

DXS-1100 Series

10 GIGABIT ETHERNET SWITCH USER MANUAL

Ver. 1.10



Copyright and Trademarks

Information in this document is subjected to change without notice.

© 2016 D-Link Corporation. All rights reserved.

Reproduction in any manner whatsoever 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.

FCC Warning

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

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.

CE Mark Warning

This equipment is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

VCCI Warning

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

BSMI Notice

此為甲類資訊技術設備，於居住環境中使用時，可能會造成射頻擾動，在此種情況下，使用者會被要求採取某些適當的對策。

Safety Compliance

Warning: Class 1 Laser Product.

- **EN:** When using a fiber optic media expansion module, never look at the transmit laser while it is powered on. Also, never look directly at the fiber TX port and fiber cable ends when they are powered on.
- **FR:** Ne regardez jamais le laser tant qu'il est sous tension. Ne regardez jamais directement le port TX (Transmission) à fibres optiques et les embouts de câbles à fibres optiques tant qu'ils sont sous tension.

SFP (Mini-GBIC), XENPAK, and XFP Regulatory Compliance

Networks pluggable optical modules meet the following regulatory requirements:

- Class 1.
- IEC/EN60825-1:2007 2nd Edition or later, European Standard
- FCC 21 CFR Chapter 1, Subchapter J in accordance with FDA and CDRH requirements.
- Application of CE Mark in accordance with 2004/108/EEC EMC Directive and the 2006/95/EC Low Voltage Directives.
- UL and/or CSA registered component for North America.
- 47 CFR Part 15, Class A when installed into products.

Table of Contents

| | |
|--|-----------|
| Intended Readers | 1 |
| Terms/Usage..... | 1 |
| Safety Instructions | 1 |
| General Precautions for Rack-Mountable Products | 3 |
| Protecting Against Electrostatic Discharge..... | 3 |
| 1 Product Introduction..... | 4 |
| DXS-1100-10TS..... | 5 |
| Front Panel..... | 5 |
| Rear Panel..... | 5 |
| Side Panels | 5 |
| DXS-1100-16TC | 6 |
| Front Panel..... | 6 |
| Rear Panel..... | 6 |
| Side Panels | 6 |
| 2 Hardware Installation..... | 8 |
| Step 1: Unpacking..... | 8 |
| Step 2: Switch Installation..... | 8 |
| Desktop or Shelf Installation..... | 8 |
| Rack Installation | 8 |
| Step 3: Plugging in the AC Power Cord with Power Cord Retainer | 10 |
| Power Failure | 12 |
| 3 Getting Started..... | 13 |
| Management Options..... | 13 |
| Using Web-based Management | 13 |
| Supported Web Browsers | 13 |
| Connecting to the Switch..... | 13 |
| Login Web-based Management | 13 |
| Smart Wizard | 14 |
| Web-based Management..... | 14 |
| D-Link Network Assistant (DNA)..... | 14 |
| 4 Configuration..... | 16 |
| Smart Wizard Configuration..... | 16 |
| System IP Information | 16 |
| User Accounts Settings..... | 17 |
| SNMP | 18 |
| Web-based Management..... | 19 |
| Tool Bar > Save Menu | 20 |
| Save Configuration..... | 20 |
| Tool Bar > Tools Menu..... | 20 |
| Firmware Upgrade and Backup..... | 20 |
| Configuration Restore and Backup | 22 |
| Log Backup..... | 24 |
| Ping | 25 |
| Reset | 26 |
| Reboot System..... | 27 |
| Tool Bar > Wizard | 27 |
| Tool Bar > Online Help..... | 27 |

| | |
|--|----|
| Function Tree | 28 |
| Device Information | 28 |
| System > System Information Settings | 29 |
| System > Peripheral Settings | 29 |
| System > Port Configuration > Port Settings | 30 |
| System > Port Configuration > Port Status | 31 |
| System > Port Configuration > Error Disable Settings | 32 |
| System > Port Configuration > Jumbo Frame | 32 |
| System > System Log > System Log Settings | 33 |
| System > System Log > System Log Discriminator Settings | 34 |
| System > System Log > System Log Server Settings | 34 |
| System > System Log > System Log | 35 |
| System > System Log > System Attack Log | 35 |
| System > Time and SNTP > Clock Settings | 36 |
| System > Time and SNTP > Time Zone Settings | 36 |
| System > Time and SNTP > SNTP Settings | 37 |
| System > Time Range | 38 |
| Management > User Accounts Settings | 38 |
| Management > Password Encryption | 39 |
| Management > SNMP > SNMP Global Settings | 39 |
| Management > SNMP > SNMP Linkchange Trap Settings | 40 |
| Management > SNMP > SNMP View Table Settings | 41 |
| Management > SNMP > SNMP Community Table Settings | 42 |
| Management > SNMP > SNMP Group Table Settings | 43 |
| Management > SNMP > SNMP Engine ID Local Settings | 43 |
| Management > SNMP > SNMP User Table Settings | 44 |
| Management > SNMP > SNMP Host Table Settings | 44 |
| Management > RMON > RMON Global Settings | 45 |
| Management > RMON > RMON Statistics Settings | 46 |
| Management > RMON > RMON History Settings | 46 |
| Management > RMON > RMON Alarm Settings | 47 |
| Management > RMON > RMON Event Settings | 48 |
| Management > Web | 48 |
| Management > Session Timeout | 49 |
| Management > File System | 49 |
| Management > D-Link Discovery Protocol | 50 |
| L2 Features > FDB > Static FDB > Unicast Static FDB | 51 |
| L2 Features > FDB > Static FDB > Multicast Static FDB | 52 |
| L2 Features > FDB > MAC Address Table Settings | 52 |
| L2 Features > FDB > MAC Address Table | 53 |
| L2 Features > FDB > MAC Notification | 54 |
| L2 Features > VLAN > 802.1Q VLAN | 54 |
| L2 Features > VLAN > Asymmetric VLAN | 55 |
| L2 Features > VLAN > VLAN Interface | 55 |
| L2 Features > VLAN > Auto Surveillance VLAN > Auto Surveillance Properties | 58 |
| L2 Features > VLAN > Auto Surveillance VLAN > MAC Settings and Surveillance Device | 59 |
| L2 Features > VLAN > Voice VLAN > Voice VLAN Global | 60 |
| L2 Features > VLAN > Voice VLAN > Voice VLAN Port | 61 |
| L2 Features > VLAN > Voice VLAN > Voice VLAN OUI | 61 |

