Setting

The MLD Snooping Settings page allows you to configure the MLD snooping settings.

Charles Settings	84	_	_			_
Crome State		United	* Duehe			- Analy
All Mater Settergs						
VE (1-489.0)		CENTRE	in Drushke			Acoly
ALL Strengting Table						
90.0-4090 [					Find	Find All
Total Extres : 0						
W0	SCAN No.	10		States .	a company	
6 W	10000	1.		Storese.	Story Catal	Edt

Figure 4.80 – L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Setting

### **Global Settings:**

**Global State:** Select to enable or disable the MLD Snooping state. Click the **Apply** button to save your settings.

### **VLAN Status Settings:**

**VID (1-4094):** Enter the VLAN ID and select to enable or disable MLD snooping on the VLAN. Click the **Apply** button to save your settings.

### MLD Snooping Table:

VID (1-4094): Enter the VLAN ID to be searched.

Click the **Find** button to locate a specific entry based on the information entered. Click the **Find All** button to view all the entries. Click the **Show Detail** button to see the detail information of the specific VLAN. Click the **Edit** button to re-configure the specific entry.

After clicking the Show Detail button, the following window will appear.

MD Strengting VLAN Precentations VID Status Fast Loove Guarter State Guarter State Guarter Vention	r Draabled Draabled Draabled Vi
Guery Hannal Max Response Time Robustemes Value Last Werkler Guery Hiltimal	r 25 saconte 18 saconte 2 3 seconte 2 Modify
	Modey

Figure 4.81 – L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Setting – Show Detail

The window displays the detail information about MLD snooping VLAN. Click the **Modify** button to edit the information in the following window.

After clicking the **Edit** button in MLD Snooping Settings window, the following window will appear.

II Senapang VLAN Settings ND (1-4094) Status Fast Laws Guarter State Quarty Version	Enobled +	Drudded Drudded Druddeo
Outry Warrel(1-31744)	1,25	ter:
Max Response Time(1-26)	10	100
Robustness Value(5-7)	2	
Last Member Guers Interval(1-25)	2	100
		Apply

Figure 4.82 – L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Setting – Edit

Fast Leave: Select to enable or disable the MLD snooping fast leave function.

Querier State: Select to enable or disable the querier state.

Query Version: Select the general query packet version sent by the MLD snooping querier.

**Query Interval (1-31744):** Enter the interval at which the MLD snooping querier sends MLD general query messages periodically.

Max. Response Time (1-25): Enter the maximum response time, in seconds, advertised in MLD snooping queries. The range is 1 to 25.

**Robustness Value (1-7):** Enter the robustness variable used in MLD snooping.

Last Member Query Interval (1-25): Enter the interval at which the MLD snooping querier sends MLD group-specific or group-source-specific (channel) query messages.

Click the **Apply** button to save your settings.

### L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Groups Setting

The MLD Snooping Groups Settings page allows you to configure and view the MLD snooping static group, and view MLD snooping group.

AD Swaping Quin Group				
VD (1-4294) VD (1-4294) *	Group Address Broup Address C	Press Pade [add.020 +]	To Fiel [att1/07 •]	Apply Delete
Tertal Entries : 2				
VO.		Grand Address 1		Paris :
2 E		FE2.1		##/100
1 E		#2.2		att11010
				99 III III III III III
LS Secondary Groups Tell				
VED (1-4894)	Broup Av	dance.		
*[				First First All
Testal Enforms : 8				
	Grange Addresses	Searce Address	Lippers	Pata

Figure 4.83 – L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Group Setting

VID (1-4094): Enter the VLAN ID.

Group Address: Enter the IP multicast group address.

From Port / To Port: Select the range of ports to be configured.

Click the **Apply** button to save your settings.

Click the **Delete** button to remove the specified entry.

Click the **Find** button to locate a specific entry based on the information entered.

Click the Find All button to view all the entries.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

The fields that can be configured for the **MLD Snooping Groups Table** are described below: **VID (1-4094):** Enter the VLAN ID.

Group Address: Enter the IP multicast group address.

Click the **Find Snooping** button to locate a specific entry based on the information entered.

Click the Find All Snooping button to view all the entries.

### L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Mrouter Settings

The MLD Snooping Mrouter Settings page allows you to configure the specified interface(s) as the router ports or forbidden to be IPv6 multicast router ports on the VLAN interface on the Switch.

LD Scenging Winder S				
NO CHARM	Configuration	From Pad.	Tartot	
1	Ped •	attri/0/1 *	* 10.1/01	Apply Durieta
Fortal Entries : 1				Tend And All
VIII			Parte	
		1	RVDGPTOL ORIGINAL TODORSS	

Figure 4.84 – L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Mrouter Settings

VID (1-4094): Enter the VLAN ID.

Configuration: Select the port configuration. Available options are Port and Forbidden Port.

Port: Select to have the configured ports as being connected to multicast-enabled routers.

Forbidden Port: Select to have the configured ports as being not connected to multicast-enabled routers.

From Port / To Port: Select the range of ports to be configured.

Click the **Apply** button to save your settings.

Click the **Delete** button to remove the specified entry.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Find All** button to view all the entries.

Enter a page number and click the Go button to navigate to a specific page when multiple pages exist.

# L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Statistics Settings

The MLD Snooping Statistics Settings page allows you to clear and display the MLD snooping related statistics.

	Songalag Statistica, Table	a Tabe	VO	012-4084		Find	
Endestria Edita	A ·						

Figure 4.85 – L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Statistics Settings

Statistics: Select the type of statistics to display. Available options are All and VLAN.. VID (1-4094): Enter the VLAN ID.

Click the **Find** button to locate a specific entry based on the information entered. Click the **Find All** button to view all the entries.

# L2 Features > L2 Multicast Control > Multicast Filtering

The Multicast Filtering page allows you to view and configure multicast filtering settings.

Filteringle		
hering .		
(1+1-1 ) NA	aut/Filer Hole (Forward Unwgestand )	Apply
is it		
VLAN	Multicasi Filter Mode	
autout:	Farware MI Dropped	
	161 II	<b>13</b> 160
	Farward MI Drazel	

Figure 4.86 – L2 Features > L2 Multicast Control > Multicast Filtering

#### VID List: Enter the VLAN ID.

**Multicast Filter Mode:** Select the multicast filter mode. Options to choose from are **Forward Unregistered**, **Forward All**, and **Filter Unregistered**. When selecting the **Forward Unregistered** option, registered multicast packets will be forwarded based on the forwarding table and all unregistered multicast packets will be flooded based on the VLAN domain. When selecting the **Forward All** option, all multicast packets will be flooded based on the VLAN domain. When selecting the **Filter Unregistered** option, registered packets will be forwarded based on the forwarding table and all unregistered multicast packets will be flooded based on the forwarding table and all unregistered multicast packets will be filtered.

Click the **Apply** button to save your settings.

Enter a page number and click the Go button to navigate to a specific page when multiple pages exist.

### L2 Features > LLDP > LLDP Global Settings

**LLDP (Link Layer Discovery Protocol)** provides IEEE 802.1AB standards-based method for switches to advertise themselves to neighbor devices, as well as to learn about neighbor LLDP devices. SNMP utilities can learn the network topology by obtaining the MIB information in each LLDP device. The LLDP function is enabled by default.

LLDP Global Settings			
LLDP Global Settings			
LLCP Task LLCP Tasked Date LLCP Task Date LLCP WED Task Date	Otrabel ei Otrabel ei	Studied Studied Studied Studied	Auto
LLDP-MED Configuration			
Fast Mart Populat Court (F-13)	1	jaran .	Appro
LLEP Configerations			
Mensage Th Internal (5-12710) Message Th Intel Methodes (2-10) Harint Datas (5-10) Th Datas (1-10)	90 (4 (2 (3) (3)	949 Dés Dés	4400
11.0P System Information			
Cheves ID Eastern Cheves ID Solar Name Solar Name Bolar Causifier Supported Anter Causifier Supported Anter Causifier States	MAC Address Dis GD-44-47-03-79 Sinders_Hamme_Text Dirds-1216-1216-1216 10 Heapenber/Dirdspr Heapenber/Dirdspr	n Ogaant Etherrari Terlich	
LLDP-MED System Information			
Device Clans Hardware Resistor Farmann Resistor Daras Resistor Daras Resistor Manufladure Resistor Manufladure Resistor Manufladure Resistor Manufladure Resistor	Nativesk Connected AC 1.00.002 V1.00.010 D.Livik Consolution D.Livik Consolution D.Livik Consolution		

Figure 4.87 – L2 Features > LLDP > LLDP Global Settings

### LLDP Global Settings:

LLDP State: When this function is enabled, the switch will start to transmit, receive and process the LLDP packets. For the advertisement of LLDP packets, the switch announces the information to its neighbor

through ports. For the receiving of LLDP packets, the switch will learn the information from the LLDP packets advertised from the neighbor in the neighbor table. Click **Apply** to make the change effective.

**LLDP Forward State:** Select to enable or disable LLDP forward state. When the **LLDP State** is disabled and **LLDP Forward Sate** is enabled, the received LLDPDU packet will be forwarded.

**LLDP Trap State:** Select to enable or disable the LLDP trap state.

**LLDP-MED Trap State:** Select to enable or disable the LLDP-MED trap state.

Click the **Apply** button to save your settings.

# LLDP-MED Configuration:

Fast Start Repeat Count (1-10): Enter the LLDP-MED fast start repeat count value. This value must be between 1 and 10.

Click the **Apply** button to save your settings.

# **LLDP Configurations:**

**Message TX Interval (5-32768):** This parameter indicates the interval at which LLDP frames are transmitted on behalf of this LLDP agent. The default value is **30** seconds.

**Message TX Hold Multiplier (2-10):** This parameter is a multiplier that determines the actual TTL value used in an LLDPDU. The default value is **4**.

**LLDP ReInit Delay (1-10):** This parameter indicates the amount of delay from the time adminStatus becomes "disabled" until re-initialization is attempted. The default value is **2** seconds.

**LLDP TX Delay (1-8192):** This parameter indicates the delay between successive LLDP frame transmissions initiated by value or status changes in the LLDP local systems MIB. The value for txDelay is set by the following range formula:  $1 < txDelay < (0.25^{\circ} - msgTxInterval)$ . The default value is **2** seconds.

Click the **Apply** button to save your settings.

# L2 Features > LLDP > LLDP Port Settings

The Basic LLDP Port Settings page displays LLDP port information and contains parameters for configuring LLDP port settings.

DP Part Settings							
From Part	ToPut	Butter	ABVACUAN	Fisher	81800 ····		NEWS
#0x1/0/1 *	eth10/1 +	1004 *	TX and RX .	Pul	Renove		and the second second
tioner. The address stars	uld be the switch's acces						Apply .
Part	1	inity of	- dalteren State		- 19	VE INTRA	Colorest
001100		10100	D(and R)(				
481.602		LAIM	(1000)				
##1(0)3		Link.	T1 and 451				
101.014		1814	Tit and Pol				
101/48		Lanat:	Tit was Fig.				
04/101		1000	Triand Riv				
atri07		taral	711 and Sti				
#8100		Qui	The send Period				
887.00		Larat	T2(and RIC				
101012		10.00	71( and 71)				
10011021		ERON:	75 and 450				
CTOTING .		2414	Transition (199				

Figure 4.88 – L2 Features> LLDP > LLDP Port Settings

**From Port**/ **To Port:** A consecutive group of ports may be configured starting with the selected port. **Subtype:** Select the subtype of LLDP TLV(s). Options to choose from are **MAC Address**, and **Local**. **Admin Status:** Select the LLDP transmission mode on the port. The available options are:

TX – Enables transmitting LLDP packets only.

RX – Enables receiving LLDP packets only.

TX and RX – Enables transmitting and receiving LLDP packets. This is the default value.

**Disabled** – Disables LLDP on the port.

IP Subtype: Select the type of the IP address information to be sent. Options to choose from are All, IPv4

and IPv6.

Action: Select to remove or add the action field. Address: Enter the IP address to be sent.

Click **Apply** to accept the changes made.

# L2 Features > LLDP > LLDP Management Address List

The LLDP Management Address List page displays the detailed management address information for the entry.

				Find	
Sutton	Aster	V feet	640	Adventising Parts	
194	10.00.001440	20.000	1001212211		
214	946 340 100 10T W/ 576	- Origonal-			

Figure 4.89 – L2 Features > LLDP >LLDP Management Address List

**Management Address:** Select IPv4, IPv6 or All address to be displayed. Click **Find** and the table will update and display the values required.

**Subtype:** Displays the managed address subtype. (e.g., MAC or IPv4)

Address: Displays the IP address.

IF Type: Displays the IF Type.

**OID:** Displays the SNMP OID.

Advertising Ports: Displays the advertising ports.

# L2 Features > LLDP > LLDP Basic TLVs Settings

This LLDP Basic TLVs Settings page allows you to configure the LLDP Port settings.

LDP Bessel 1	D.Vo Tetting	5					
Press Park ets1/0/1	•	ToPat eth10/1	Part Description Deabled	Dysherr Harra Dreahled	Dviden: Deschahon [Chashled: *]	Durben Casubilities Duratied	Apply .
	Post		hat Description	Santorn Name	System Destite	ALL STOLEN	micasemes
1	10101		Disatient	Disanan	Disease		Droofing
	48/18/3		The most	Tressai	Thursd		Delument
	10100		Olasied	thusand .	Diseas :		Distained
			2294003	Disatra	Unabre		Distance
	1011044		Disated :	theseas:	Duster		Drishe#
	18/10/6		Desired	Donest	frister:		Ditates:
	100/94		Drammi	Duston,	Dister		Decement
	10100		23.4 alloted	Desired	Disales		Distanting .
	48.005		Disabert	Disabeti	Detailed		Disident
	e#1/0/14		(Asame	(historie)	Duides		Division .
	******		Crowned.	Diseased	Disaber		Disolar
10 10	4858007		Dayson .	Diseased.	Devere		Distance .

Figure 4.90 – L2 Features > LLDP > LLDP Basic TLVs Settings

**From Port** / **To Port:** A consecutive group of ports may be configured starting with the selected port. **Port Description:** Select to enable or disable the Port Description option.

**System Name:** Select the system name to be enabled or disabled in the LLDP port. If select is Enabled, users can specifies the content of system Name or all.

**System Description:** Select to enable or disable the System Description option. **System Capabilities:** Select to enable or disable the System Capabilities option.

Click **Apply** to accept the changes made.

# L2 Features > LLDP > LLDP Dot1 TLVs Settings

This LLDP Dot1 TLVs Settings page allows you to configure an individual port or group of ports to exclude one or more of the IEEE 802.1 organizational port VLAN ID TLV data types from outbound LLDP advertisements.

P Burt D.Vs. Sats	145 ·····			
um Pat 4916/1 •	To Pod (#010/1 •	PostVLAN Protocol (LAN [Deadled •] [	vijet name [Dryabled •]]	Protocol laborith [Discabled +][Note +] Apple
Part	Partition	Enabled Part and Protectal VE	Enabled VCAN Harns	Transied Protocol Monthly
	Children			
att: 00	Comeé			
001100	Chisteri			
antine	Chivese .			
antins	Closed			
481105	Children			
101100	Chatter			
4811495	Chintee			
001103	Challed			
38114210	Champer .			
atritety	Chumpe.			
shittiz .	Counted			

Figure 4.91 – L2 Features > LLDP > LLDP Dot1 TLVs Settings

From Port / To Port: A consecutive group of ports may be configured starting with the selected port.

**Port VLAN:** Select to enable or disable the port VLAN ID TLV to send. The Port VLAN ID TLV is an optional fixed length TLV that allows a VLAN bridge port to advertise the port's VLAN identifier (PVID) that will be associated with untagged or priority tagged frames.

**Protocol VLAN:** Select to enable or disable Port and Protocol VLAN ID (PPVID) TLV to send, and enter the VLAN ID in PPVID TLV.

VLAN Name: Select to enable or disable the VLAN name TLV to send, and enter the ID of the VLAN in the VLAN name TLV.

**Protocol Identity:** Select to enable or disable the Protocol Identity TLV to send, and the protocol name. Options for protocol name to choose from are **None**, **EAPOL**, **LACP**, **GVRP**, **STP**, and **AII**.

Click the **Apply** button to save your settings.

### L2 Features > LLDP > LLDP Dot3 TLVs Settings

The LLDP Dot3 TLVs Settings page allows you to configure an individual port or group of ports to exclude one or more IEEE 802.3 organizational specific TLV data type from outbound LLDP advertisements.

P Dord 31 via Sortio	da .				
00 Pad 0.007 •	39998 (eh10/1 •	Incoher Contact Deated	noorthatus Leve.Appregation [Decabled •]	Meanware Franse Bigs [Disabled +]	Prover Via MDI Distabled • Apply
Post	NAC FIN Centre	adam Status	Link Appropriate	Manirose Transe Size	Present Vita MCH
-99/1071	0.00	41	Chinese	Distance of the second	Chiefes
48100	Dass	ad .	Chaterol	Dustei	Chummel
atritat	Disate	ei	Distant .	Durent	Oreaster
481.04	Dyan	ed	Disting	Chiebert	Chiefed
shiss	Daw	ed	Childrend	Dated	Chinkled
48.100	Dist	ed	COLUMN C	211d/ht	DHARME
s#ri307	Dist	ed.	Outstind	Chiefed	Ceation
48.100	Ottav	4.1	(Distant)	Distant	Deater
481100	Dear	ed.	CHIENE	District	Chiefent
	Disasi	ed	Creative	Chisbled	Creative
1000000	Diago	64	CHLIRING	Childred	CHARGE
WANGIG	Dage	ed be	Chatted	Dastar	Cetagenet

Figure 4.92 – L2 Features > LLDP > LLDP Dot3 TLVs Settings

From Port/To Port: A consecutive group of ports may be configured starting with the selected port.

**MAC/PHY Configuration/Status:** Select whether the MAC/PHY Configuration Status is enabled on the port. The possible field values are:

Enabled – Enables the MAC/PHY Configuration Status on the port.

Disabled – Disables the MAC/PHY Configuration Status on the port.

Link Aggregation: Specifies whether the link aggregation is enabled on the port. The possible field values are:

**Enabled** – Enables the link aggregation configured on the port.

**Disabled** – Disables the link aggregation configured on the port.

**Maximum Frame Size:** Specifies whether the Maximum Frame Size is enabled on the port. The possible field values are:

**Enabled** – Enables the Maximum Frame Size configured on the port.

**Disabled –** Disables the Maximum Frame Size configured on the port.

**Power via MDI:** Advertises the Power via MDI implementations supported by the port. The possible field values are:

Enabled – Enables the Power via MDI configured on the port.

**Disabled** – Disables the Power via MDI configured on the port.

Click **Apply** to implement changes made.

# L2 Features > LLDP > LLDP-MED Port Settings

The LLDP-MED Port Settings page allows you to enable or disable transmitting LLDP-MED TLVs.

OF MED Port	Fettings				
LDP-MED Field Setting					
Franc Part (wh1/G/1 *	ToPat en10/1	Capabilies Deabled	Network Paray [Teached +]	Deaties	hears
Post -		Entertains	Heterr	t Party	beautiery.
48.431		Dreament	DHA	ad hit	Disation
981.00		Disation	Chin	1996	Danner
084303		Dission	Des	1604	Dearne
48/0.04		Distance	Dtie		Dested
481.00		Databad	Dwa	akieŭ .	Dusses
98156		Dreamed .	Chief	WW	During
98±807		Desived	Cate	die#	Towadoud.
68,1028		Disation	046	1004	(Disable)
101194		Doubled :	One	MNR :	Double#
atmoto		Davent	Des	446	Doorer.
settion1		Invenet	1 Dres	white the second se	Dhated.
1011012		Divisions	Chia	and the second sec	Duster

Figure 4.93 – L2 Features > LLDP > LLDP-MED Port Settings

**From Port/To Port:** A consecutive group of ports may be configured starting with the selected port. **Capabilities:** Select to enable or disable transmitting the LLDP-MED capabilities TLV. **Network Policy:** Select to enable or disable transmitting the LLDP-MED network policy TLV. **Inventory:** Select to enable or disable transmitting the LLDP-MED inventory management TLV.

Click **Apply** to accept the changes made.

# L2 Features > LLDP > LLDP Statistics Information

The LLDP Statistics Information page displays an overview of all LLDP traffic.

UP Name	Information .						
Last Charge Total Cristino Total Cristin Total Aphrodit	tine .	8 8 8 8					Courter
LUP Statistics	Parts						
Port	ath1.0/1 +					Clear Counter	Clear All
INIT	Total Transmiss	Deatherades	Titermes	Destaura	Total TLV Decards	Total IL V Linknows	Internet
anvior		- marganese				and the second sec	
+#1100	1	6	4	- 1	1	(E)	-1
(0110)		6		1		. 8	8
****	1		1	- 1	1	1.0	1
etrites			4	4	8	(#)	
481100		- E	4	1	0	12.4.2	
1000184	1	6	4	-1	30	1.0.1	1
##11535	1	((#))	(K)		)(	000	1
001196	1	e	4	1	1		1
1112/128	(I) (II)	3	τ.	- 1	.0.	11011	
wenters		6	4	1	0		
					1		

Figure 4.94 – L2 Features > LLDP > LLDP Statistics Information

The following information can be viewed:

LLDP Statistics Information: Displays the counters that refer to the whole switch.

**Last Change Time** – Displays the time for when the last change entry was last deleted or added. It is also displays the time elapsed since last change was detected.

Total Inserts - Displays the number of new entries inserted since switch reboot.

**Total Deletes** – Displays the number of new entries deleted since switch reboot.

Total Drops – Displays the number of LLDP frames dropped due to that the table was full.

Total Ageouts – Displays the number of entries deleted due to Time-To-Live expiring.

LLDP Statistics Ports: Displays the counters that refer to the ports.

**Ports:** Select the port to be displayed.

Total Transmits – Displays the total number of LLDP frames transmitted on the port.

Total Discards – Displays the total discarded frame number of LLDP frames received on the port.

Total Errors – Displays the Error frame number of LLDP frames received on the port.

Total Receives – Displays the total number of LLDP frames received on the port.

**Total TLV Discards** – Each LLDP frame can contain multiple pieces of information, known as TLVs. If a TLV is malformed, it is counted and discarded.

Total TLV Unknowns – Displays the number of well-formed TLVs, but with a known type value.

**Total Ageouts** – Each LLDP frame contains information about how long time the LLDP information is valid. If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.

Click the **Clear Counter** button to clear the counter information for the statistics displayed. Click the **Clear All** button to clear all the counter information displayed.

### L2 Features > LLDP > LLDP Local Port Information

The LLDP Local Port Information page displays LLDP local port information.

IN an According to the Court Party Street Take			
not ethility	•		Find Those Data
Patter	Peril D Sampler	Part IV	Phillipscopen
481/97	Line	100/1027	
California -		(Rrin)7	
C01498	Line .	18110/2	
400123/4	Line	0811024	
whites.	Long	um1/2/5	
and the second	LIDE	261128	
s0110/f	Local .		
001155	Line .	attrick	
101100	Lave	1001002	
BRINSTE	Local	advit/datu	
##12019	Line	#8110/11	
#810103	CHOR	21031040	

Figure 4.95 – L2 Features > LLDP > LLDP Local Port Information

Port: Displays the port number.

Port ID Subtype: Displays the port ID subtype.

Port ID: Displays the port ID (Unit number/Port number).

Port Description: Displays the port description.

Click Find to displays more information for the specified port.

After clicking the Show Detail button, the following page will appear.

LLDP Local Port Information	
ELDP Local Information Table	
Pol Pol E Pol Disarbase Pol G Pol Polypton Managerowst Aptress Count PrvDo Dimes VLAN Instee Entres Count PrvDo Dimes VLAN Instee Entres Count MACPHY Configuration MACPHY Configuration MACPHY Configuration MacPHY Configuration MacPHY Configuration MacPHY Configuration MacPHY Configuration MacPHY Configuration MacPHY Configuration	um trăm Lan ai am trăm Î Î Î Î Î Î Î Î Î Î Î Î Î Î Î Î Î Î Î

Figure 4.96 – L2 Features > LLDP > LLDP Local Port Information – Show Detail

Click the **Back** button to return to the previous window.

#### L2 Features > LLDP > LLDP Neighbor Port Information

This LLDP Neighbor Port Information page allows you to display the information on a per port basis currently available for populating outbound LLDP advertisements in the local port brief table shown below.

The printiple of the	Clined Taken					
von 🔄	+10/1 *				Fired	Clear
						Clear All
TERMER REPORT						_
Total Entries :	Channel D Sublype	Channe B	Fort \$2 TARRAN	Porter	Part Decemption	

Figure 4.97 – L2 Features > LLDP > LLDP Neighbors Port Information

Click the Find button to locate a specific entry based on the information entered.

Click the **Clear** button to remove the specified port of LLDP neighbor port or click **Clear All** button to remove all LLDP neighbor ports.

# L3 Features > ARP > ARP Aging Time

The ARP Aging Time page allows you to view and configure the ARP aging time settings.

AP Aging Time		
999 Augeng Time		
Total Entropy : 1		
beautace Name	Timerest drive	
(ter)	00	Fat
		11

Figure 4.98 – L3 Features > ARP > ARP Aging Time

**Timeout(min):** Specifies the aging time of the ARP entry. The default is 5 minutes.

Click the **Apply** button to save your settings.

Click the Edit button to re-configure the specific entry.

Enter a page number and click the Go button to navigate to a specific page when multiple pages exist.

# L3 Features > ARP > Static ARP

The Static ARP page provides information regarding each interface, including which IP address was mapped to what MAC address. Enter an **IP Address** or **Hardware Address** and then click **Apply** to create a new ARP entry.

Antess	manin				Apply
dalEntras; 1					Culsto A
Interface Name	T Address-	Hardward Address	Ageng Tires	lawe	-
ward	102 104 10 101	BLOUDER, MURITY	10-00	iner.	e det
and a	182.164.50.141	34-86-95-86-86-CX	Firmer'	iner-	Dei

Figure 4.99 – L3 Features > ARP > Static ARP

Click Edit to modify the Hardware Address.

Click **Delete** to remove the information from ARP table.

Click **Delete All** to remove all information from ARP table.

Enter a page number and click the Go button to navigate to a specific page when multiple pages exist.

### L3 Features > ARP > ARP Table

The ARP Table page allows you to view and configure the ARP table settings.

Interface (4.40) (1-4054)	1	C PARTERS T	Matk		
Haldware Address		(), 7We	•	11	Fint
laitetres:0					Clear A
basiface Name	W AARINA	Hartleven Abbres	Againg Term (2001)	THE	
sia(1	102.100.11	06+4+16-3F-4F-8D	100	Departm	Celete
watt	102398.1031	10.0011-0519-01	100	Deverse	Ownerby.
them .	152.168.12.88	10-10-27-49-37-84	100	Detreme:	Dwiete
1001	1621681681	10 00 00 00 00 00 00	Former	(Table	Ourieta.
1997)	1921553.64	74-04-75-30-14-63	100	Detatto	Deleta
statt	582.188.1K(24)	00-DC-26-AD-AB-TE	100	Devariat	Deleta

Figure 4.100 – L3 Features > ARP > ARP Table

Interface VLAN (1-4094): Select and enter the interface's VLAN ID.

IP address: Select and enter the IP address to be displayed.

Mask: Enter the mask address for the specified IP address.

Hardware Address: Select and enter the MAC address.

**Type:** Select the type.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the Go button to navigate to a specific page when multiple pages exist.

#### L3 Features > IPv4 Interface

The IPv4 Interface page allows you to configure the IPv4 Interface settings.

set batter Facilie						
derbi e vijale († 40945	£			1	Apply	End
Install Englishes 1 1						
Inter Cases	3446	<b>ITAAkuus</b>	LUACTUALS			
stany.	Change .	K27 E.E. 10255 DOLD Market	1.6	3 54		elete

Figure 4.101 – L3 Features > IPv4 Interface

Interface VLAN (1-4094): Enter the VLAN ID of IP interface.

Click **Apply** for the settings to take effect.

Click the **Find** button to display the specific entry.

Click the **Edit** button to re-configure the specific entry.

Click the **Delete** button to remove the specific entry.

Enter a page number and click the Go button to navigate to a specific page when multiple pages exist.

After clicking the **Edit** button, the following window will appear.

<b>Evit Interface Settings</b>	DHCP Cavet	
netice .	Hart	East.
Sattings		
State	Enabled +	Acoly
# Settings		
Out P Faire	Data +	
(F.Addati)	127 0 0 1	
Mate	255.0.0000	Apply

Figure 4.102 – L3 Features > IPv4 Interface - Edit

Click the **Back** button to return to the previous window.

State: Select to enable or disable the IPv4 interface's global state.

Click the **Apply** button to save your settings.

### **IP Settings:**

**Get IP From:** Select the IP from option. The values are Static and DHCP. When the **Static** option is selected, users can enter the IPv4 address of this interface manually in the fields provided. When the **DHCP** option is selected, this interface will obtain IPv4 information automatically from the DHCP server located on the local network.

IP Address: Enter the IPv4 Address for this interface.

Mask: Enter the IPv4 subnet mask for this interface.

Click the **Apply** button to save your settings.

After clicking the **DHCP Client** tab, the following page will appear.

A LANDARD CARSING PLUS			
Bhyd Referitions Settings	DHOP Clean	f	
OHOP Cleve Chine ID (1-4314)	0		
Divers 4D Diving	23 ities	C Het	
-Uniforme	al men	a second s	
Lanca	6	Deser 18-100000 (00 + Hours 00 + Minutes	Apply

Figure 4.103 – L3 Features > IPv4 Interface – DHCP Client

**DHCP Client Client-ID (1-4094):** Enter the VLAN interface, whose hexadecimal MAC address will be used as the client ID to be sent with the discover message.

**Class ID String:** Enter the vendor class identifier with the maximum of 32 characters. Tick the **Hex** check box to have the class identifier in the hexadecimal form.

Host Name: Enter the host name.

**Lease:** Enter the preferred lease time for the IP address to request from the DHCP server. Enter the day duration of the lease, or select the hour and minute duration of the lease.

Click the **Apply** button to save your settings.

### L3 Features > IPv4 Default Route

The IPv4 Default Route page allows you to view and configure the IPv4 static and default route settings.

Default Rante				
and the second se		1		40
P Address	Meth	Constant of Constant	Martine Name	
1000	0.010	12100121		Delete

Figure 4.104 – L3 Features > IPv4 Default Route

Gateway: Enter the gateway address for IPv4 default route.

Click **Apply** for the settings to take effect.

Click the **Delete** button to remove the specific entry.

### L3 Features > IPv6 Interface

The IPv6 Interface page provides user to the IPv6 interface's settings.

Pv6 adarbece			
sterace VLAN (1-40940			Apply I finit
Total Entries : 1			
Sector Factor		Link States	
mail	Prisé ferre		Detail

Figure 4.105 – L3 Features > IPv6 Interface

Interface VLAN (1-4094): Enter the VLAN ID of IP interface.

Click Apply for the settings to take effect.

Click the **Find** button to display the specific entry.

Click the Detail button to view and configure more detailed settings for the IPv6 interface entry.

After clicking the **Detail** button, the following window will be appear.

While Interface Settings	Worface Pvt Air	A YON	DHCPVS Chint		
intice (	east (				
Pret State	Enabled.			Back	Appris
Index EV-6 Address Setting					
Pyd Adamys					Approv
45 Interval Settings					
Add methodal (1-38.00)	B	10			Apply

Figure 4.106 – L3 Features > IPv6 Interface - Detail

**IPv6 State:** Select to enable or disable the IPv6 interface's global state. Click the **Apply** button to save your settings.

# Static IPv6 Address Setting:

**IPv6 Address:** Enter the IPv6 address for this IPv6 interface. Select the **EUI-64** option to configure an IPv6 address on the interface using the EUI-64 interface ID. Select the **Link Local** option to configure a link-local address for the IPv6 interface.

Click the **Apply** button to save your settings.

#### **NS Interval Settings:**

**NS Interval (1-3600):** Specify the NS interval and the values are between 1 and 3600. Click the **Apply** button to save your settings.

After clicking the Interface Address tab located at the top of the page, the following page will appear.

Bhit Interface Settings	Worlace IPVE Address	DHCPvS Client	
Ral Boltiles ( 1 .			
Ashters Ta		EVO AARTON	
Law Local Acta		Net Did same there	Dates 1

Figure 4.107 – L3 Features > IPv6 Interface – Interface IPv6 Address

After clicking the **DHCPv6 Client** tab located at the top of the page, the following page will appear.

The knowledge Suffrage	wherige a DVG Address	DISCPusi Client	
HOP/6 Chief			Restirt
ON Case Settings			
Land Shata	Disabled + 8	apid commit	Apply

#### Figure 4.108 – L3 Features > IPv6 Interface – DHCPv6 Client

Click the **Restart** button to restart the DHCPv6 client.

**Client State:** Select to enable or disable the DHCPv6 client state. Click the **Apply** button to save your settings.

### L3 Features > IPv6 Neighbor

The user can configure the Switch's IPv6 neighbor settings. The Switch's current IPv6 neighbor settings will be displayed in the table at the bottom of this window.

demack VLAN (1-4334)	Prickapola (1111)	MAC ADDRES	125.469	T	Apply
methica VLAN (1-4294)				Frid	Clear
etal Entities (2					City Al
Pv6.Address	Link Layer Address	forfast Cascie.	Type	1044	- Contraction
PERCIPACIFIC PERCIPACITY	10 00 40 PL 34 22	of set	Dimanes	21040	Debte
RENO: NOO 27117 / EBIE 704	18-00-27-08-87-84	diam'r.	Dynami	20am	. Deine

Figure 4.109 – L3 Features > IPv6 Neighbor

Interface VLAN (1-4094): Enter the VLAN ID of the IPv6 neighbor.

**IPv6 Address:** Specifies the neighbor IPv6 address.

MAC Address: Specifies the link layer MAC address.

Click the **Apply** button to save your settings.

Click Find to locate a specific entry based on the information entered.

Click **Clear** to clear the specified information entered in the fields.

Click **Clear all** to clear all the information entered in the fields.

Enter a page number and click the Go button to navigate to a specific page when multiple pages exist.

### L3 Features > IPv6 Default Route

The IPv6 Default Route is used to configure the IPv6 static or default routes.