| | |
|---|-----|
| L2 Features > VLAN > Voice VLAN > Voice VLAN Device | 62 |
| L2 Features > VLAN > Voice VLAN > Voice VLAN LLDP-MED Device | 62 |
| L2 Features > STP > STP Global Settings | 62 |
| L2 Features > STP > STP Port Settings | 63 |
| L2 Features > STP > STP Global Information | 65 |
| L2 Features > STP > STP Port Information | 65 |
| L2 Features > Loopback Detection | 65 |
| L2 Features > Link Aggregation | 66 |
| L2 Features > L2 Multicast Control> IGMP Snooping > IGMP Snooping Settings..... | 68 |
| L2 Features > L2 Multicast Control> IGMP Snooping > IGMP Snooping Groups Settings..... | 70 |
| L2 Features > L2 Multicast Control> IGMP Snooping > IGMP Snooping Mrouter Settings | 71 |
| L2 Features > L2 Multicast Control> IGMP Snooping > IGMP Snooping Statistics Settings | 72 |
| L2 Features > L2 Multicast Control> MLD Snooping > MLD Snooping Settings..... | 72 |
| L2 Features > L2 Multicast Control> MLD Snooping > MLD Snooping Groups Settings..... | 75 |
| L2 Features > L2 Multicast Control> MLD Snooping > MLD Snooping Mrouter Settings | 76 |
| L2 Features > L2 Multicast Control> MLD Snooping > MLD Snooping Statistics Settings | 77 |
| L2 Features > L2 Multicast Control> Multicast Filtering..... | 77 |
| L2 Features > LLDP > LLDP Global Settings | 79 |
| L2 Features > LLDP > LLDP Port Settings | 80 |
| L2 Features > LLDP > LLDP Management Address List..... | 80 |
| L2 Features > LLDP > LLDP Basic TLVs Settings..... | 81 |
| L2 Features > LLDP > LLDP Dot1 TLVs Settings..... | 82 |
| L2 Features > LLDP > LLDP Dot3 TLVs Settings..... | 82 |
| L2 Features > LLDP > LLDP-MED Port Settings..... | 83 |
| L2 Features > LLDP > LLDP Statistics Information | 84 |
| L2 Features > LLDP > LLDP Local Port Information | 85 |
| L2 Features > LLDP > LLDP Neighbor Port Information | 87 |
| L3 Features > IPv4 Interface..... | 87 |
| L3 Features > IPv6 Interface..... | 88 |
| L3 Features > IPv6 Neighbor | 89 |
| L3 Features > IPv6 Route Table | 90 |
| QoS > Basic Settings > Port Default CoS | 90 |
| QoS > Basic Settings > Port Scheduler Method | 91 |
| QoS > Basic Settings > Queue Settings | 91 |
| QoS > Basic Settings > CoS to Queue Mapping | 92 |
| QoS > Basic Settings > Port Rate Limiting | 93 |
| QoS > Advanced Settings > Port Trust State..... | 94 |
| QoS > Advanced Settings > DSCP CoS Mapping..... | 94 |
| Security > Port Security > Port Security Global Settings | 95 |
| Security > Port Security > Port Security Port Settings | 96 |
| Security > Port Security > Port Security Address Entries | 97 |
| Security > ARP Spoofing Prevention | 97 |
| Security > Safeguard Engine Settings | 98 |
| Security > Traffic Segmentation Settings..... | 99 |
| Security > Storm Control | 99 |
| Security > DoS Attack Prevention Settings..... | 101 |
| Security > SSL > SSL Global Settings | 102 |
| Security > SSL > Crypto PKI Trustpoint..... | 103 |
| Security > SSL > SSL Service Policy..... | 104 |