Pv6 Dofaalt flowin				
100 Feb VLAN (1-4104)				
Mand Hop (Frid, Application	director.			Apply
Tetal Extrem : 1				
			- Protocol	
Shi dahara Prefix Langh	Head May	Interface Revie		

Figure 4.110 – L3 Features > IPv6 Default Route

Interface VLAN (1-4094): Enter interface's VLAN ID that will be associated with this route Next Hop IPv6 Address: Enter the next hop IPv6 address

Click the **Apply** button to save your settings.

Click **Delete** to remove the information from IPv6 default route table.

# QoS > Port Default CoS

The Port Default CoS page allows you to view and configure the port's default CoS settings.

et bereat call				
fran Purl eth16/1 +	10.896 [#010/12 *]	Defect Coll (0 • [0 • ] © Oversex	(Josef	Apphy
10		Default Cold	Oversite	
	1001		Tab	
-	102	1	194	
	100	*	PA6	
	104	10	140	
-	1000		10/	
	ilmini .	8		
-	1.007	4	24	
	NUDR /	¥.	Nie	
	0.000	8.7	http	
13	0016		14	
**	ANNY ST.	1	Ne	
	A6H3	8	April 1	

Figure 4.111 – QoS > Port Default CoS

From Port / To Port: Select the range of ports to be configured.

**Default CoS:** Select the default CoS option for the specified ports. The values are from **0** to **7**. Click the **Override** check box to apply the port's default CoS to all packets (tagged or untagged) received by the port. Select the **None** option to use the default settings.

Click the **Apply** button to save your settings.

# QoS > Port Scheduler Method

The Port Scheduler Method page allows you to view and configure the port scheduler method settings.

ort Scheduler Meth	od -			_
at Scheduler Moltani				
rion Port eth/140/1 +	76.4%#   wb1/5/12   +	Branpus Helicol (SP)		Auty
	Part		Schoolsky Medical	
d.	- 101.011			
	401002		10	
	4911/25		5P	
	451124		9	
	am1615		10	
	-25104		9	
	( #010kf			
	101104		38	
	100100		27	
	88.0877		<i>w</i>	
	senant.		14 M	
	481040			

Figure 4.112 – QoS > Port Scheduler Method

From Port / To Port: Select the range of ports to be configured.

**Scheduler Method:** Select the scheduler method for the specified ports. Available options are Strict Priority (**SP**), Round-Robin (**RR**), Weighted Round-Robin (**WRR**), and Weighted Deficit Round-Robin (**WDRR**). By default, the output queue scheduling algorithm is **WRR**.

Click the **Apply** button to save your settings.

### QoS > Queue Settings

The Queue Settings page allows you to configure the queue settings.

e Setinge			
n Port	Tu finit (em16/12_+) (0_+)	white Weight (3:121) MORE Granter	v (8-127)
Part	Oanse D	Will Height	WORE CAREER
	*	1	1
		(a)	1
	1	(11) (11)	2
0001001		(4)	
Contraction of the	*	- 5	+
	1		
		P	1
		2.1	
		2	1
	4	3	3
Datate		199	
		1997 (A. 1997)	
			4
	1		2
		1.0	1
	1		1
			1
	1		
08100			

Figure 4.113 – QoS > Queue Settings

From Port / To Port: Select the range of ports to be configured.

Queue ID: Select the queue id value. The range is between 0 and 7.

WRR Weight (0-127): Enter the WRR weight value. The value is between 0 and 127.

WDRR Quantum (0-127): Enter the WRR quantum value. The value is between 0 and 127.

Click the **Apply** button to save your settings.

### QoS > CoS to Queue Mapping

The CoS to Queue Mapping page allows you to view and configure the CoS-to-Queue mapping settings.

Casi	Cuerae ID	
0	2 *	
1	0 •	
2	1 •	
3	3 •	
4	4 *	
5	5 *	
8	6 •	
7	7 •	

Figure 4.114 – QoS > CoS to Queue Mapping

**Queue ID:** Select the queue ID that will be mapped to the corresponding CoS value. The value is from are **0** to **7**.

Click the **Apply** button to save your settings.

#### QoS > Port Rate Limiting

The Port Rate Limiting page allows you to view and configure the port rate limiting settings.

ort Flate Catalling						
nos net Te ha en 164 • (en 13	12 +	Deether Han Lord (hand 1) & Sandwall O Penanti () Name	n (d.4. 100000000). L-1000	1041	Barri Say (8-12000) Barri Rei (8-12000)	12ve
			414		Ordipat	
Part		0.000	literet		Hate	Hurst
-101/08		Heline	File Land		visiting.	He Lint
10100		Tes Lovar .	For Land		2401248	He Line.
ar0100.5		Malana	No Level		TaxLand	hellerd.
1011104		-tert.me	NULIN		sectand	lise Light
10105		THEFT	PELPH .		No. Line	Nethern
antine		Hatleh	No Lesi		Heline	Notient
att0.097		THE GAME	PRIDE		THE LAW	THE LIVET
eth1701		Halane	No Levil		Heriuma	No.Level
		Hallow.	Pill Land		NALIMI	Holient
491015		NELINE	Poi Linte		140 Linet	the Limit
ans.551		Notice	Nor Land		- NALIMA	-116 s.)reff
#91012		Nesser	Neterit		NO LINK	101101

Figure 4.115 – QoS > Port Rate Limiting

From Port / To Port: Select the range of ports to be configured.

**Direction:** Select the direction. Available options are **Input** and **Output**. When **Input** is selected, the rate limit for ingress packets is configured. When **Output** is selected, the rate limit for egress packets is configured.

Rate Limit: Enter the Rate Limit for the specified port.

When **Bandwidth** is selected, enter the input/output bandwidth value used in the space provided. This value must be between 64 and 10000000 kbps. Also, enter the **Burst Size** value in the space provided. This value must be between 0 and 128000 kilobytes.

When **Percent** is selected, enter the input/output bandwidth percentage value used in the space provided. This value must be between 1 and 100 percent (%). Also, enter the **Burst Size** value in the space provided. This value must be between 0 and 128000 kilobytes.

Select the **None** option to remove the rate limit on the specified port(s). The specified limitation cannot exceed the maximum speed of the specified interface. For the ingress bandwidth limitation, the ingress can trigger a pause frame or a flow control frame when the received traffic exceeds the limitation.

Click the **Apply** button to save your settings.

#### QoS > Queue Rate Limiting

The Queue Rate Limiting page allows you to view and configure the queue rate limiting settings.

anne Mate	1. and and															
Hore Part white//	•	15-754 em140/12	1100110	0	-	itel Bandvid Pasianti		ooren [		1241		eriveite d		*		120
					11/40		0.000								0.0	estr
-	-	in the second		140) - I	-07	Pro-		1		and the second	and the second		10-	-	and the second	-
المعا	din FLAR	Max Folde	din too	Mar Puter	Maritar	Ran Hide	Maillan	Mar Press	Min. IL.M.	Ster Harr	distant.	Man Plate	101122	MAX PURP	Mar Flate	Mars Rose
annan.	301100	Missee	2012/01/	railing.	MALLING	Mariana.	No Link	THE LOCAL	DELET	NULLINE	No Links	TRACKS.	Abi Limit	THE LOOP	No Links	THE LOW
10102	Matter	NULERS	INCL.Fril	Wilcont.	Notion	101.000	NULWER	No.Lent.	NULAW	Mathem	THE LEVEL	100.1,000	Molard	NULTRI	PROLEMS.	hitre
401022	1411.411	10/1214	No. Long	PALLING.	1111-00	HELING	1021.000	HELINE	Netant	101.415	1111.00	1012214	1015214	ALL LOOP	Pai Land	Poi Las
antria.	2012/08	NULERS	THE LPTH	100 Leef	NUMB	ANX HER	And Lot of	HELEN.	NULTER	3491,6416	TRACKS.	1011201	NUMBER	<b>MAGENT</b>	PROLEME	101.00
1005	NULIN	MULTER	William B	I BILING	NULTRA	WLINE	Hel Lines	NULTE	Rou Lives	Poller.	HILDER	PRILEVE	NULIME	History	THE LOOP	THE Loss
mi/ps:	Notine	His Land	In Lovit	NELINE.	Notient	Notine	tes paret	Heysine	NATION	Molave	No Lant	the Linest	NOLIME	NULINE	ne Level	1011.01
491/97	Helpel	3812218	THE LOOP	TRILING.	NUMBER	BALLINE.	HILPH	NUMBER	Tex Land	INCLUSE.	To Link	NULTRE	HILIPPE	MILPH.	PRILING.	THE LOT
antitia.	Holizant	101.000	THEFT	Tex Land	ferrined.	1012200	Reserve	Haume	No.Louis	Holist	THE LOCAL	10.1114	TRILIPPE	for Lovel	for Line	fering
10005	HILIN	TALLEY.	NUM	(MALERIA)	HOURS	(MACON M	101200	Marganet.	No.Lond	NALLANE	MALLER	NULTRA	NUCCHAR	HALPHI	NALISA	Halles
01000	NoLINE	Heilert	10012118	1011210	NUMBER	NIGHT	No Lines	NUMB	PROLINE	-	No Line	PERCENT.	1011218	<b>Numm</b>	THE LOOP	the Los
diverit.	Hillin	ARCLER	101200	TRALING.	NULIME	MALLONG.	No Loss	NULLER:	PALANE	william	NALIMA	THYLSTE	Willia	Hannet	PELINE	No Los
Ensine .	MOLINE	PRILIPHI	Ni Land	THE LIVE	NUMBER	NUCLIM	Tex Lorest	No Lord	THELEWE	NOLINE	No Lordi	MALENN!	Mittent	Hitset	Thi Level	NALT

Figure 4.116 – QoS > Queue Rate Limiting

From Port / To Port: Select the range of ports to be configured.

Queue ID: Select the queue ID for the specified ports. The value is between 0 and 7.

Rate Limit: Specify the Rate limit option.

If you selected the **Min Bandwidth** option, enter the minimum bandwidth rate limit value in the space provided. This value must be between 8 and 10000000 kbps. Also enter the maximum bandwidth (**Max Bandwidth**) rate limit in the space provided. This value must be between 8 and 10000000 kbps.

If you selected the **Min Percent** option, enter the minimum bandwidth percentage value in the space provided. This value must be between 1 and 100 percent (%). Also enter the maximum percentage value (**Max Percent**) in the space provided. This value must be between 1 and 100 percent (%).

Click the **Apply** button to save your settings.

#### QoS > Port Trust State

The Port Trust State page allows you to view and configure the port trust state settings.

Port Trust State				
Part Drast Slude				
FrancFlat [ath:10/1 +]	To Past white/12 •	Tool Base Codi 💌		
1	Ret		Trust State	
	+http:/		Cut	
	10101		548	
	e8/1/017		Cell	
	10104		- Cut	
	and cars		Coll	
12	sectors.		Cut	
	48/1/07		Cell	
	101/08		0.04	
	4011225		0.0	
	2010/01/2		548	
	ahtiptti		Sift	
2	ae(10)(2		044	3

Figure 4.117 – QoS > Port Trust State

From Port / To Port: Select the range of ports to be configured. Trust State: Select the trust state to be CoS or DSCP.

Click the **Apply** button to save your settings.

## QoS > DSCP CoS Mapping

The DSCP CoS Mapping page allows you to view and configure the DSCP CoS mapping settings.

CP CVS Maxing						
art Parl To Part	Call	DQCP Limits-KD				
616/1 • (#16/12 •	<u>()</u>		Apply			
Hatt	Geli	31909° Liat	_			
	0	¥7				
		bit /				
	3	14-22				
weit041		24.01				
Serior 1	*	32.38				
	4	45.47				
	*	49-01				
		88.82				
		±1				
	1	618				
	1.	16.22				
vertical.	1	34.21				
		32.18				
		440				
		45-58				
	1	53-68				
	8	67				
		8.15				
	1	(9.22)				
W105	1	29.21				
	*	32-28				
	5	45-47				
		48.58				

Figure 4.118 – QoS > DSCP CoS Mapping

From Port / To Port: Select the range of ports to be configured.

**CoS:** Select the **CoS** priority.

DSCP List (0-63): Enter the DSCP list number.

Click the **Apply** button to save your settings.

#### ACL > ACL Configuration Wizard

The ACL Configuration Wizard page allows you to create a new ACL access list or configure an existing ACL access list.



Figure 4.119 – ACL > ACL Configuration Wizard

Create: Select Create and enter the ACL Name with a maximum of 32 characters.

**Update:** Select to see a table below with the existing ACL access lists. Select the specific re-configure the entry.

Click the **Next** button to continue.

After clicking the **Next** button, the following window will appear.



Figure 4.120 – ACL > ACL Configuration Wizard – Packet Type

MAC: Select to create a MAC ACL.

IPv4: Select to create an IPv4 ACL.

IPv6: Select to create an IPv6 ACL.

Click the **Back** button to return to the previous window.

Click the Next button to continue.

To define the MAC ACL: Select MAC and then click the Next button. Click the associated tabs with MAC Address, Ethernet Type and 802.1Q VLAN, the following page will appear:

	Solid: Packet Type >> And		igi	
Tespenne Ho (1-82525) seige role citterta MAC Address MAC Address			121	
MAC Address	Eliternet Type			
MAC Address	Eliternet Type			
		HEZ. 10 VEAN		
# MN				
			16 AV	12
Barre	1	Cartholic	_ 990.0	
C MAG		DerBrahen	MAC	
4003	aid in the		Manad .	121
5 TES				
Ethernet Type				
Specify Different Type	Please 5	Hatt +		
Ethernel Tipe (0x000-0x*	(0):			
Ethernal Time Marie (DeC-	64FFF)			
HEZ TO VLAH				
Cell	Please Select	1. •		
VEH CHARRING				
Tere Harpt	11(1993)			
Auton	+ form C.Devr			

Figure 4.121 – ACL > ACL Configuration Wizard – Create MAC ACL

The Add ACL Profile MAC ACL contains the following fields:

Sequence No.(1-65535): Select the ACL rule number. The value is between 1 and 65535. Select Auto Assign to automatically generate an ACL rule number for this entry.

**Source:** Select and enter the source information. Available options are **Any**, **Host**, and **MAC**. When **Any** is selected, any source traffic will be evaluated according to the conditions of this rule. When **Host** is specified, enter the source host's MAC address. When **MAC** is selected, the **Wildcard** will also be available. Enter the source MAC address and wildcard value in the spaces provided.

**Destination:** Select and enter the destination information. Available options are **Any**, **Host**, and **MAC**. When **Any** option is selected, any destination traffic will be evaluated according to the conditions of this rule. When **Host** is selected, enter the destination host's MAC address. When **MAC** is selected, the **Wildcard** will also be available. Enter the destination MAC address and wildcard value in the spaces provided.

Specify Ethernet Type: Select the Ethernet type option. Options to choose from are aarp, appletalk, decent-iv, etype-6000, etype-8042, lat, lavc-sca, mop-console, mop-dump, vines-echo, vines-ip, xns-idp, and arp.

**Ethernet Type (0x600-0xFFFF):** Enter the Ethernet type hexadecimal value. The value is between 0x600 and 0xFFFF. When any Ethernet type profile is selected in the **Specify Ethernet Type** drop-down list, the appropriate hexadecimal value will automatically be entered.

**Ethernet Type Mask (0x0-0xFFFF):** Enter the Ethernet type mask hexadecimal value. The value is between 0x0 and 0xFFFF. When any Ethernet type profile is selected in the **Specify Ethernet Type** drop-down list, the appropriate hexadecimal value will automatically be entered.

**CoS:** Select the CoS value used. This value is between **0** and **7**.

**VID (1-4094):** Enter the VLAN ID that will be associated with this ACL rule. The value should be between 1 and 4094.

Time Range: Enter the time range.

Action: Select the action that this rule will take. The values are Permit and Deny.

Click the **Back** button to return to the previous window.

Click the **Next** button to continue.

To define the IPv4 ACL: Select IPv4 and then click the Next button. Click the associated tabs with IPv4 Address, Port, IPv4 DSCP and TCP Flag, the following page will appear:

constitut Antigenent >>	Select Pathol	Type => AALS	alle >> Apply Port			
kana antiga o sequence o	ander to pro-	da é neve roke.		Autor		
Gegarron No. (1-85525) obcer Trev		TOP			50. Pisaniwa	
nesso rulo criteria						
IPvi Address	Pe	et	and DISCH	TOP Hag	2	
Time Hange	112734		111			
Vetter.	+ Parts	i Den				

Figure 4.122 – ACL > ACL Configuration Wizard – Create IPv4 ACL

Sequence No. (1-65535): Select and enter the ACL rule number. This value must be between 1 and 65535. Select Auto Assign to automatically generate an ACL rule number for this entry. Protocol Type: Select the protocol type option. Options to choose from are TCP, UDP, ICMP, EIGRP, ESP, GRE, IGMP, OSPF, PIM, VRRP, IP-in-IP, PCP, Protocol ID, and None.

After selecting the **TCP** option as the **Protocol Type** then Click the associated tabs with **IPv4 Address**, **Port**, **IPv4 DSCP** and **TCP Flag**, the following page will appear:

Interingen     Interingen <th>ene antique a nomenica reas Generativa filo (1-40522)</th> <th>liver to conside a new ride.</th> <th>DAM</th> <th>estign.</th> <th></th> <th></th>	ene antique a nomenica reas Generativa filo (1-40522)	liver to conside a new ride.	DAM	estign.		
Hyper Ammenda   Baser a   Baser a   Baser a   Baser a   Destanders Port   Person Salert		TCP	100		00.000	Fragments
Not Ammend   Not   Net   Net <th>Harriste Letterne</th> <th></th> <th></th> <th></th> <th></th> <th></th>	Harriste Letterne					
Note:   Note:   Prime:	IN Address	Put	IPvt DSCP	TOP Hag		
estimates Per Please Select  Please	ana (Jean Minar		Centrula	a jest		
NA GROP A PF Precedences Place Solicit • Tex CBCP (0+4) CPF Page J and C Re C path C ref. C ref. C wg			11			
Time Range	laon a Port	Please Select •			H.	a entrata

Figure 4.123 – ACL > ACL Configuration Wizard – Create IPv4 ACL-TCP

Destination: Select the destination information. The values are Any, Host and IP.

**Source Port:** Select the source port value.

Destination Port: Select the destination port value.

IP Precedence: Select the IP precedence value. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).

ToS: Specify the Type-of-Service (ToS) value that will be used. Options to choose from are 0 (normal), 1 (min-monetary-cost), 2 (max-reliability), 3, 4 (max-throughput), 5, 6, 7, 8 (min-delay), 9, 10, 11, 12, 13, 14, and 15.

DSCP (0-63): Enter the DSCP value. And the range is between 0 and 63.

**TCP Flag:** Select the appropriate TCP flag option to include the flag in this rule. Options to choose from are **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are Permit and Deny.

After selecting the **UDP** option as the **Protocol Type** then click the associated tabs with **IPv4 Address**, **Port** and **IPv4 DSCP**, the following page will appear:

constitut Assignment == Se	and Packet Type >> &	At Ball 10 Ap	ale Pert			
(1+22)-140 (1-11)-1555	deat to conside a new o	ik.	Auto Arrag			
otorii Tale	UDP -		•	11/0-15	ti i frigmens	
esiágis role collecta						
Shit Address	Pat	-	A DISCH			
Put Address						
=. Avy				Ary		
Citizet .				Orest		
State OF		11	Dephysion	OF. 10		
Wikdcast	19			Veidante		
Part Depart Foll	Please Select	•12				
September 1			22/22	1977	100	
	Phone Labol	•	0-615	135 Press Taker		
Contration Patt.	Please Select	•				
	Please Select	*£	/D-855	1958 Player Salest	• F	0-65125
Pyt05CP			-			
# P Precelance	Please Select	• <u>30</u>	Please Salett	•		
DICK 0-43	Harve Serect	•	-			
Tirre Hange	11 mars -	61				

Figure 4.124 – ACL > ACL Configuration Wizard – Create IPv4 ACL-UDP

Destination: Select the destination information. The values are Any, Host and IP.

Source Port: Select the source port value.

Destination Port: Select the destination port value.

IP Precedence: Select the IP precedence value. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).

**ToS:** Specify the Type-of-Service (**ToS**) value that will be used. Options to choose from are **0** (normal), **1** (min-monetary-cost), **2** (max-reliability), **3**, **4** (max-throughput), **5**, **6**, **7**, **8** (min-delay), **9**, **10**, **11**, **12**, **13**, **14**, and **15**.

DSCP (0-63): Enter the DSCP value. And the range is between 0 and 63.

**TCP Flag:** Select the appropriate TCP flag option to include the flag in this rule. Options to choose from are **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**.

**Time Range:** Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting the **ICMP** option as the **Protocol Type** then click the associated tabs with **IPv4 Address**, **ICMP** and **IPv4 DSCP**, the following page will appear:

L Configura	tion Wisard		_		
C. Configuration I					
ACCESS LINE ANNU	personal via Sela	at Packet Type >	-	E >> Apady Port	
Name analysis a b	the second s	no to create a net	w rialm.	C Ada Ar	
Promote Type		KMP	ř.		19-2550 Pragmenta
Antipo cale coltar					
E'vi Ashis	-	KMP		Bive DSCP	
Root Address	a hey i tool of of of of of of of of of of	Please Select		Destruto	# Any C Head # Without
STAP Manuage			T	Manhage Come (5-204	
PM DSEP + IF Precessor C DECF dives		Please Select	•	Test Please Sele	in •
Tene Bange Autori		e Panal Col		Ъř	Fact land

Figure 4.125 – ACL > ACL Configuration Wizard – Create IPv4 ACL-ICMP

Destination: Select the destination information. The values are Any, Host and IP.

IP Precedence: Select the IP precedence value. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).

ToS: Select the Type-of-Service (ToS) value that will be used. Options to choose from are 0 (normal), 1 (min-monetary-cost), 2 (max-reliability), 3, 4 (max-throughput), 5, 6, 7, 8 (min-delay), 9, 10, 11, 12, 13, 14, and 15.

**DSCP (0-63):** Select the DSCP value. And the range is between 0 and 63.

Specify ICMP Message Type: Specify the ICMP message type.

**ICMP Message Type (0-255):** When the **ICMP Message Type** is not selected, enter the ICMP Message Type numerical value used. When the **ICMP Message Type** is selected, this numerical value will automatically be entered.

**Message Code (0-255):** When the **ICMP Message Type** is not selected, enter the Message Code numerical value used. When the **ICMP Message Type** is selected, this numerical value will automatically be entered. **Time Range:** Enter the time range.

Action: Specify the action for the rule. The values are Permit and Deny.

After selecting the **EIGRP** option as the **Protocol Type** then click the associated tabs with **IPv4 Address** and **IPv4 DSCP**, the following page will appear:.

Cantigeration										
cores-Lini Asso	general >> Sol	nd Packet Type -	ANT	ite >> Appe	y Port					
Conguerra Ita		der to create a be	windo.		C Adv Holige	с				
and here		(2004)	P		• [80		di-25% 🗇 Foquetti			
	-									
Evi Add		Pvi ISCF	-							
District	A Ary Post Post Wellow			ţ	Destrutue	k Ann C Hand C P MAG and				
BV4 DSCP										
A IP Presedu		Please Salect		CT16	Please Select.					
COCP (D.K		These Select			1	10				
Tena Harga Alber		* Peret	iere -					back	-11-	tiest.

Figure 4.126 - ACL > ACL Configuration Wizard - Create IPv4 ACL-EIGRP

Destination: Select the destination information. The values are Any, Host and IP.

Fragments: Specify the Fragments option to include packet fragment filtering.

Source: Select the source information. The values are Any, Host and IP.

Destination: Select the destination information. The values are Any, Host and IP.

IP Precedence: Select the IP precedence value. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).

ToS: Select the Type-of-Service (ToS) value that will be used. Options to choose from are 0 (normal), 1 (min-monetary-cost), 2 (max-reliability), 3, 4 (max-throughput), 5, 6, 7, 8 (min-delay), 9, 10, 11, 12, 13, 14, and 15.

**DSCP (0-63):** Select the DSCP value. And the range is between 0 and 63.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting the **ESP** option as the **Protocol Type** then click the associated tabs with **IPv4 Address**, and **IPv4 DSCP**, the following page will appear:

inite preservable.		
10 a contractor	(), Auto-Assage	
ESP.	• (10	(P-240) 11 Frighteette
1 DSCP		
	Decimation Decim	
	The second second	
· Jami · · · · ·		
	( Seed. • ) To: • To:: • )	Estend •) The Preset Select •

Figure 4.127 – ACL > ACL Configuration Wizard – Create IPv4 ACL-ESP

Destination: Select the destination information. The values are Any, Host and IP.

IP Precedence: Select the IP precedence value. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).

ToS: Select the Type-of-Service (ToS) value that will be used. Options to choose from are 0 (normal), 1 (min-monetary-cost), 2 (max-reliability), 3, 4 (max-throughput), 5, 6, 7, 8 (min-delay), 9, 10, 11, 12, 13, 14, and 15.

DSCP (0-63): Select the DSCP value. And the range is between 0 and 63.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting the **GRE** option as the **Protocol Type** then click the associated tabs with **IPv4 Address**, and **IPv4 DSCP**, the following page will appear:

L Configuration Worme	1		C TANK ON A DATA OF THE OWNER OF
3. Configeration Wicerst			
Access 4.00 Annument >> Sele	of Parket Type >> Add thile >= 1	Apply: Port	
Nume and a support of sum E. Datasets No. D. (1925)	ant to conside a new role.	D Adv Acres	
Pottoni Tgie	GRE	. [47	(0-255 () Pregnam
Analysi rule unline to			
EVI Albitess	PHIDSCP		
Bona () m Bona () m Webcart		Sectories (	Any Final P Wildcard
#54350P			
President	Please Select + Th	Please Select .	]
DECE di-Ka	Pears Select .		1
Test Parge	17:549		
Alber	e Pentil C Dely		
			Back Next

Figure 4.128 – ACL > ACL Configuration Wizard – Create IPv4 ACL-GRE

Fragments: Select the Fragments option to include packet fragment filtering.

Source: Select the source information. The values are Any, Host and IP.

**Destination:** Select the destination information. The values are **Any**, **Host** and **IP**.

IP Precedence: Select the IP precedence value. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).

ToS: Specify the Type-of-Service (ToS) value that will be used. Options to choose from are 0 (normal), 1 (min-monetary-cost), 2 (max-reliability), 3, 4 (max-throughput), 5, 6, 7, 8 (min-delay), 9, 10, 11, 12, 13, 14, and 15.

**DSCP (0-63):** Select the DSCP value. And the range is between 0 and 63.

**Time Range:** Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting the **IGMP** option as the **Protocol Type** then click the associated tabs with **IPv4 Address**, and **IPv4 DSCP**, the following page will appear:

Configuration Weard						
2258 List Assignment >> Se	list Packel	type >> And the	RE >> Apply P	urt		
Sequence Tax, 11-PTSTS	ndwar too carwaad	e a neve rubi.	a (1100)	C Material	N.	
mus Type		IOMP		• 2		(5-295) []) Fragmants
enige role criterio						
Pol Astress	SP-4.05	OP .				
Events States				Dectrutor	- 8 Mile - 1944 - 197 - 197	×
PVI DSDI						
* Precession	Please S	elect •	790	Nexue Select		
	Peak S	••••	3		1	
0.0007/0403			-			
C DOLF (I-63)	TH-max					

Figure 4.129 – ACL > ACL Configuration Wizard – Create IPv4 ACL-IGMP

Source: Select the source information. The values are Any, Host and IP.

Destination: Select the destination information. The values are Any, Host and IP.

IP Precedence: Select the IP precedence value. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).

ToS: Specify the Type-of-Service (ToS) value that will be used. Options to choose from are 0 (normal), 1 (min-monetary-cost), 2 (max-reliability), 3, 4 (max-throughput), 5, 6, 7, 8 (min-delay), 9, 10, 11, 12, 13, 14, and 15.

DSCP (0-63): Select the DSCP value. And the range is between 0 and 63.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting the **OSPF** option as the **Protocol Type** then click the associated tabs with **IPv4 Address**, and **IPv4 DSCP**, the following page will appear:

1. Carfiguration V	eres .					
constant Anny	retard >> Sela	ct Partiest Type => Add	Balle >> Apply 4	Port		
nan andar a n Esparantia		er to croate a new rok	6	Databilit		
uture Type		OBPE		100		(0.25% [] Pragments
segmente como						
SVI AAA	-	Pvi DSCP				
Put Assess	e An Unital Unital Mescari			Cestimiter	in Any () Pesal () P Webcart	-
Evilosce = F Frankes DACE (3-43)		Please Select	15 TH	Please Select	•	
Tirm Range Action		Penal Colory			1	Each Next

Figure 4.130 - ACL > ACL Configuration Wizard - Create IPv4 ACL-OSPF

Source: Select the source information. The values are Any, Host and IP.

Destination: Select the destination information. The values are Any, Host and IP.

IP Precedence: Select the IP precedence value. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).

**ToS:** Specify the Type-of-Service (**ToS**) value that will be used. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.

**DSCP (0-63):** Select the DSCP value. And the range is between 0 and 63.

**Time Range:** Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting the **PIM** option as the **Protocol Type** then click the associated tabs with **IPv4 Address**, and **IPv4 DSCP**, the following page will appear:

Nears and a superior set	lest to create a new rule.		C Alth Arright			
e localere ou crierano	PM		4 101	a	(8-205 () Pagnete	
Antibac role collects	19.0		1.12			
Evil Address	PV4 DSCP					
Pvi Addana						
(a. Any-				1.40		
State Unit			Destination	() said		
1000 C	1			04		
Weekand	-	-		With and		
Peter						
-A: IP Precedental	Please Select	366	Please Select			
( DECPORES	Pare Solid .					
Toric Ronge	Columnal .					

Figure 4.131 – ACL > ACL Configuration Wizard – Create IPv4 ACL-PIM

Fragments: Select the Fragments option to include packet fragment filtering.

Source: Select the source information. The values are Any, Host and IP.

Destination: Select the destination information. The values are Any, Host and IP.

IP Precedence: Select the IP precedence value used. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).

ToS: Select the Type-of-Service (ToS) value that will be used. Options to choose from are 0 (normal), 1 (min-monetary-cost), 2 (max-reliability), 3, 4 (max-throughput), 5, 6, 7, 8 (min-delay), 9, 10, 11, 12, 13, 14, and 15.

DSCP (0-63): Select the DSCP value. And the range is between 0 and 63.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting the **VRRP** option as the **Protocol Type** then click the associated tabs with **IPv4 Address**, and **IPv4 DSCP**, the following page will appear:

CL Configuration We	ani -							
Access List Assigns	wat too Said	ect Packati Ty	pe >> Add flui	(>> Apply	Purt			
Norme ortologie in series 		ien to create	a reny rule.		0.000.0000	e.		
Protocal Type		D.	VRRP		112		(0-255) [] Fiagrants	
Anorga role criteria								
Pvi Address		IPv4 DSc	a a					
811 m	a Any Head P Without				Dectrolos	a Anj O Holt O P Without		
INTERN								
· Photosom		Please Se Please Se	• t • ]	794	Please Select			
Tere Kanpe Adam		+ Fortal	D-Deve				Rack Root	

Figure 4.132 – ACL > ACL Configuration Wizard – Create IPv4 ACL-VRRP

Source: Select the source information. The values are Any, Host and IP.

Destination: Select the destination information. The values are Any, Host and IP.

IP Precedence: Select the IP precedence value. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).

ToS: Select the Type-of-Service (ToS) value that will be used. Options to choose from are 0 (normal), 1 (min-monetary-cost), 2 (max-reliability), 3, 4 (max-throughput), 5, 6, 7, 8 (min-delay), 9, 10, 11, 12, 13, 14, and 15.

DSCP (0-63): Select the DSCP value. And the range is between 0 and 63.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are Permit and Deny.

After selecting the **IP-in-IP** option as the **Protocol Type** then click the associated tabs with **IPv4 Address**, and **IPv4 DSCP**, the following page will appear:

ess Lint Ausign	10073-50	oct Packet 14	pe >> juit the	e >> Axely	Part			
ave orthigt o yes		Ger to create a	e norw robs."					
Despense No. /	40220		1246				di 200 () Yogeneti	
ALC: TYPE		19	NWP:	~	• 14	- 0	To sea Change	
star rule criteri	97							
Puthikes	•	84650	•					
free at a	= Any Honi (P Weican				Destrutio	× W¥ ⊖ Hoff ⊖ JF WEILM		
PHEDROP		Production for Local						
* PPiecedence	·~ 3	Please Sel	• 19	The (	Please Select			
D007 (3-61)		Titere Ser	- ·					
Trea Ballyr		Et clinet.		-10				
		a Fared	127	_				

Figure 4.133 - ACL > ACL Configuration Wizard - Create IPv4 ACL-IP in IP

Source: Select the source information. The values are Any, Host and IP.

Destination: Select the destination information. The values are Any, Host and IP.

IP Precedence: Select the IP precedence value. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).

**ToS:** Select the Type-of-Service (**ToS**) value that will be used. Options to choose from are **0 (normal)**, **1 (min-monetary-cost)**, **2 (max-reliability)**, **3**, **4 (max-throughput)**, **5**, **6**, **7**, **8 (min-delay)**, **9**, **10**, **11**, **12**, **13**, **14**, and **15**.

**DSCP (0-63):** Select the DSCP value. And the range is between 0 and 63.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting the PCP option as the Protocol Type then click the associated tabs with IPv4 Address, and IPv4 DSCP, the following page will appear:

None annigs a requester ward 6. Deservice fris (1-85522)	or to create a s	ew tubi.		C Auto Annes	(	10-200 😳 Pageante	
Tentanot Type	PCI	2	1	• 100			
Anongo culto contacta							
Put Akkness	PHIDSOP						
Styl Address							
* Ary					a Are		
tours Off			-	Destination	See	in the second se	
WARAN					Witten av		
	111						
#v4.DHCP							
+ If Protatence	Please Belect	•	Tat	Please Salact			
2000P-0-612	Hance Sainer			1	_		
Time Hange:	Cit Hart						
Taure standar	The Parameter State of Street, Street, St.	Darts					

Figure 4.134 – ACL > ACL Configuration Wizard – Create IPv4 ACL-PCP

Fragments: Select the Fragments option to include packet fragment filtering.

Source: Select the source information. The values are Any, Host and IP.

Destination: Select the destination information. The values are Any, Host and IP.

IP Precedence: Select the IP precedence value. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).

ToS: Select the Type-of-Service (ToS) value that will be used. Options to choose from are 0 (normal), 1 (min-monetary-cost), 2 (max-reliability), 3, 4 (max-throughput), 5, 6, 7, 8 (min-delay), 9, 10, 11, 12, 13, 14, and 15.