| | |
|--|------------|
| OAM > Cable Diagnostics | 105 |
| Monitoring > Utilization > Port Utilization | 106 |
| Monitoring > Statistics > Port | 107 |
| Monitoring > Statistics > Port Counters..... | 108 |
| Monitoring > Statistics > Counters | 110 |
| Monitoring > Mirror Settings | 111 |
| Monitoring > Device Environment | 112 |
| Green > Power Saving | 113 |
| Green > EEE | 115 |
| Appendix A - Technical Specifications | 116 |
| Hardware Specifications | 116 |
| Key Components / Performance | 116 |
| Port Functions | 116 |
| Physical & Environment | 116 |
| Emission (EMI) Certifications | 116 |
| Safety Certifications | 116 |
| Features | 116 |
| L2 Features | 116 |
| L3 Features | 117 |
| VLAN | 117 |
| QoS (Quality of Service)..... | 117 |
| Security..... | 117 |
| OAM | 117 |
| Management..... | 117 |
| D-Link Green Technology | 117 |
| Appendix B - System Log Entries..... | 118 |
| Auto Surveillance VLAN..... | 118 |
| Configuration/Firmware..... | 118 |
| DHCPv6 client..... | 120 |
| DOS Prevention | 121 |
| Interface | 121 |
| IPv6 Duplicate Address..... | 122 |
| LACP..... | 122 |
| LBD | 123 |
| LLDP(-MED)..... | 123 |
| Peripheral..... | 124 |
| Port Security..... | 125 |
| Safeguard..... | 125 |
| SNMP | 126 |
| Storm Control | 126 |
| STP Debug Enhancement | 126 |
| System | 127 |
| Voice VLAN..... | 128 |
| Web | 129 |
| Appendix C - Trap Entries | 131 |
| Authentication Fail | 131 |
| DOS Prevention | 131 |
| ErrDisable | 131 |
| General Management | 131 |

| | |
|-----------------------|-----|
| LBD | 131 |
| LLDP | 132 |
| MAC-notification..... | 132 |
| Peripheral..... | 132 |
| Port..... | 133 |
| Port Security..... | 133 |
| RMON | 133 |
| Safeguard..... | 134 |
| Start..... | 134 |
| Storm Control..... | 134 |
| STP | 134 |
| System File | 135 |

Intended Readers

This guide provides instructions to install the D-Link 10 Gigabit Ethernet Switch DXS-1100-10TS, and DXS-1100-16TC, how to configure Web-based Management step-by-step.



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 mainly divided into three parts:

1. Hardware Installation: Step-by-step hardware installation procedures.
2. Getting Started: A startup guide for basic switch installation and settings.
3. Configuration: Information about the function descriptions and configuration settings.

Terms/Usage

In this guide, the term “Switch” (first letter capitalized) refers to the 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 **NOTICE** indicates either potential damage to hardware or loss of data and tells how to avoid the problem.



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

Safety Instructions

Use the following safety guidelines to ensure your own personal safety and to help protect your system from potential damage. Throughout this safety section, the caution icon () is used to indicate cautions and precautions that need to be reviewed and followed.



CAUTION: Only trained and qualified service personnel should install, replace or perform maintenance on D-Link switches.

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

- Observe and follow service markings.
 - Do not service any product except as explained in your system documentation.
 - Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose you to electrical shock.
 - Only a trained service technician should service components inside these compartments.
- If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your trained service provider:

- The power cable, extension cable, or plug is damaged.
- An object has fallen into the product.
- The product has been exposed to water.
- The product has been dropped or damaged.
- The product does not operate correctly when you follow the operating instructions.
- Keep your system away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the system gets wet, see the appropriate section in your troubleshooting guide or contact your trained service provider.
- Do not push any objects into the openings of your system. Doing so can cause fire or electric shock by shorting out interior components.
- Use the product only with approved equipment.
- Allow the product to cool before removing covers or touching internal components.
- Operate the product only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local power company.
- To help avoid damaging your system, be sure the voltage on the power supply is set to match the power available at your location:
 - 115 volts (V)/60 hertz (Hz) in most of North and South America and some Far Eastern countries such as South Korea and Taiwan
 - 100 V/50 Hz in eastern Japan and 100 V/60 Hz in western Japan
 - 230 V/50 Hz in most of Europe, the Middle East, and the Far East
- Also, be sure that attached devices are electrically rated to operate with the power available in your location.
- Use only approved power cable(s). If you have not been provided with a power cable for your system or for any AC-powered option intended for your system, purchase a power cable that is approved for use in your country. The power cable must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.
- To help prevent electric shock, plug the system and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a 3-wire cable with properly grounded plugs.
- Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.
- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables and power cables carefully; route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local/national wiring rules.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:
 - Install the power supply before connecting the power cable to the power supply.
 - Unplug the power cable before removing the power supply.
 - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.
- Move products with care; ensure that all casters and/or stabilizers are firmly connected to the system. Avoid sudden stops and uneven surfaces.