**DSCP (0-63):** Select the DSCP value. And the range is between 0 and 63.

**Time Range:** Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting the **Protocol ID** option as the **Protocol Type** then click the associated tabs with **IPv4 Address**, and **IPv4 DSCP**, the following page will appear:

comp.Cot Analgam	nat 20 Salad	Pariet Type >> 1	LAST TARE >+ Ave	de Port		
Norman annikari a sangar 9 Disbustera 740 (1-8	nea narda			C.Adl.Ang	e	
vature Tale		Protecto	(10)			(3-201) 📋 Pragnette
esilgerrole collecto						
IN Address		PV4 DSCP	13			
(1999) (1999)	Any Invet (F Whiteed			Destrution	n Arg   - 1993)   - 19   - 19   - 19	
PHOSEP						
BICF (1-52	125	Phone Select	• 100	Please Select	•	
Tire Rauge		Panel Cite	N			

Figure 4.135 – ACL > ACL Configuration Wizard – Create IPv4 ACL-Protocol ID

Source: Select the source information. The values are Any, Host and IP.

Destination: Select the destination information. The values are Any, Host and IP.

IP Precedence: Select the IP precedence value used. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).

**ToS:** Select the Type-of-Service (**ToS**) value that will be used. Options to choose from are **0** (normal), **1** (min-monetary-cost), **2** (max-reliability), **3**, **4** (max-throughput), **5**, **6**, **7**, **8** (min-delay), **9**, **10**, **11**, **12**, **13**, **14**, and **15**.

DSCP (0-63): Select the DSCP value. And the range is between 0 and 63.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting the **None** option as the **Protocol Type** then click the associated tabs with **IPv4 Address**, and **IPv4 DSCP**, the following page will appear:

. Centigeration	Antonia							
const.List Ass	ganent >> Sal	nct Packet Type 77	Add Hule >>	Apply Port				
nana analysian Sagorena Mo		toer the creating a lower	vrule.		ALAN ANNUAL			
totic al Type		None					(10-255) [] Fragments	
laster relation	rha							
-	ess	EVERAL PARTY	1					
Pol Addens	n Ara U stand U Without			c	estration -	e Avy O thead O # 		
IPH OSCP			• 1	2	ece Gefect			
DISCRIGATION		Please Select			910 D#90			
Time Range Action		A-Perrol - O D						

Figure 4.136 - ACL > ACL Configuration Wizard - Create IPv4 ACL-None

Source: Select the source information. The values are Any, Host and IP.

Destination: Select the destination information. The values are Any, Host and IP.

IP Precedence: Select the IP precedence value. Options to choose from are 0 (routine), 1 (priority), 2, (immediate), 3 (flash), 4 (flash-override), 5 (critical), 6 (internet), and 7 (network).

**ToS:** Select the Type-of-Service (**ToS**) value that will be used. Options to choose from are **0** (normal), **1** (min-monetary-cost), **2** (max-reliability), **3**, **4** (max-throughput), **5**, **6**, **7**, **8** (min-delay), **9**, **10**, **11**, **12**, **13**, **14**, and **15**.

**DSCP (0-63):** Select the DSCP value. And the range is between 0 and 63.

**Time Range:** Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

Click the **Back** button to return to the previous window.

Click the **Next** button to continue.

To define the IPv6 ACL: Select IPv6 and then click the Next button. Selecting the TCP option as the Protocol Type then click the associated tabs with IPv6 Address, Port, IPv6 DSCP, TCP Flag and Flow Label, the following page will appear:

S ACCOUNT ON A D	10				Contraction of the local states
beauerine has in 455352	daine -	Auto Annage	11		
robust Tays	TCP		0.250	Fragments	
longe role criteria					
Puli Astron	Port	PHILISCP	SCP Fina	Flow Labor	
Pv6 Address					
= hty			e.80		
toans - Host	1 https://www.	Decision			
0.044			D PMC		
Portici,	imph:		Petitegh		
Part					
Same Pad	Please Select +				
and the Law	the state of the s				
	Figure Induct	ili eca	10 Provid Still		
Demains Pat	Flease Select •				
	Plane Select	30.415	ID Oven Delect		0.01230
\$VEDSCP					
DECP 的书法	Plazas Select •				
TCP Float					
2.48 U.M. 1734	1 S.M. S.M. S.	149			
Three Latter					
Flow Label UP-10488(PS)	1				
The Hange	Downey	10			
Actor	· Parat Dew				
					Bark I News

Figure 4.137 – ACL > ACL Configuration Wizard – Create IPv6 ACL-TCP

Source Port: Select the source port value.

Destination Port: Select the destination port value.

IPv6 DSCP (0-63): Select the DSCP value. And the range is between 0 and 63.

**TCP Flag:** Tick the appropriate TCP flag option to include the flag in this rule. Options to choose from are **ack**, **fin**, **psh**, **rst**, **syn**, and **urg**.

Flow Label (0-1048575): Enter the flow label value. This value must be between 0 and 1048575.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting the **UDP** option as the **Protocol Type** then click the associated tabs with **IPv6 Address**, **Port**, **IPv6 DSCP** and **Flow Label**, the following page will appear:

1
10.415.20

Figure 4.138 – ACL > ACL Configuration Wizard – Create IPv6 ACL-UDP

Source Port: Select the source port value.

**Destination Port:** Select the destination port value.

Source: Select the source information. The values are Any, Host and IP.

Destination: Select the destination information. The values are Any, Host and IP.

**DSCP (0-63):** Select the DSCP value. And the range is between 0 and 63.

Flow Label (0-1048575): Enter the flow label value. This value must be between 0 and 1048575.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting the ICMP option as the **Protocol Type** then click the associated tabs with **IPv6 Address**, **ICMP**, **IPv6 DSCP** and **Flow Label**, the following page will appear:

Contigacities Weard						
ourse-Lini Assignment => Selo	ct Packet Type >>					
ener steigt a nepersce surd-	er to create a new	rom.				
Segment No. (1-82520)			AND Assign			
othics Figure	<b>ICMP</b>	•	1	6-255 Prigri	1 Progenerate	
antiga rodo crittorio						
BNS Address	KMP	IFV6 DSCP	Revised			
Pvi Address						
= A10			- A14			
THEFT.	1000		Destrution			
200			1.00			
Pretto Le	ngih	1	Pter	be provide the first of the second		
KENIP -						
2755 (A. 1997) - 1997 (A. 1997)	Please Select					
The second second second second second	Plague Select					
Specify CMP Malorapi Tele	Plasse Select		na 206 📋			
Specify CMP Malorapi Tele	Plaque Select		10-206 [			
Eperate CMP Matchings Teles (CMP Message Type (C-255) (MATCHING) COCP (2-53)	Please Select		10.29% [			
Saesty CMP Makeupi Teler CMP Message Type (5:200) IPMERICP		Mansage Cra	-10.29% [			
Sanche C.M.P. Materiage Train C.M.P. Mansage Train (2015) ENGESCH DOCP (2015) Here Label		Mansage Cra	- 10 27% [			
Early CMP Matrice Tex CMP Message Type (3.255) PMESCP DOCP (3-53)		Mansage Cra	- 10 2750 [			
Taxish CMP Matriage Teles CMP Manage Tele (3-200) EVELOCH DOCH (3-63) They Laber (3-1340075)	Please Select	Mansage Cra	+ 00 2795 [			
Eperaty CMP Materiage Teles CMP Message Type (2010) EVALUESCP COCP (2-C3) EVALUESC		• ) • • • • • • • • • • • • • • • • • •	- 10 29%			

Figure 4.139– ACL > ACL Configuration Wizard – Create IPv6 ACL-ICMP

**Destination:** Select the destination information. The values are **Any**, **Host** and **IP**.

DSCP (0-63): Select the DSCP value. And the range is between 0 and 63.

Flow Label (0-1048575): Enter the flow label value. This value must be between 0 and 1048575.

Specify ICMP Message Type: Select the ICMP message type used.

**ICMP Message Type (0-255):** When the **ICMP Message Type** is not selected, enter the ICMP Message Type numerical value. When the **ICMP Message Type** is selected, this numerical value will automatically be entered.

**Message Code (0-255):** When the **ICMP Message Type** is not selected, enter the Message Code numerical value. When the **ICMP Message Type** is selected, this numerical value will automatically be entered. **Time Range:** Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting the **Protocol ID** option as the **Protocol Type** then click the associated tabs with **IPv6 Address**, **IPv6 DSCP** and **Flow Label**, the following page will appear:

Contigeration Witcent						
cores (ini Ansignment		at this Apply Port				
inne onlige e noporee n - Desarres No. († 1955)	andian to create a never		Add Across			
uttool figer	Protecto	0 •		(D-25% (_) P	agrants	
insign role arthretis						
Eve Address	Predsch	Rese Cabel				
Bed Address Sector (control Pedia	r Langh		Declevation	in Any Lines Ind Patricingh	11 12	
#MI05CP DISCP (8-03)	Peace Serect	•				
Non Label From Label (17348575)						
	MINARY.	1.1				

Figure 4.140 – ACL > ACL Configuration Wizard – Create IPv6 ACL-Protocol ID

Destination: Select the destination information. The values are Any, Host and IP.

DSCP (0-63): Enter the DSCP value. And the range is between 0 and 63.

Flow Label (0-1048575): Enter the flow label value. This value must be between 0 and 1048575.

Action: Select the action for the rule. The values are Permit and Deny.

After selecting the **ESP** option as the **Protocol Type** then click the associated tabs with **IPv6 Address**, **IPv6 DSCP** and **Flow Label**, the following page will appear:

Act, Configuration Wig	ing:	_	_	_				Contraction of the second second	10.60
AG Configentian Woard									
Access Ltd Assegnment => 1	Select Packs	e Type >>		e Apply in	11				
<ul> <li>Debaines No. (1-61525)</li> </ul>					C Add A	verigh.			
Pressol Type		(ESP +)		80		(6-25% :// Pragments			
Anternale otherta									
246 Address	Pv61	DECE		OperLat	èt :				
Tana Hanga Albah	8.Park	A Obs	*	H				Back I weet	

Figure 4.141 – ACL > ACL Configuration Wizard – Create IPv6 ACL-ESP

Source: Select the source information. The values are Any, Host and IP.

Destination: Select the destination information. The values are Any, Host and IP.

DSCP (0-63): Enter the DSCP value. And the range is between 0 and 63.

Flow Label (0-1048575): Enter the flow label value. This value must be between 0 and 1048575.

Time Range: Enter the time range.

Action: Select the action for the rule. The values are Permit and Deny.

After selecting the **PCP** option as the **Protocol Type** then click the associated tabs with **IPv6 Address**, **IPv6 DSCP** and **Flow Label**, the following page will appear:

Configuration Wound						
cons List Anigement 74 Selec	t Packet Tab	e >> <u>Add Tad</u>	++ Apply Par			
kano analyn a negalece metho E Begarros No. (1.99535)	e to coeste e	oww.cule.	_	Antonia		
interactive	PC	P.		100	(8-250 C) Fogniett	
landen mille collecte						
EVG ARATES	Prédisch		Here Lake	1 I I		
Put Astron		2.1			1. A.V.	
State Other Other Fably				Destroiter	interest interest Prefix Langh	
Seate Othe				Destrutor	in i	
Sease Orig Francisco President		a •)[		Destrotan	in i	
Baste Orid Politicae Politicae		a •) [		Destrution	in i	

Figure 4.142 – ACL > ACL Configuration Wizard – Create IPv6 ACL-PCP

Destination: Select the destination information. The values are Any, Host and IP.

DSCP (0-63): Enter the DSCP value. And the range is between 0 and 63.

Flow Label (0-1048575): Enter the flow label value. This value must be between 0 and 1048575. Time Range: Enter the time range.

Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting the SCTP option as the **Protocol Type** then click the associated tabs with **IPv6 Address**, **IPv6 DSCP** and **Flow Label**, the following page will appear:

ses and a sequence out	der ta crastic a nese cale.			
Exqueres No. (1-00532)	in a second	- Auto Arteige	IS-253 () Program	
ED-LAT THEM	SCTP .	• (132	(0-250) (_] Gagman	**
enger rules colleges				
ENS AND FES	INSUSCI!	Flow Label		
Prel Address	1.000			
			10.104	
OWNE	299.9		(Chief)	
David UPM-	1. A. 1999 A. 1	Deuterate	The Carlos Carlo	
Pottel	angh .		Prefectoright	
PHODO				
D009 (0-63)	Piesse Select •	- F		
Filme Label				
Film Called (5 1040878)	1			
Torso Ronger	Children .			
	a faired Cally			

Figure 4.143 – ACL > ACL Configuration Wizard – Create IPv6 ACL-SCTP

Source: Select the source information. The values are **Any**, **Host** and **IP**. **Destination:** Select the destination information. The values are **Any**, **Host** and **IP**.

DSCP (0-63): Enter the DSCP value. And the range is between 0 and 63.

Flow Label (0-1048575): Enter the flow label value. This value must be between 0 and 1048575. Action: Select the action for the rule. The values are **Permit** and **Deny**.

After selecting the **None** option as the **Protocol Type** then click the associated tabs with **IPv6 Address**, **IPv6 DSCP** and **Flow Label**, the following page will appear:

L Configuration Wize	ii d	_		The second second second second
2. Crefiguration Witcard				
Access Lint Assignment 72 S	elect Packet Type >> Add But	e >> Apple Pwrt		
· Tenner 141. (1-811.25)	millioned the extension of a source studies.	) (c) Alas A	unge	
emoni Tale	None		SF2550 Pragments	
lassign rule contenta		568ML		
ENE Address	#v60SCP	Filler Labert		
Phi Astron				
4.50			a fee	
bierr.	12.1.	1000	CHear Done L	
C.94	1.000		C Py6	
Pretty	Length		PietuLergh	
#MINCP				
DECK (9-41)	Please Select .			
FlowLabel				
Filme Laber (0-1348575)		_H		
Timu Ranga	Examin			
Adam	a Parent Decy	10		
(All all all all all all all all all all	States Conta			tack have
				CORD. S MINT

Figure 4.144 – ACL > ACL Configuration Wizard – Create IPv6 ACL-None

Source: Select the source information. The values are Any, Host and IP.

Destination: Select the destination information. The values are Any, Host and IP.

DSCP (0-63): Enter the DSCP value. And the range is between 0 and 63.

Flow Label (0-1048575): Enter the flow label value. This value must be between 0 and 1048575. Time Range: Enter the time range.

Action: Select the action for the rule. The values are Permit and Deny.

Click the **Back** button to return to the previous window.

Click the **Next** button to continue.

After clicking the **Next** button, the following page will appear.

ACL Configuration W	1287G	_	_		A COLUMN A COLUMN A COLUMN
M3. Configuration Witcom Access-List Avoignment	o Salari Darket Tana	100 C 100 C 100 C	- Austra Port		
(#91521 +	101109	•	h.	•	Back Apply

Figure 4.145 – ACL > ACL Configuration Wizard – Create IPv6 ACL-Next

From Port / To Port: Select the range of ports to be configured. Direction: Select either In or Out.

Click the **Back** button to return to the previous window. Click the **Apply** button to save your settings.

## ACL > ACL Access List

The ACL Access List page allows you to view and configure the ACL access list settings.

CLACOBEL											
ACLTINY	[At	٠	# \$2(5-14)			G ROL Name	1			find	1
Total Detries										AttA	c1
0	40.44		ACL Type	Start Segments No.	Meg	Caster State	Renati				
1000	ACI_HARTE,	Taut:	Harrive P.A.C.	14	14	Dusted			Edit	Daleta	
1001	ACT_MARKS	Vest	Busines P.A.L.	ing i	- 10 C-	Dealwe			6:st	Delata	
								11	10100 W		10
						0.00	MAR COL	ntar	Clear Court	ter Add Pu	in:
Segur	are No.	Atta	12	Their		Tires Ita	and the second	Contract of the local division of the local			

Figure 4.146 – ACL > ACL Access List

ACL Type: Select the ACL profile type to find. Options to choose from are AII, IP ACL, IPv6 ACL, MAC ACL, and Expert ACL.

**ID** (1-14999): Select and enter ACL ID. The range is between 1 and 14999.

ACL Name: Select and enter ACL name. The name can be up to 32 characters long.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Add ACL** button to create a new ACL profile.

Click the **Clear All Counter** button to clear all the counter information displayed.

Click the **Clear Counter** button to clear the counter information for the rule displayed.

Click the Add Rule button to create an ACL rule for the ACL profile selected.

## ACL > ACL Interface Access Group

The ACL Interface Access Group page allows you to view and configure the ACL interface access group settings.

	e Access Ge										
rin fuet		To Part		Oreston		ubon Add +1	Type IF ACL		ACLINETO		
r61.01		ath1/0/1		8	•	Add +	IF ACL	•		Please Select	Apply
	These	1						and services		····: 197	
	24.62		W AC			PMI ALL		MAC	NG.	Treport Ac	0
	- MOUNT										
	series -										
	OPILIAT -										
	idition :										
	10113/1										
	101104										
	WILDO.										
	101104										
	HERITAR.										
	-481.0115										
	att01/0/11										
	******										

Figure 4.147 – ACL > ACL Interface Access Group

From Port / To Port: Select the range of ports to be configured.

**Direction:** Select the direction.

Action: Select the action to be Add or Delete.

ACL Type: Select the ACL profile type to find. Options to choose from are AII, IP ACL, IPv6 ACL, MAC ACL, and Expert ACL.

ACL Name: Enter ACL name. The name can be up to 32 characters long.

Click the **Apply** button to save your settings.

MINISTANIA SU	(† ) († )		
		ACL Name)	ACL Type
	1000	ACL_Name_Term	READING IP ACL.
	1007	ACL_Norme_Tast2	Standard IP ACL
	1800	AGL_Name_Test1	Etandory P.ACL
	3.001	ACL_NAME_Test2	Etandaril IP ACL
			OK

After clicking the **Please Select** button, the following page will appear.

Figure 4.148 – ACL > ACL Interface Access Group - Select

#### Security > Port Security > Port Security Global Settings

The Port Security Global Settings page allows you to view and configure the port security global settings. 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.

Strates - Drates	Aerty.
10	Restr
e Nu Lant	Paper
	© Erukket + Doublet

Figure 4.149 – Security > Port Security > Port Security Global Settings

Trap Security Trap Settings:

**Trap State:** Select to enable or disable the port security trap of the Switch. Click the **Apply** button to save your settings.

Port Security Trap Rate Settings:

**Trap Rate (0-1000):** Enter the number of traps per second. The range is from 0 to 1000. Click the **Apply** button to save your settings.

Port Security System Settings:

System Maximum Address (1-6656): Enter the maximum number of secure MAC addresses allowed. If not specified, the default value is **No Limit**. The valid range is from 1 to 6656. Tick the **No Limit** checkbox to allow the maximum number of secure MAC addresses.

Click the **Apply** button to save your settings.

#### Security > Port Security > Port Security Port Settings

The Port Security Port Settings page allows you to view and configure the port security port settings of the Switch.

ait Secu	ALC: N	Settings				_	_	_	_
net Recardly	Per Sala								
Trem Pat		To Port.	2549	Mainut (1-8950	Values Artes	Security Marm		Aging Time (D- 1 #40)	April Tex
#85.627	•	• 10/149	Dreatied *	12	Shutsiven +	Delete-so-Tim			Absender • Apply
Sec.	COLUMN ST	STREET, NA	WARRAN ALTER	Westman Court	Security Mode	Anna Sare	Contraction in the	The Ares in	al dance Type
emilian .			Sindowe	1.1	Deste-on-Timesul	Downed.	T	18	Advande
401102	τ.		Diddet	ALC: NO.	Dance on Second	Distant			-maximum at
mint		18	Distant		Deale-les Teseud	Duster.			Appallate
1011/5/5	100	1	Butthes	1 CONTRACTOR 1	Desta of Televisi	Distant		11 (Cal)	Address of the
40100			Buldan		Deate-oryTreamd	Do and			49103.65
antitut.	1		Butchet		Deers-on-Tennid	Disamed .		3	Absorber
amplant	18		Bladoowe		prests-on-trend	Desavet			Ad-potate
sminh/h	7		Distant	1 × 1	Denkis-lefs Treasured	Destel			ADDITION !
0011090	. 9	7.00	Distant	(10) (1)	Dears or Terrind	Deswood		6	AND COLUMN
white the	100	1.1.1	DARMAN	1.1.1	Date of Immed	Design		1	ALL
ammitt.			Duktown	1.8.1	Delete-ol-Timenul	Disastoi		ŧ	Abertale
white a	-	1	SALASSAS	Contraction of the	Dante on Transid	Diamid 1		11000	NUMBER

Figure 4.150 – Security > Port Security > Port Security Port Settings

From Port / To Port: Select the range of ports to be configured.

State: Select to enable or disable the port security state of specified ports.

**Maximum (1-6556):** Enter the maximum number of secure MAC addresses that will be allowed on the specified ports. The value is between 1 and 6656.

Violation Action: Select the violation action that will be taken. The values are Protect, Restrict, and Security Mode: Select the security mode option. The values are Permanent and Delete-on-Timeout. If you select Permanent to under this mode, all learned MAC addresses will not be purged out unless you manually delete those entries. If you select Delete-on-Timeout, all learned MAC addresses will be purged out when an entry is aged out or when you manually delete these entries.

Aging Time (0-1440): Enter the aging time for auto-learned dynamic secured addresses on the specified ports.

Aging Type: Select the aging type. The values are Absolute and Inactivity. Select Absolute so that all the secure addresses on this port age out exactly after the time specified and is removed from the secure address list. This is the default type. Select Inactivity so that the secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period

Click the **Apply** button to save your settings.

#### Security > Port Security > Port Security Address Entries

The Port Security Address Entries page allows you to view, clear and configure the port security address entries.

	the Letters					
here -		MAC ADDRess	WEID-ADDAL			
41.07	+	31-14-10-12-00-00				
				Add	Delete Clear by Port	Cinut by Hild
S: mittel to						Chief All
Port	100	MACARA		C. Antonio Type	Resulting Time I	und .
	1.1.44	89-00-30-88	100.88	Fernansel	1. T	
ARTHON.				Derem on Toronal		

Figure 4.151 – Security > Port Security > Port Security Address Entries

**Port:** Select the port to be configured.

MAC Address: Enter the MAC address for the specified port.

VID (1-4094): Enter the VLAN ID. The range is between 1 and 4094.

Click the **Add** button to add a new entry based on the information entered.

Click the **Delete** button to remove a new entry based on the information entered.

Click the Clear by Port button to clear the information based on the port selected.

Click the Clear by MAC button to clear the information based on the MAC address entered.

Click the **Clear All** button to clear all the information in this table.

Enter a page number and click the Go button to navigate to a specific page when multiple pages exist.

#### Security > DHCP Server Screening > DHCP Server Screening Global Settings

DHCP Server Screening function allows you to restrict the illegal DHCP server by discarding the DHCP service from distrusted ports.

DHCP Server Screening Glob	al Settings		
DHCP Server Screening Chilud Setting			
Trac Itale	[Disative]		Repty
Profile Settings			
Probe Name Chief MAC	in many In the V-Sel Analy		Asstr
Total Entries 12			
Profile Name	ClinicHMC		
Pullichare_list.	00-03-00-03-08-03	Datate	Detete Profile
Fiste, Name, Tetti	00/00/00/00/00-02	Dekte	Datate Profile
		(89)	
Lagitderotion			
Log Buthi Erman (10-1000)	11		Apply Dear Log
Total Extrem 10			
1.00	Server IP	Class MAC	Opparence
	Yakimin arms	1 T M	

Figure 4.152 – Security > DHCP Server Screening > DHCP Server Screening Global Settings

#### **DHCP Server Screening Global Settings:**

Trap State: Select to enable or disable the trap state.

Click the **Apply** button to save your settings.

#### **Profile Settings:**

Profile Name: Enter the profile name.

Client MAC: Enter the MAC address.

Click the **Delete** button to remove the specified entry of the table.

Click the **Delete Profile** button to remove the specified profile.

Click the **Apply** button to save your settings.

Enter a page number and click the **Go** button to navigate to a specific page when multiple pages exist.

## Log Information:

Log Buffer Entries (10-1024): Enter the logged buffer entries. The value is between 10 and 1024.

Click the **Apply** button to save your settings.

Click the **Clear Log** button to clear the log.

#### Security > DHCP Server Screening > DHCP Server Screening Port Settings

The DHCP Server Screening Port Settings page allows you to view and configure the DHCP server screening port settings.

10m Fiel		To Purt		Then	Profestionana		
eth1/0/1	•	ets1/01	•	Enabled +			
lever # e :Pok Address				() the Address	Larris		Apply
Dur		7. III		iener Ø		Yofile Remain	
4811891	D(14	ined.		11 C			Delate
441112	2564	iner I					Delete
4811853	Des	cied .					Delete
STATE	3018	1945					Delete
48/1075	0.54	(dia)					Delate
481100	2144	idet.					Debete
091507	Disc	ntat					Delete
##1000	CHIN	inet.					Delete
48.1829	0.54	med					Defate
aminitie	Ose	ldet .					Delete
0010319	-Dise	1495					Delete
addition 2	Oits	1244					Detete

Figure 4.153 – Security > DHCP Server Screening > DHCP Server Screening Port Settings

From Port / To Port: Select the range of ports to be configured.

State: Select to enable or disable the DHCP server screening port state.

Profile Name: Enter the profile name of specified ports.

Server IP: Select IPv4 Address or IPv6 Address and enter the DHCP server IP.

Click the **Apply** button to save your settings.

#### Security > Safeguard Engine

D-Link's **Safeguard Engine** is a robust and innovative technology that automatically throttles the impact of packet flooding into the switch's CPU. This function helps to protect the DXS-1210 Series Switch from being interrupted by malicious viruses or worm attacks. This option is enabled by default.



Click the **Apply** button to save your settings.

#### Security > Trusted Host

The Trusted Host page allows you to view and configure the trusted host settings.

ended Head				
OLNING DUTIE		7999	Tetret •	Pasty
and the first manacher of	ACC, Kanno Multipe & Infr	1999		
			NOAD COMPANY	
And Entries : 2			ACL Name	
stal Entries : 2				Delete

Figure 4.155 Security > Trusted Host

ACL Name: Specify the ACL name. The name can be up to 32 characters long.

Type: Specify the trusted host type. The options are Telnet, Ping, HTTP and HTTPS.

Click the **Apply** button to save your settings.

#### Security > Traffic Segmentation Settings

This feature provides administrators to limit traffic flow from a single port to a group of ports on a single Switch. This method of segmenting the flow of traffic is similar to using VLANs to limit traffic, but is more restrictive.

afte Segmentation	Seffeque			
eh101 •	TuPat [etht01 *]	From Prevent Part [#b\10/1 *]	Tx Forward Part	Add Delete
_	Fart		Tett	furneral daige Dramann
	4/87/5/1		13	RA/6/1 #R/1/0112
	101101		10	ktast-akmipt2
	101.00		e1	81/0/1-48/1/0/12
	485384		**	e1/8/1-i#11/21/2
	101/01		41	1001-001012
	N81/54		10	E10/1-46(10/212
	() emi1007			1/6/1-etrrr10+2
	147.04			entre-lenters .
	491704			EV01-001012
	etritorite		**	entim vernigit2
	##150215		20	NAMA HENRY 2
				CRIMINAL CRIMINAL

Figure 4.156 – Security > Traffic Segmentation Settings

From Port / To Port: Select the range of ports to be configured.

From Forward Port / To Forward Port: Select the range of forward ports to be configured.

Click the Add button to add a new entry.

Click the **Delete** button to remove an entry based on the information entered.

#### Security > Storm Control Settings

The Storm Control Settings page allows you to view and configure the storm control settings.

irm Control s	and the second se				
turn Castrol Trast	Sattings				
Tradi State	None				Apply
haves Canterol Public	a Settinan				
minnai (5-828)	3	201 Ruban (2-202)	3	an U. Mala	4pp/w
Anno Cantool Flart 1	Settings				
From Figel	TUPLE (shift) •	Tiph Action (Evolution) • Norm	Land 7/p4 87	PS Rue (S-2147423047) P	PD Low (0-21474030471
( worthown )	and the company	There are a compared and the compared of the c	Contraction of the		
					Apple
Tetal Centers 136					
Tatal Entrins : 36 INAT	Marter	Act==	Terrenet /	Center	Apply
Tetal Cettins : 36	Marca	Actor	Thereined /	Center	
Tetal Cettins : 36	Law and	Artes Des	Territed	Center	tim
1	Broadcast (				Size Fre
Tatal Centros 136	Broadcool Material				Name Seattre Inactive
Tatal Centros 136	Broad and Multicast Streeped			-	States Station Institut
Faila Colorian - 36 Post elittezh	Broadt And Anderson Universit Universit	Die		+	Norm Seattre Darties Seattre Seattre
Faila Colorian - 36 Post elittezh	Broadcool Mutteract Broadcool Mutteract Mutteract	Die			Norm Seattlee Inactive Seattlee Seattlee Seattlee
Faila Colorian - 36 Post elittezh	Breadland Maderast United United Maderand Maderand United	Die			Norm Seator Inactor Inactor Inactor Inactor Inactor
reta Centres : 26 PMP eltitizh efficial	Bread off Mathemat Uncentrant Mathemat Uncentrant Uncentrant Development	Cros			Norm Seator Inactor Inactor Inactor Inactor Inactor Inactor Inactor
reta Centres : 26 PMP eltitizh efficial	Bread off Mathemat Uncentrant Uncentrant Mathemat Uncentrant Mathemat	Cros			Name Seattine Inactive Inactive Inactive Inactive Inactive Inactive Inactive Inactive Inactive

Figure 4.157 – Security > Storm Control Settings-PPS

**Trap State:** Select the storm control trap state. The options are **None**, **Storm Occur**, **Storm Clear**, and **Both**. When **None** is selected, no traps will be sent. When **Storm Occur** is selected, a trap notification will be sent when a storm event is detected. When **Storm Clear** is selected, a trap notification will be sent when a storm event is cleared.

Click the **Apply** button to save your settings.

#### **Storm Control Polling Settings:**

**Interval (1-300):** Enter the interval value. The range is from 1 to 300. **Retries (0-360):** Enter the retry value. The range is from 0 to 360. Click the **Apply** button to save your settings.

## Storm Control Port Settings:

From Port / To Port: Select the range of ports to be configured.

Type: Select the type of storm attack. The values are Broadcast, Multicast, and Unicast.

Action: Select the action for the specified ports. The values are None, Shutdown and Drop.

Level Type: Select the level type to be PPS or Kbps. When selected PPS. The PPS Rise & PPS Low will be showed.

**PPS Rise (1-2147483647):** Enter the rise packets per second value. The value is from 1 to 2147483647.

**PPS Low (1-2147483647):** Enter the low packets per second value. The value is from 1 to 2147483647.

onn Control S							
term Careford Trage 5	atings						
Tran Date	Norw	•)					Apply
tern Cartral Policy							
Interval (5-503)	1	and a	Hamas (3.1943)	2	inter (1)	de las	Appla
Anny Caminal Port S	attage						
Fourt Part	To Part	1000	the last state of the	1000 C 1000 C 1000 C 1000 C		Concernance of the	and the second second second second
emid/1 •	(eth:50/1 •	Tee Dradiat	• Actual Nove	+) (Fage	•]		Vasa Apply
		Dradcart	• Name	• (Fage	•] .[		
• h0.inv		Dreadcast	• Nave	(Fage	•) [		Vaple
Total Letters : 30	(##5507 • )	Tee [Breakart	• Nave	•) (F388	•) [	_ rites	Apply
Total Letters : 30	(eth:507 +)	Erraduart	• Nave	•) (Fage Densi	•) [	_rbes	vani Apply Scan
(eth)/C/1 • Total testies (30 Part)	Genston + Stern Promise	Tiger [Dreadcast	• Name	•) (Happ	•) [	Caroof	Apply
(eth)/C/1 • Total testies (30 Part)	(envior) •	Tee [Presideart	• Name	•) (Figs Densi	•) [	Canad	Vitel Apply State Taction
renizin •	Constant Distant Units and Units and Units and	Tee Dradcart	Nave	•) (Fays	•) [	Canad	Vitel Apply Name Itacies Itacies
enizii • Total teenes i 30 Deal aboritii	Constant Disastant Universit Universit Universit	Tee Dradtart	• Nave	•) (Fage Dress)	•) [	Canad	VAH Apply Nactor Nactor Nactor Nactor Nactor Nactor Nactor

Figure 4.158 – Security > Storm Control Settings-Kbps

When select the level type to be **Kbps**, the **Kbps Rise** will be showed, and **Kbps Low** will be disabled. And the column **Current** of Storm Control information table will only show "-".

**Kbps Rise (1-2147483647):** Enter the rise packets per second value. The value is from 1 to 2147483647.

Kbps Low (1-2147483647): The field is un-configured.

Click **Apply** for the settings to take effect.

#### Security > DoS Attack Prevention Settings

The DoS Attack Prevention Settings page allows you to view and configure the Denial-of-Service (DoS) attack prevention settings.

arX Type Selector			
🛃 and – lack	🖻 l lal – lat k	🗹 i 'N I	ICL Musz
≝ TCP SY+ FN	🛃 TOF BIN StoPolt Lets 1024	🛃 Ping of Death (deck	🛃 TOP Thy Plagment Adads
₹ AL -:#-			
SuS Sellinge			
State			
Distbes 🔹 Disp	•		Apple -
Dat Tura			
			Berline.
DaS Type	State		Action
Long office -	Distbiet		Iro:
Long office -	Distbiet		Iro:
Long abay - U M – M K	Distbiot Distbiot		Diro : One
Lond Attack Ust – Isok TOP (101	Distributi President Distributi		Dirol: tan: Dirol:
Loni obsi Hal-hak TiF rul Hill russ	Distbes Distbes Distbes Distbes		Dirok Dirok Dirok Dirok
Londoffacio Historian TOP ful HOL Annas TOP Syn PN	Distbes Poster Distbes Poster Distbes		Dires Dires Dires Dires Dires

Figure 4.159 – Security > DoS Attack Prevention Settings

## **DoS Attack Prevention Settings:**

DoS Type Selection: Tick the DoS type option that will be prevented

State: Select to enable or disable the DoS attack prevention state.

Action: Select the action for the DoS attack.

Click the **Apply** button to save your settings.

## Security > SSL > SSL Global Setting

Secure Sockets Layer (SSL) is a security feature that provides a secure communication path between a Web Management host and the Switch Web UI by using authentication, digital signatures and encryption. These security functions are implemented by Ciphersuite, a security string that determines the cryptographic parameters, encryption algorithms and key sizes.