General Precautions for Rack-Mountable Products

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

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



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



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

Protecting Against Electrostatic Discharge

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

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

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

1 Product Introduction

Thank you and congratulations on your purchase of D-Link 10 Gigabit Ethernet Switch Products.

The product 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 advanced features including network security, traffic segmentation, QoS and versatile management.

Flexible Port Configurations. The DXS-1100 series is the new generation of Web 10 Gigabit Ethernet Switch series. It provides a variety of port counts that can operate at up to 10 Gbps wire speed.

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-1100 series such as shutting down a port, or turning off some LED indicators, 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 and Loopback Detection to enhance performance and network resiliency.

Traffic Segmentation, QoS and Auto Surveillance VLAN. The switches support 802.1Q VLAN standard tagging to enhance network security and performance. The switches also support 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 in the network. Auto Surveillance VLAN will automatically place the video traffic from pre-defined IP surveillance devices to an assigned VLAN with higher priority, so it can be separated from normal data traffic. Asymmetric VLAN is implemented in these switches for a more efficient use of shared resources, such as server or gateway devices.

Network Security. D-Link's innovative Safeguard Engine function protects the switches against traffic flooding caused by virus attacks. 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. ARP Spoofing Prevention protects the Switch from intercepting data frames on the network.

Versatile Management. The new generation of D-Link 10 Gigabit Ethernet Switches provides 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. The **D-Link Network Assistant (DNA)** is a program that allows administrators to quickly discover all D-Link smart switches and D-Link Discover Protocol (DDP) supported devices that are in the same subnet as the PC, collect traps and log messages, and provide quick access to basic configurations of the switch.

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

Automated Fan Speed. Switches in this series have a built-in temperature sensor that will measure the switch's internal temperature and then automatically adjust the speed of the fans to either high-speed or low-speed.

DXS-1100-10TS

The DXS-1100-10TS 10 Gigabit Ethernet Switch supports the following ports:

- Eight 100/1000/10000Mbps copper Ethernet ports.
- Two 1/10Gbps SFP+ module ports.

Front Panel

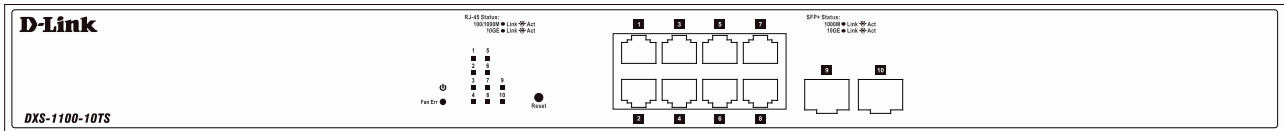


Figure 1.1 – DXS-1100-10TS Front Panel

Power LED : The Power LED lights up when the Switch is connected to a power source.

Port Link/Act/Speed LED (1-10): 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 10G.

Fan Err: The LED illuminates red when the fan has run time failure and is brought offline.

Reset: By pressing and holding the Reset button inside the pinhole for 3 to 5 seconds, the Switch will change back to the default configuration and all changes will be lost.

Rear Panel

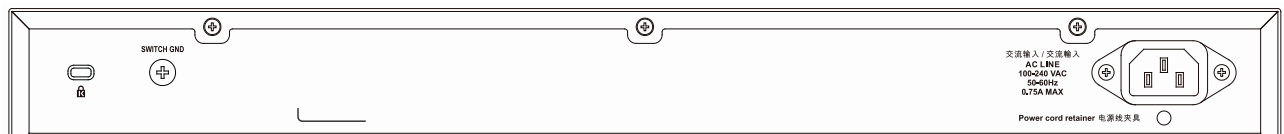


Figure 1.2 – DXS-1100-10TS Rear Panel

Power: The power port is where to connect the external power adapter.

Security Lock: Provide a Kensington-compatible security lock to be able to connect to a secure immovable device. Insert the lock into the notch and turn the key to secure the lock. The lock-and-cable apparatus should be purchased separately.

Switch GND: Use an electrical grounding wire and connect one end of the wire to the Switch GND and the other end of the wire to an electrical grounding point most commonly found on the switch mounting rack itself.

Side Panels

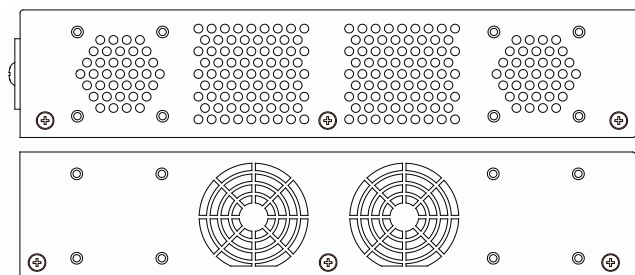


Figure 1.3 – DXS-1100-10TS Side Panels

Heat Vents: The heat vents are used to dissipate internal heat and facilitate internal air circulation. Do not block these openings. Leave at least 6 inches of space at the rear and sides of the Switch for proper ventilation. Without proper heat dissipation and air circulation, system components might overheat which could lead to system failure or even severely damaged components.

Rack-mounting Screw Holes: The screw holes are used for attach mounting brackets when installing the Switch to the rack.