This page allows you to configure the SSL global state settings.

S. Golial Settings		
10. Disku Ianvice Pattay	- Evalued & Deamed	
Service Pattoy		Apply

Figure 4.160 – Security > SSL > SSL Settings

#### SSL Global Settings:

SSL Status: Select to enable or disable the SSL feature's global status.

Service Policy: Enter service policy name.

Click **Apply** for the settings to take effect.

**NOTE:** When SSL is enabled, it will take longer to open a web page due to encryption. After saving, please wait about 10 seconds for the system summery page to load.

#### Security > SSL > SSL Service Policy

The SSL Service Policy page allows you to view and configure the SSL service policy settings.

100-1-7 W	E-2H		3-50	8-1	1457	1000	
551.	610.	14/1	640	2.1	91	1971	
		_		_	_		_

SI, Service Policy			
Policy Name	[11 rftwo		Add Find
Policy Name	12 met		
Besolon Came Timeout (83-68400) Center Subes	100 # RSA_MALL_MD5 # RSA_NALL_MD5 # RSA_DEE_SHA # RSA_DEE_SHA # DH_RSA_DEE_SHA # DH_RSA_DEE_SHA # RSA_DEP1034_DEE_SHA # RSA_DEP1034_DEE_SHA # RSA_DEP1034_DEE_SHA # RSA_WTH_AEE_128_CBC_DHA # RSA_WTH_AEE_128_CBC_DHA # DHE_RSA_WTH_AEE_128_CBC_U		Apply
TotalEntries : 2			
Total Entries : 2 Folcy Name	Carles Salas	Second Cache Tennet (seco	
	Cather Salans RelativeTH_AES_128_CERC_SHA	Servision Cacher Terrinoist (sinc) 388	Edit

Figure 4.161 – Security > SSL > SSL Service Policy

Policy Name: Enter a policy name for SSL.

Click the **Add** button to save your settings.

Click the Find button to locate a specific entry based on the information entered.

**Session Cache Timeout (60-86400):** Enter the session cache timeout value. The value is between 60 and 86400 seconds.

Cipher Suites: Select the cipher suites that will be associated with this profile.

Click the **Apply** button to save your settings.

#### OAM > Cable Diagnostics

The Cable Diagnostics page is designed primarily for administrators and customer service representatives to examine the copper cable quality. It determines the type of cable errors in the cable.

Select the range of ports and then click the **Test** button to start the diagnosis.

in Dagantice ren Fut	7141				
491631	• (etit	0/12 • )			Test
					Dear Al
Port	Link States	Terri (	uua:	Catilet Longith (M)	
altrifet.	Daven				Cour
18/1/02	14				Cear
##1103	Dive:				Char
1001104	Daven				Cear
serring.	110000				Cear -
491105	(Deer)				Cwar
skrout!	Dawn				Char
1011125	Deen				Car
29/55711	Uterry				Chie
##100113	Daven				Cear

Figure 4.162 – OAM > Cable Diagnostic

Click the **Clear** button to clear all the information for the specific port. Click the **Clear All** button to clear all the information in this table. **\** 

**NOTE:** Cable length detection is available on Gigabit ports only.

**NOTE:** Please be sure that the Power Saving feature is disabled before enabling the Cable Diagnostics function.

## Monitoring > Statistics > Port

This page allows you to display the packet statistics of ports.

•									
on Pot	985-08/1	•	WPod.	eth1/0/	•			P	nd Refresh
		74	_			10.00			
timet 1		Rate:				ltate		Date#	
	Byden ser	picketune	Inches	BB(AUR)	Ballin Same	and an arrest	later.	partiette	
100098	1. E	.0	4	8	10	.4	.0.		Shiw Detail
100.000	1	100 N	1	1	*	1			Show Detail
10/000	F	0	4		0.		0		show Detail
-	10	00	1.	1	4	2	T.		Show Detail
480.045	8.	0	8.		0		0.		show betail
ables	1	18	1	1		1	1		Show Detail
apolat.	F		8.2			1	0	5.815	Shiw Detail
ahton	B		8.5	- 8	0;	1	0	128.7	Show Detail
48/1097	1	0	0.1	. 1	0		11	191	Brow Detail
ARADIE.	1	18	8.2		10.0		:11:	0.000	Show Detail
1000011	1	0			0	1 B.	0		Show Detail
antott	. E	100			0	- 1	.U.	2810	Show Detail

Figure 4.163 – Monitoring > Statistics > Port

From Port / To Port: Select the range of ports to be configured.

Click the **Find** button to locate a specific entry based on the information entered. Click the **Refresh** button to refresh the display table.

After clicking the **Show Detail** button, the following page will appear.

and Based		
urt Duteil		
		Back Refrects
ventroit.		
RS take rate	E tylestrer:	
TTI huma sala	1. Februarie	
ON Tabé Bylen	E.	
TIL Today Bayless	1.	
Pili packet rele	E paristiches.	
To pusched rate	C parinettal	
MM. Total Packatts	Real Provide Landscore and the second s	
Tri Tutsi Femete	h	
for multi-anti-	1	
Rat Brown Add	1.	
RUCHC.etal	1	
ET un partition	1	
AC HEALTH	1	
fit Fagmeri (	E	
Richard and Annual State	B	
PE Manual Cold	1	
RUMPU analasta	1	
Til ancerane dataras	1	
TIT single sulfares	F	
To an a serie collector	13	
Tri lais roleane.	1	

#### Figure 4.164 – Monitoring > Statistics > Port – Show Detail

Click the **Back** button to return to the previous window. Click the **Refresh** button to refresh the display table.

#### Monitoring > Statistics > Port Counters

The Port Counters page allows you to display port counter statistics.

(Castler									
som Poel	etht	. na	ToPut	ath.	14021	•		Find	Petresh
1977	Sector B	WAR AND INCOME.	Witness No.	MALANTAN	041041076	Orthogoall Nate	OutMountiNet	CARLAND AND	_
shirin	10		0	- 11		-0	8	1	Show Errord
4811022	. X.		0	H					show troors
101100	.0.	1. (#)	.0	0	1	0.0	8.	1	Show Errors
4811015		1	#		- 1			1	Shiw Etters
401105		1		8	1		1	1	Show Errica
annint.	0		0	0	1	9	4	1	Show Errors
eth1007	0		10	10	1	\$		- 1	Show Drors
481123.5		( <b>1</b>	18	11:	1	00	8.1	1	Show Errors
4811/09	. 0			0	. 1	0	¥		Shire Errors
101012		11-14-		-11-		0			Show Errora
warden's	T.	1	-16	1	1	. 8	1	1	Show Errors
amount)				W		10		1000 august 100	Show Errors

Figure 4.165 – Monitoring > Statistics > Port Counters

From Port / To Port: Select the range of ports to be configured.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Refresh** button to refresh the display table.

Click the **Show Errors** button to see all error counters of the specific port.

After clicking the **Show Errors** button, the following page will appear.

ten ) tene

Figure 4.166 - Monitoring > Statistics > Port Counters - Show Errors

Click the **Back** button to return to the previous window.

Click the **Refresh** button to refresh the display table.

#### Monitoring > Statistics > Counters

The Counters page allows you to display all port counters, and clear the port counters of the specified or all ports.

and an a						
From Port	eth1.0/1 +	To Port eth1/6/1	•		Fint	Refresh
				1.11	Cear .	Char Al
-	Part	Beckinge				
	EMM	1		Show Detail		
	elect .	1		Show Detail		
-	61/0/3	1		Show Detail		
	1.04	+		Strow Detail		
	EMMIN	1		Show Detail		
	1.15M	1		Show Detail	1	
**	157	1		Show Defail		
	1.5.5	1		Show Detail		
	109			Show Detail		
1	1018	. 8		Show Detail		
	10001	1		Stow Detail		
- 10	HARTS:			Show Cetal		

Figure 4.167 – Monitoring > Statistics > Counters

From Port / To Port: Select the range of ports to be configured.

Click the **Find** button to locate a specific entry based on the information entered.

Click the **Refresh** button to refresh the display table.

Click the Clear button to clear all the information for the specific ports.

Click the **Clear All** button to clear all the information in this table.

Click the Show Detail button to see the detail information of the specific port.

After clicking the Show Detail button, the following page will appear.

Counters Errors		
Exonitara Emara		
		Saca Balwoh
An U.S.T. Doursen Directo		
nHCT-mailim		
WACTOWFOR		
WHCL/NELKIFHTE		
are to a second s		
HHCALBRANE IN		
Introduction Proc.		
(v) COmmitta (APR)		
HICD Ladian Prog.		
(HOOmes	1103346	
WHECHINE	424640	
(WKCPIELLDate:		
HHCPHINITOPOINME:		
www.cPirt28idt50.dels		
NHCP9[2504/0100364;		
HICPHERDATE2DOMS		
Incontrol tables		
WKCPVMS104/2047OrWite		
GHCPAQUARADARDOWN:		
(HICPsHOOds #2780 dwis:		
And the statement		

Figure 4.168 – Monitoring > Statistics > Counters – Show Detail

Click the **Back** button to return to the previous window. Click the **Refresh** button to refresh the display table.

#### Monitoring > Mirror Settings

The Mirror Settings page allows you to view and configure the mirror feature's settings.

. See	nas Marridae		Second States	Searce Parts Rots Sta Ex	Dealiteation Part
Sessae	•				Fed
e Sooren Tablo					
00 B	G [#101	•	[en:0] •	(Bath •	Add Delete
aa (	Furn Part		To Post.		
divated.	E Lesona :	•			
ioun feardar	1	•			
e Settege					

Figure 4.169 – Monitoring > Mirror Settings

Session Number: Select the mirror session number for the entry. Destination: Select the destination port for mirror settings.

Source: Select the range of ports to be the source port and Frame Type to be mirrored.

Click the **Add** button to add the newly configured mirror entry based on the information entered. Click the **Delete** button to delete an existing mirror entry based on the information entered.

Mirror Session Table: Select the Mirror Session Type to be displayed.

Click the **Find** button to locate a specific entry based on the information entered.

#### Green > Power Saving

The Power Saving page allows you to configure the power saving settings of the Switch.

Power Saving Gaultal Settings Power 1	every Souldoese Serlings	
unders Version character Plat analytick Plaser Saving characteric Planers characteric Direction Power Saving characteric Direction Power Saving	200 - Enstand - Onumbed Destand - Destand Destand - Destand	Apple
transfalle DevGD	- Crosted - e Doubled	Apply
Inter Range Suttings Inter Carlos Inter Range	Tirre Kanga	Appry Delete

Figure 4.170 – Green > Power Saving

**Scheduled Port-shutdown Power Saving:** Select to enable or disable applying the power saving by scheduled port shutdown.

**Scheduled Hibernation Power Saving:** Select to enable or disable the scheduled hibernation power saving feature. When this option is enabled, the system will enter into the hibernation mode based on the specified time range profile associated with it. When the system enters the hibernation mode, the switch will go into a low power state and idle. It will shut down all the ports and LEDs, all network function will be disabled. If the Switch is an endpoint type Power Sourcing Equipment (PSE), the Switch will not provide power to the port. **Scheduled Dim-LED Power Saving:** Select to enable or disable applying the power saving by scheduled dimming LEDs.

Administrative Dim-LED: Select to enable or disable the port LED function.

Type: Select the type of power saving. Options to choose from are **Dim-LED** and **Hibernation**.

Time Range: Select the name of the time range to associate with the power saving type.

Click the **Apply** button to save your settings for each individual section.

Click the **Delete** button to remove the specified entry.

Power Saving Glub	d Settinge Pok	our Soving Statione Settings			
NeiniPat.	Torrie.	Title Runge			
alf:501 +	#016/12: *	Itinas it			Apply
_	Diet		i Forge		-
	entrant.			Delata	
	am169			Deinte	
	a#i1003			Debrte	
	##1173W			Delote	
	.atmos			Dekita	
	2011194			Delote	
	4811137			DeWte	
	1 101110/0			Delete	
	8811099			Delete	
	#1157.8			Detute	
	#81/011			Delote	
	#511013			Delete	

After clicking the Power Saving Shutdown Settings tab, the following page will appear.

Figure 4.171 – Green > Power Saving – Shutdown Settings

From Port / To Port: Select the range of ports to be configured.

Time Range: Enter the time range to associate with the specified ports.

Click the **Apply** button to save your settings.

#### Green > EEE

The Energy Efficient Ethernet (EEE) is defined in IEEE 802.3az. It is designed to reduce the energy consumption of a link when no packets are being sent.

TT: Seffeyn		
Tipes Patt eth10/1 +	76766 their en10/12 • Evelow •	Acch
	Per l	State
	white	Chinding
	10101	Getaalwa
	-m1/b0	Creative
	am1/04	Dosawa
	-en/dds	Drywlawdt
	#1108	Chaster
	am1/9/	Crowwe
		Cleanet
	401/09	Crisewe
	venioro.	Develop
	att:1011	Coster
1	an/10/(2	Cristian

Figure 4.172 – Green > EEE

From Port / To Port: Select the range of ports to be configured. State: Select to enable or disable the EEE feature.

Click the **Apply** button to save your settings.

# **5** Command Line Interface

The D-Link DXS-1210 Series Switch allows a computer or terminal to perform some basic monitoring and configuration tasks by using the Command Line Interface (CLI) via TELNET protocol.

# To connect a switch via TELNET:

1. Make sure the network connection between the switch and PC is active.

To connect, launch any terminal software like *HyperTerminal* in Microsoft Windows, or just use the command prompt by typing the command *telnet* followed by the switch IP address, e.g., *telnet 10.90.90.90*.
 The logon prompt will appear.

## Logging on to the Command Line Interface:

Enter your User Name and Password to log on. The default user name and password are empty. Note that the user name and password are case-sensitive. Press **Enter** in both the Username and Password fields. The command prompt will appear as shown below **(DXS-1210-12TC>)**:

DXS-1210-12TC login: Password:

DXS-1210-12TC>

Figure 5.1 – Command Prompt

The user session is automatically terminated if idle for the login timeout period. The default login timeout period is 5 minutes. To change the login timeout session, please refer to chapter 5.

## CLI Commands:

The Basic Switch commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command Syntax	Description of Usage
?	The ? Displays a list of CLI commands on the device.
config ipif <short <1-4094="">&gt; { ipaddress <ip_addr> <ip_mask>   dhcp }</ip_mask></ip_addr></short>	
config ipif <short <1-4094="">&gt; {ipv6address <ip6_addr> <short <1-<br="">128&gt;   dhcpv6_client <enable  <br="">disable&gt;}</enable></short></ip6_addr></short>	Configure IP setting of interface.
logout	Logout from this session.
ping [ <ipv4_addr>   <ipv6_addr>] [size <integer 1-60000="">] [timeout <time_out 1-100&gt;] [repeat <integer 0-255="">]</integer></time_out </integer></ipv6_addr></ipv4_addr>	This command checks if another computer is on the network and listens for connections. The terminal interface sends five pings to the target station.
reboot	This command reboots the system. All network connections are terminated and the boot code executes.
reset config	Reset the device to factory default
show ipif [ <short <1-4094="">&gt;]</short>	Displays the current IPv4 address of the interface.
show ipv6 interface [ <short <1-<br="">4094&gt;&gt;] [brief]</short>	Displays the current IPv6 address of the interface.
show switch	Show system information.
config account username <string &lt;32&gt; privilege <short <1-15="">&gt; { nopassword   password <string &lt;32&gt;}</string </short></string 	Configure password.

save {startup-config   config-1   config-2}	Save configuration.
boot image [image-1   image-2]	Select the boot up image.
debug info	Displays Debug Table.
debug show tech-support	Displays technical support information.

## Each command is listed in detail, as follows:

?	
Purpose	To display a list of commands.
Syntax	?
Description	The ? command displays a list of commands of the switch.
Parameters	None.
Restrictions	None.

## Example usage:

To display a list of commands of the switch:

DXS-1210-12TC> ?
USEREXEC commands :
config ipif <short <1-4094="">&gt; { ipaddress <ip_addr> <ip_mask>   dhcp   bootp } config ipif <short <1-4094="">&gt; { ipv6address <ip6_addr> <short <1-128="">   dhcpv6_client <enable disable=""  ="">} debug info logout ping [<ipv4_addr>   <ipv6_addr>] [size <value <1-60000="">&gt;] [timeout <time_out< td=""></time_out<></value></ipv6_addr></ipv4_addr></enable></short></ip6_addr></short></ip_mask></ip_addr></short>
<pre><!--</td--></pre>
reboot
reset config
save
show ipif [INTERFACE-ID]
show switch
DXS-1210-12TC>

config ipif	
Purpose	To configure the System IP interface.
Syntax	config ipif <short <1-4094="">&gt; { ipaddress <ip_addr> <ip_mask>   dhcp } config ipif <short <1-4094="">&gt; {ipv6address <ip6_addr> <short &lt;1-128&gt;   dhcpv6_client <enable disable=""  ="">}</enable></short </ip6_addr></short></ip_mask></ip_addr></short>
Description	The <b>config ipif system</b> command configures the System IP interface on the Switch.
Parameters	<pre>short &lt;1-4094&gt; - Specifies the name of ipif setting. ipaddress <ip-addr> <ip_mask> - The IP address and subnet mask to be created. Users need to specify the address and mask</ip_mask></ip-addr></pre>

	information using the traditional format (for example,10.1.2.3/255.0.0.0)	
	<i>dhcp</i> – Allows the selection of the DHCP protocol for the assignment of an IP address to the Switch's System IP interface.	
	<i>ipv6address <ip6_addr></ip6_addr></i> – Use this parameter to statically assign an IPv6address to this interface. This address should define a host address and a network prefix length. Multiple IPv6 addresses can be configured for a single IP interface. Ex: 3ffe:501:ffff:100::1/64. The /64 represents the prefix length of the IPv6 addresses.	
	<i>dhcpv6_client <enable disable=""  =""> -</enable></i> Specify the DHCPv6 client to be disabled or enabled.	
Restrictions	Only Administrator or operator-level users can issue this command.	