Fans: Switches in this series have a built-in temperature sensor that will measure the switch’s internal temperature and then automatically adjust the speed of the fans to either high-speed or low-speed.

DXS-1100-16TC

The DXS-1100-16TC 10 Gigabit Ethernet Switch supports the following ports:

- Twelve 100/1000/10000Mbps copper Ethernet ports.
- Two 100/1000/10000Mbps copper, 1/10Gbps SFP+ combo ports
- Two 1/10Gbps SFP+ module ports.

Front Panel

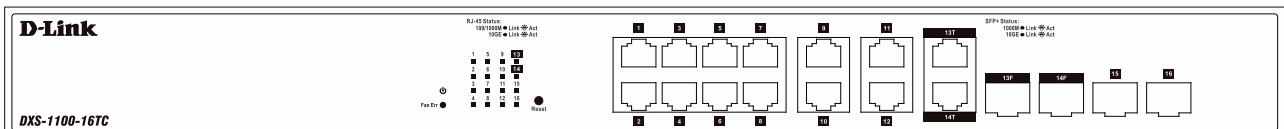


Figure 1.4 – DXS-1100-16TC Front Panel

Power LED : The Power LED lights up when the Switch is connected to a power source.

Port Link/Act/Speed LED (1-16): 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 10G.

Fan Err: The LED illuminates red when the fan has run time failure and is brought offline.

Reset: By pressing and holding the Reset button inside the pinhole for 3 to 5 seconds, the Switch will change back to the default configuration and all changes will be lost.

Rear Panel

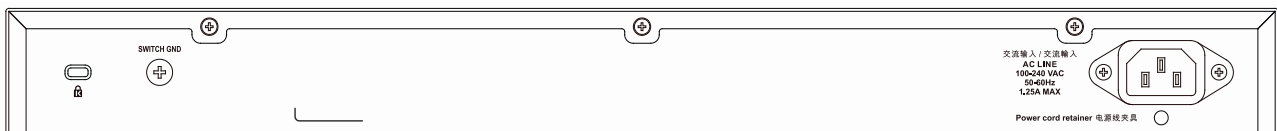


Figure 1.5 – DXS-1100-16TC Rear Panel

Power: The power port is where to connect the AC power cord.

Security Lock: Provide a Kensington-compatible security lock to be able to connect to a secure immovable device. Insert the lock into the notch and turn the key to secure the lock. The lock-and-cable apparatus should be purchased separately.

Switch GND: Use an electrical grounding wire and connect one end of the wire to the Switch GND and the other end of the wire to an electrical grounding point most commonly found on the switch mounting rack itself.

Side Panels

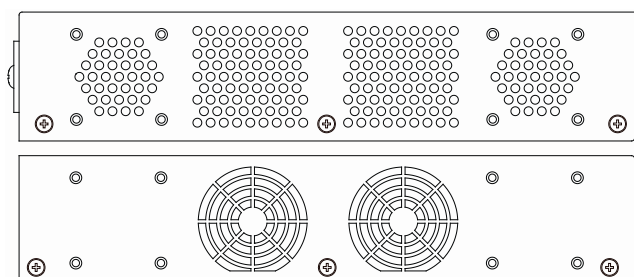


Figure 1.6 – DXS-1100-16TC Side Panels

Heat Vents: The heat vents are used to dissipate internal heat and facilitate internal air circulation. Do not block these openings. Leave at least 6 inches of space at the rear and sides of the Switch for proper ventilation. Without proper heat dissipation and air circulation, system components might overheat which could lead to system failure or even severely damaged components.

Rack-mounting Screw Holes: The screw holes are used for attach mounting brackets when installing the Switch to the rack.

Fans: Switches in this series have a built-in temperature sensor that will measure the switch's internal temperature and then automatically adjust the speed of the fans to either high-speed or low-speed.

2 Hardware Installation

This chapter provides unpacking and installation information for the Switch.

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.

- › One D-Link 10 Gigabit Ethernet Switch
- › One AC power cord
- › One set of Power cord retainer
- › Four rubber feet
- › Screws and two mounting brackets
- › One Multi-lingual Getting Started Guide
- › One CD with Web UI Reference Guide, Getting Started Guide, and D-Link Network Assistant User Guide.

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.

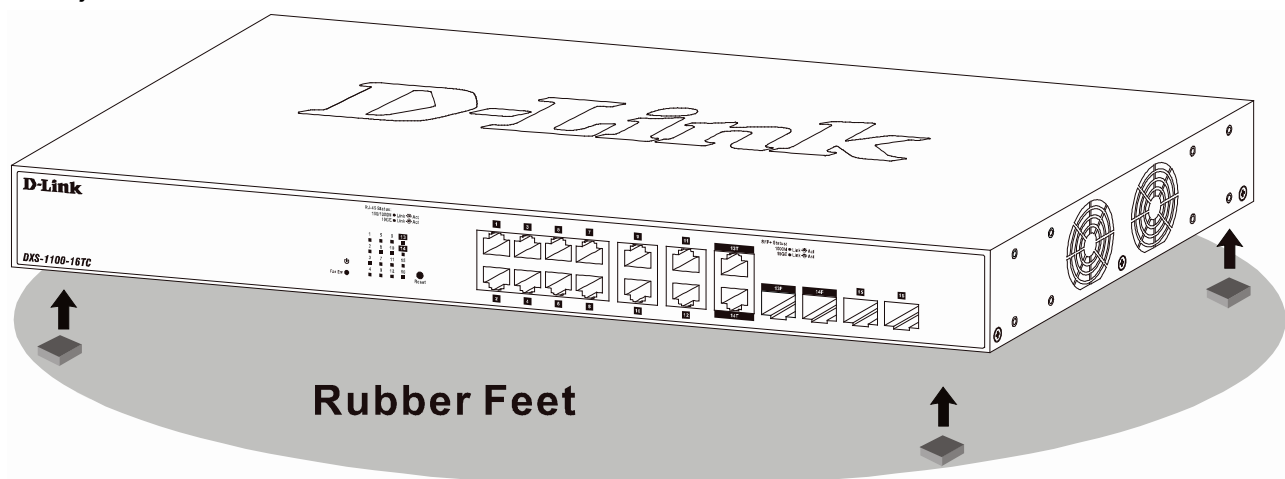


Figure 2.1 – Attach the adhesive rubber pads to the bottom

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 (please note that these brackets are not designed for palm size switches).