To configure the IP interface System:

## DXS-1210-12TC> config ipif 1 ipaddress 10.90.90.98 255.0.0.0

Success.

DXS-1210-12TC>

logout	
Purpose	To log out a user from the Switch's console.
Syntax	logout
Description	The <b>logout</b> command terminates the current user's session on the Switch's console.
Parameters	None.
Restrictions	None.

## Example usage:

To terminate the current user's console session:

DXS-1210-12TC> logout



**NOTE:** Save your configuration changes before logging out.

ping	
Purpose	To test the connectivity between network devices.
Syntax	ping [ <ipv4_addr>   <ipv6_addr>] [size <integer 1-60000="">] [timeout <time_out 1-100="">] [repeat <integer 0-255="">]</integer></time_out></integer></ipv6_addr></ipv4_addr>
Description	The <b>ping</b> command checks if another IP address is reachable on the network. You can ping the IPv4 address connected to through the managed VLAN (VLAN 1 by default), as long as there is a physical path between the switch and the target IPv4 equipment. By default, Switch sends five pings to the target IP.
Parameters	<ipv4_addr> - The IPv4 address of the host.</ipv4_addr>

	<pre><ipv6_addr> - The IPv6 address of the host.</ipv6_addr></pre>	
	<value 1-60000=""> - Specify the ping packet size.</value>	
	<time_out 1-100=""> - Specify the time out value. The range is between 1 and 100 seconds.</time_out>	
	<i>repeat <integer 0-255=""></integer></i> - Specify the repeat time.	
Restrictions	Only Administrator or operator-level users can issue this command	

To ping the IP address 10.90.90.98:

DXS-1210-12TC> ping 10.90.90.98

Reply Not Received From : 10.90.90.98, Timeout : 1 secs

Reply Not Received From : 10.90.90.98, Timeout : 1 secs

Reply Not Received From : 10.90.90.98, Timeout : 1 secs

--- 10.90.90.98 Ping Statistics ---

3 Packets Transmitted, 0 Packets Received, 100% Packets Loss

DXS-1210-12TC>

reboot		
Purpose	To reboot the Switch. If the Switch is a member of a stack, it may be rebooted individually, without affecting the other members of the stack.	
Syntax	reboot	
Description	The <b>reboot</b> command reboots the system. All network connections are terminated and the boot code executes.	
Parameters	None.	
Restrictions	None.	

#### Example usage:

To restart the Switch:

DXS-1210-12TC> reboot

Are you sure you want to proceed with the system reboot?(y/n)y

Do you want to save the settings ?(y/n)y

DXS-1210-12TC>

reset confi	g
Purpose	To reset the Switch to the factory default settings.
Syntax	reset config
Description	All configurations will be reset to the default settings.
Parameters	None.

Restrictions Only Administrator can issue this command.

## Example usage:

To restore all of the Switch's parameters to their default values:

DXS-1210-12TC> reset config

This command will clear all of system configuration as factory. System will reboot after clearing. Do you want to continue? (y/n)y

DXS-1210-12TC>

show ipif	
Purpose	To display the configuration of an IP interface on the Switch.
Syntax	show ipif [ <short <1-4094="">&gt;]</short>
Description	The <b>show ipif</b> command displays the current IP address of the switch.
Parameters	[ <short <1-4094="">&gt;] - Specify the interface to be displayed.</short>
Restrictions	None.

#### Example usage:

To display IP interface settings:

DXS-1210-12TC> show	<i>v</i> ipif
IP Setting Mode	:manual
Interface Name	:vlan1
Interface Vlan Name	:default
IP Address	:10.90.90.90
Subnet Mask	:255.0.0.0
Total Entries: 1	
DXS-1210-12TC>	

show ipv6	
Purpose	To display the configuration of an IPv6 interface on the Switch.
Syntax	show ipv6 interface [ <short <1-4094="">&gt;] [brief]</short>
Description	The <b>show ipv6</b> command displays the current IPv6 address of the switch.
Parameters	[ <short <1-4094="">&gt;] - Specify the interface to be displayed. [brief] – Specify the brief of interface to be showed.</short>
Restrictions	None.

To display IPv6 interface settings:

DXS-1210-12TC> show ipv6 interface 1 brief

vlan1 is up, IPv6 is enabled

Link-local address:

fe80::ee22:80ff:fe77:2016, Link status is up

**Total Entries: 1** 

DXS-1210-12TC>

show switch	
Purpose	To display information about the Switch.
Syntax	show switch
Description	The <b>show switch</b> command displays the status of the switch.
Parameters	None.
Restrictions	None.

## Example usage:

To display the switch information:

DXS-1210-12TC> show switch		
System Name	:Switch	
System Location	:	
System Contact	:	
System Time	:27/04/2011 18:25:37	
System hardware version	:A1	
System firmware version	:V1.00.021	
System boot version	:V1.00.003	
System serial number	:S34F1E8000036	
MAC Address	:ec-22-80-77-20-16	
DXS-1210-12TC>		

config account username	
Purpose	To configure the configuration of user account on the Switch.
Syntax	config account username <string <32=""> privilege <short <1-<br="">15&gt;&gt; { nopassword   password <string <32="">}</string></short></string>
Description	The config account username command sets the administrator

password.	
Parameters	<string <32=""> - The name of the user.</string>
	<i>privilege <short <1-15=""></short></i> - Specify the privilege level. The value 1 is for Basic user, 12 for Operator and 15 for Administrator. <i>password <string <32=""></string></i> - Specify the password.
Restrictions	Only Administrator can issue this command.

To configure the account admin password:

DXS-1210-12TC> config account username dlink privilege 15 nopassword		
DXS-1210-12TC>		

save	
Purpose	To save changes in the Switch's configuration to non-volatile RAM.
Syntax	save {startup-config   config-1   config-2}
Description	The <b>save</b> command saves the configuration changes to the memory.
Parameters	<i>{startup-config   config-1   config-2} – Specify to save the configuration when startup configuration. Or specify to save the configuration to specified image.</i>
Restrictions	None.

## Example usage:

To save the Switch's current configuration to config-1:

DXS-1210-12TC> save con	fig-1
Success!	
DXS-1210-12TC>	
DX3-1210-121C>	

boot image	
Purpose	Specify to boot up the switch from which image.
Syntax	boot image [image-1   image-2]
Description	The <b>boot image</b> command specifies to boot up switch from which image.
Parameters	None.
Restrictions	Only Administrator can issue this command.

#### Example usage:

To boot up the switch from image-1:

DXS-1210-12TC> boot image image-1 Success! DXS-1210-12TC>

debug info	
Purpose	To display the ARP table and MAC FDB information of the Switch.
Syntax	debug info
Description	The <b>debut info</b> command displays the ARP table and MAC FDB of the Switch.
Parameters	None.
Restrictions	Only Administrator can issue this command.

To display the ARP table and MAC FDB information of the Switch:

DXS-1 ARP ta		C> debug info			
Addre	SS	Hardware Address	Туре	Interface	Mapping
10.90.9	90.97	 00-11-6B-66-15-E7	ARPA	vlan1	Dynamic
MAC t	able :				
Index	VLAN	MAC Address	Туре	Ports	
1	1	00-11-6B-66-15-E7	Dynam	ic 1	
Total I	MAC Add	dresses displayed: 1			
DXS-1210-12TC>					

debug show tech-support			
Purpose	To display the Switch's information needed by the engineers to troubleshoot or analyze a problem.		
Syntax	debug show tech-support		
Description	The <b>debug show tech-support</b> command displays technical support information of the Switch.		
Parameters	None.		
Restrictions	Only Administrator and Operator-Level can issue this command.		

## Example usage:

To display technical support information of the Switch:

DXS-1210-12TC> debug show tech

debug show tech-support

DXS-1210-12TC> debug show tech-support

#-----# DXS-1210-12TC 10 Gigabit Ethernet Switch **#** Technical Support Information # # Firmware: V1.00.021 # Copyright(C) 2014 D-Link Corporation. All rights reserved. #-----**Boot Time** 2 **RTC Time** :27/04/2011 18:41:32 **Boot PROM Version** :V1.00.003 **Firmware Version** :V1.00.021 Hardware Version :A1 MAC Address :ec-22-80-77-20-16 **Serial Number** :S34F1E8000036 **SNMP Status** :Disabled **Safeguard Engine** :Disabled **IGMP Snooping** :Disabled Link Detection Power Saving :Disabled Scheduled Port-shutdown Power Saving :Disabled Scheduled Hibernation Power Saving :Disabled Scheduled Dim-LED Power Saving :Disabled Administrative Dim-LED :Disabled DXS-1210-12TC>

- DEM-431XT: 10GBASE-SR 80m

# Appendix A - Technical Specifications

## Hardware Specifications

## Key Components / Performance

- Switching Capacity:
  - DXS-1210-10TS: 200Gbps
  - DXS-1210-12TC: 240Gbps
  - DXS-1210-12SC: 240Gbps
- Max. Forwarding Rate
  - DXS-1210-10TS: 148.8Mpps
  - DXS-1210-12TC: 178.56Mpps
  - DXS-1210-12TC: 178.56Mpps
- Forwarding Mode: Store and Forward
- Packet Buffer memory:
  - DXS-1210-10TS: 2MBytes
  - DXS-1210-12TC: 2Mbytes
  - DXS-1210-12TC: 2Mbytes
- DDRII for CPU: 256M Bytes
- Flash Memory: 64M Bytes

## Port Functions

- 10GBASE-T ports compliant with the following standards:
  - 10GBASE-T: IEEE 802.3an
  - 1000BASE-T: IEEE 802.3ab
  - Supports Full-Duplex operations
  - IEEE 802.3x Flow Control support for Full-Duplex mode
  - Auto MDI/MDIX
  - Auto-negotiation
  - Head-of-line blocking prevention
- 10GE SFP/SFP+ ports compliant with the following standards:
  - IEEE 802.3z
  - IEEE 802.3ae
  - 1000BASE-T transceivers supported:
  - DGS-712 (1000BASE-TX)
  - SFP transceivers:
  - DEM-310GT (1000BASE-LX, 10km)
  - DEM-311GT (1000BASE-SX, 550m)
  - DEM-312GT2 (1000BASE-SX, 2km)
  - DEM-314GT (1000BASE-LHX, 50km)
  - DEM-315GT (1000BASE-ZX, 80km) SFP WDM Transceiver:
  - DEM-330T/R (1000BASE-BX, 10km)
  - DEM-331T/R (1000BASE-BX, 40km)

- DEM-302S-BXD (1000BASE-BX-D Single-Mode, 2KM(TX-1550/RX-1310 nm))

- DEM-302S-BXU (1000BASE-BX-U Single-Mode, 2KM(TX-1310/RX-1550 nm))
- SFP+ Transceiver:

- DEM431XT-DD: 10GBASE-SR, 80m - DEM-432XT: 10BASE-LR, 10km - DEM-432XT-DD: 10GBASE-LR, 10km - DEM-433XT: 10GBASE-ER, 40km - DEM-433XT-DD: 10GBASE-ER, 40km DEM-434XT: 10GBASE-ZR, 80km WDM SFP+ Transceiver: - DEM-436XT-BXU: 10GBASE-LR 20km - DEM-436XT-BXD: 10GBASE-LR 20km CWDM SFP+ Transceiver: DEM-X10CS-1271: 10G Single-Mode 10KM CWDM SFP+ Transceiver DEM-X10CS-1291: 10G Single-Mode 10KM CWDM SFP+ Transceiver

- DEM-X10CS-1311: 10G Single-Mode 10KM CWDM SFP+ Transceiver
- DEM-X10CS-1331: 10G Single-Mode 10KM CWDM SFP+ Transceiver
- DEM-X40CS-1471: 10G Single-Mode 40KM CWDM SFP+ Transceiver

- DEM-X40CS-1491: 10G Single-Mode 40KM CWDM SFP+ Transceiver

- DEM-X40CS-1511: 10G Single-Mode 40KM CWDM SFP+ Transceiver

- DEM-X40CS-1571: 10G Single-Mode 40KM CWDM SFP+ Transceiver

- Support following Direct Attach Cable(DAC): DEMODIACE
  - DEM-CB100S
  - DEM-CB300S - DEM-CB700S

## Physical & Environment

- AC input, 100~240 VAC, 50/60Hz, internal universal power supply
- Acoustic Value:
  - DXS-1210-10TS: 44.6dB (2 Fans)
  - DXS-1210-12TC: 44.9dB (2 Fans)
  - DXS-1210-12SC: 39.2dB (2 Fans)
- Operation Temperature -5~50°C
- Storage Temperature -40~70°C
- Operation Humidity: 0%~95% RH
- Storage Humidity: 0%~95% RH

## Emission (EMI) Certifications

- FCC class A
- CE Class A
- VCCI Class A
- IC Class A
- C-Ticket Class A
- BSMI Class A

CCC Class A

## **Safety Certifications**

CUL, CB, CE, CCC, BSMI

## Features

## L2 Features

- Supports up to 16K MAC address
- Jumbo frame: Supports up to 9KB
- IGMP snooping: Supports 128 multicast group
- MLD Snooping
- 802.1D Spanning Tree
- 802.1s MSTP
- 802.1w Rapid Spanning Tree
- Loopback Detection
- 802.3ad Link Aggregation:
  - DXS-1210-10TS: up to 8 groups per device and 8 ports per group
  - DXS-1210-12TC: up to 8 groups per device and 8 ports per group
  - DXS-1210-12SC: up to 8 groups per device and 8 ports per group
- Port mirroring

## L3 Features

- ARP:
  - Max 16K ARP entries
  - Support 128 static ARP
  - Support Gratuitous ARP
- Support 8 IPv4 and 16 IPv6 interfaces
- Support IPv4 address 0.0.0.0 to prevent occupied IP address in the network
- Support IPv6 Neighbor Discovery:
  - Max 384 ND entries
  - Support up to 63 static ND entries
- Max. 64 IPv4 and 64 IPv6 static route entries
- Support secondary route
- Max. 768 IPv4 and 384 IPv6 host route

## D-Link Green Technology

- Compliant with RoHS6.
- Support D-Link Green v3.0 power saving mode.
- D-Link Green Ethernet:
  - Power Saving by LED Shut-Off: Powered LEDs can be turned on/off by port or system through schedule
  - Power Saving by Port Shut-Off: Each port on the system can be turned on/off by schedule
  - Power Saving by System Hibernation: System enters hibernation by schedule. In this mode, switches get most power-

saving figures since main chipsets (both MAC and PHY) are disabled for all ports.

Energy Efficient Ethernet (EEE): EEE is disabled by default, user can enable EEE via Web GUI

## VLAN

- 802.1Q VLAN standard (VLAN Tagging)
- Up to 4K VLAN groups
- Asymmetric VLAN

## QoS (Quality of Service)

- Be able to classify packets according to follow contents:
  - 802.1p priority
  - VLAN
  - MAC address
  - Ether Type
  - IP address
  - DSCP
  - Protocol type
  - TCP/UDP port number
  - IPv6 traffic class
  - IPv6 flow label
- TCP/UDP port number Up to 8 queues per port
- Supports Strict / WRR / Strict+WRR / Deficit Round Rbin(DRR) / Strict\_DRR mode in queue handling
- Bandwidth Control

## <u>ACL</u>

- Max 50 ingress ACL profile, 512 ingress ACL rules, 50 VLAN ACL rules.
- Each rule can be associated to a single port, multiple ports
- Supports following actions after analyzing packets:
  - Permit
  - Deny
- Support different ACL policy packet contents:
  - MAC address
  - Ethernet Type
  - IP address
  - ICMP
  - IGMP
  - TCP/UDP port number
  - 802.1p
  - DSCP
  - IPv6 traffic class
  - IPv6 flow label

### Security

Port Security: Support 64 MACs per port

- IP and MAC ACL
- Broadcast Storm Control
- D-Link Safeguard Engine
- DHCP Server Screening over IPv4 or IPv6 : Maximum 5 entries
- SSL: Support v1/v2/v3
- Support DHCP Snooping
- IP-MAC-Port Binding

- Supports ARP packet Inspection as default, ARP and IPv4 packet Inspection as option.

- Supports IPv4 DHCP Snooping
- Þ

## **Management**

- Web-based GUI (IPv6 support)
- D-Link compact CLI (Supports IPv6 commands)
- Telnet Server: Max. 4 connections (IPv6 support)
- TFTP Client over IPv4 or IPv6
- SNMP v1/2c/3 over IPv4 or IPv6
- SNMP Trap
- DHCP client over IPv4 or IPv6
- RMON v1/v2
- Trap setting for destination IP, system events, fiber port events, twisted-pair port events
- Web-based configuration backup / restoration
- Web-based firmware backup/restore
- Firmware upgrade Web-based management
- Reset, Reboot