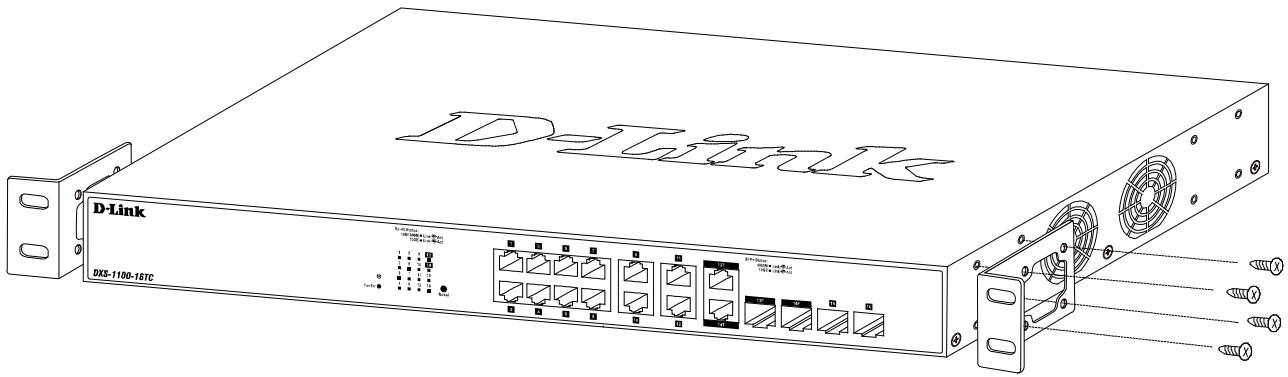


Figure 2.2 – Attach the mounting brackets to the Switch

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

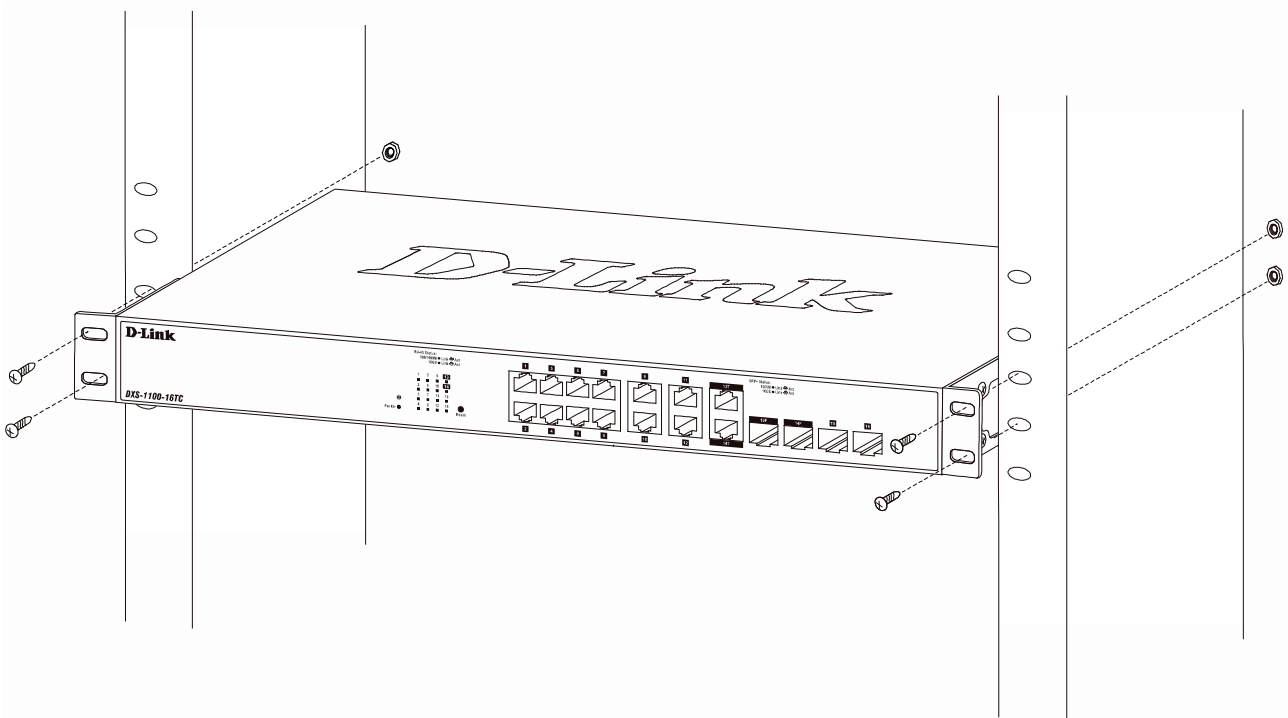


Figure 2.3 – Mount the Switch in the rack or chassis

Please be aware of following safety Instructions when installing:

- A) Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (T_{ma}) specified by the manufacturer.
- B) Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
- C) Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- D) Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit, and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

E) Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips)."

Step 3: Plugging in the AC Power Cord with Power Cord Retainer

To prevent accidental removal of the AC power cord, it is recommended to install the power cord retainer together with the power cord.

A) With the rough side facing down, insert the Tie Wrap into the hole below the power socket.

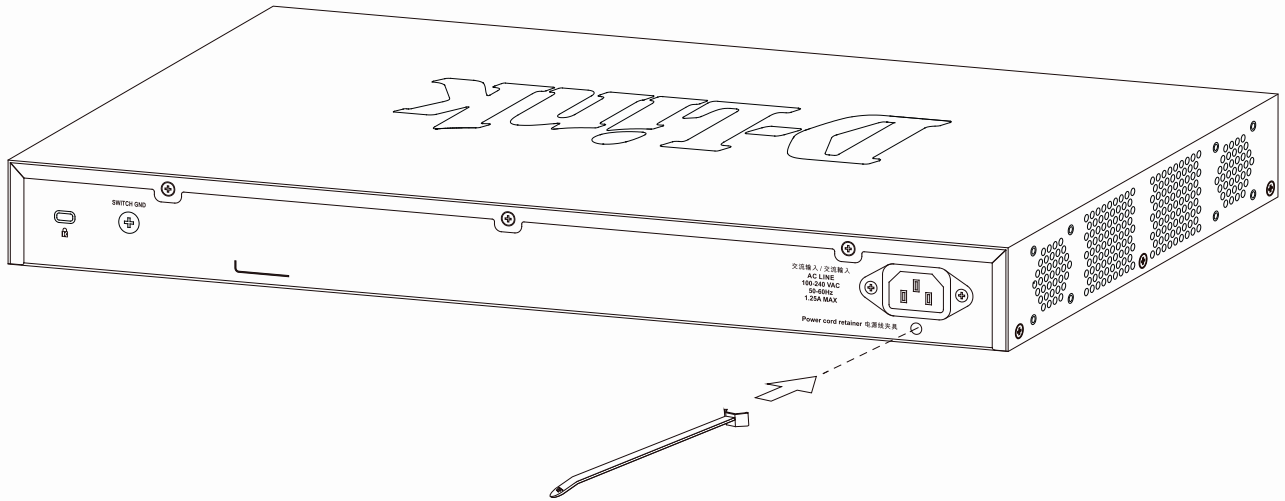


Figure 2.4 – Insert Tie Wrap to the Switch

B) Plug the AC power cord into the power socket of the Switch.

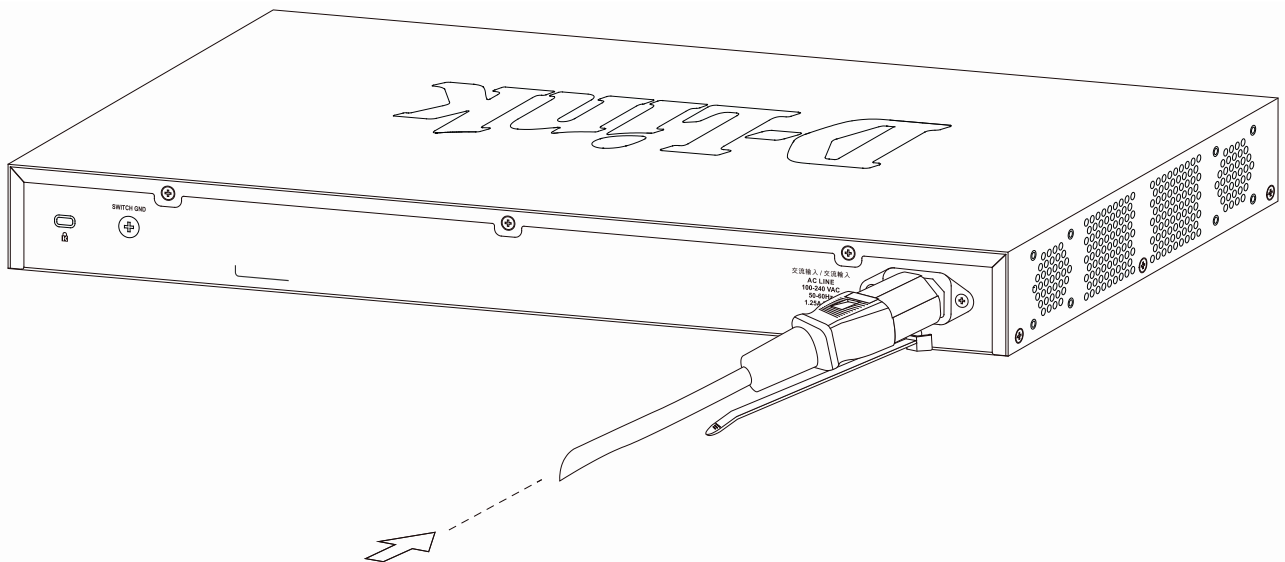


Figure 2.5 – Connect the power cord to the Switch

C) Slide the Retainer through the Tie Wrap until the end of the cord.

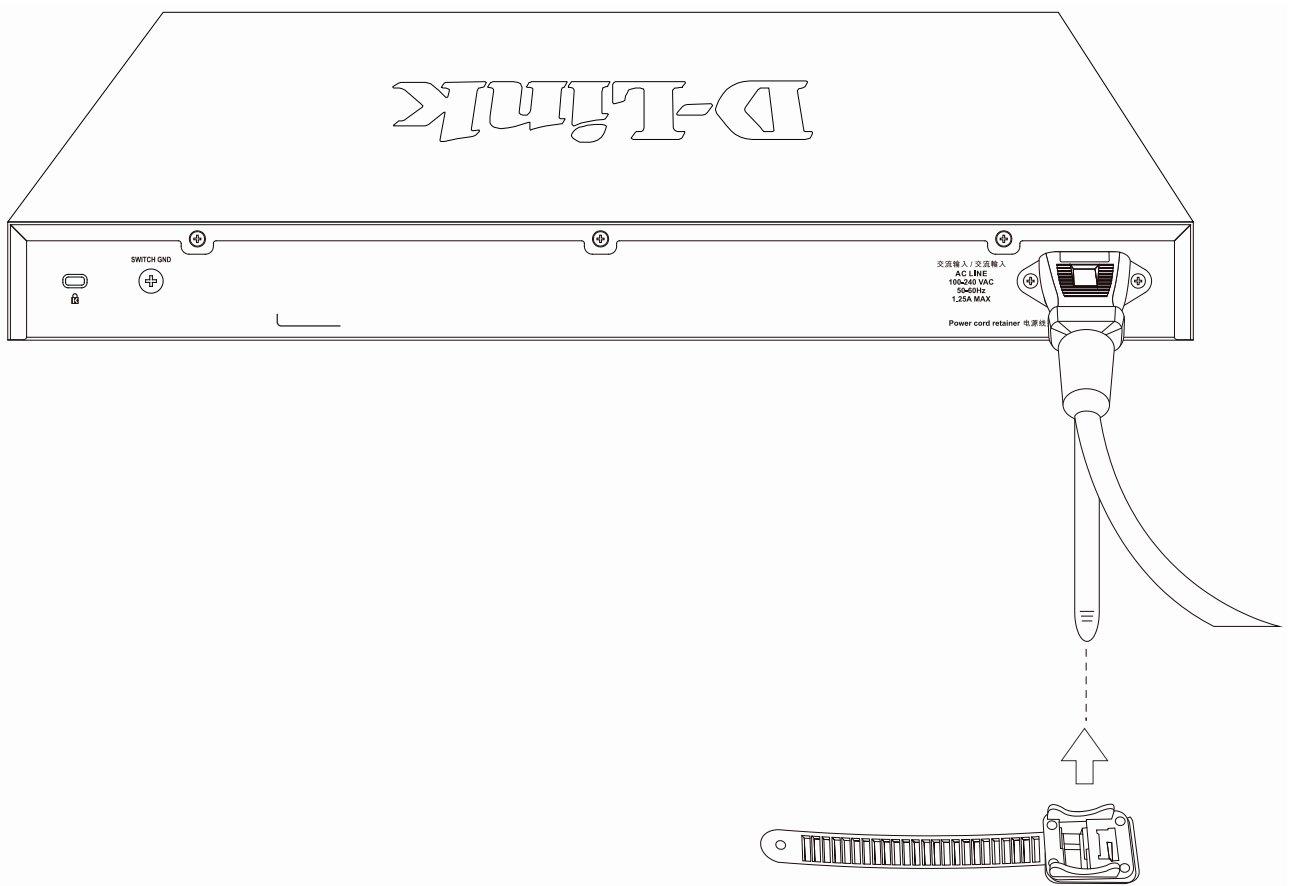


Figure 2.6 – Slide the Retainer through the Tie Wrap

D) Circle the tie of the Retainer around the power cord and into the locker of the Retainer.

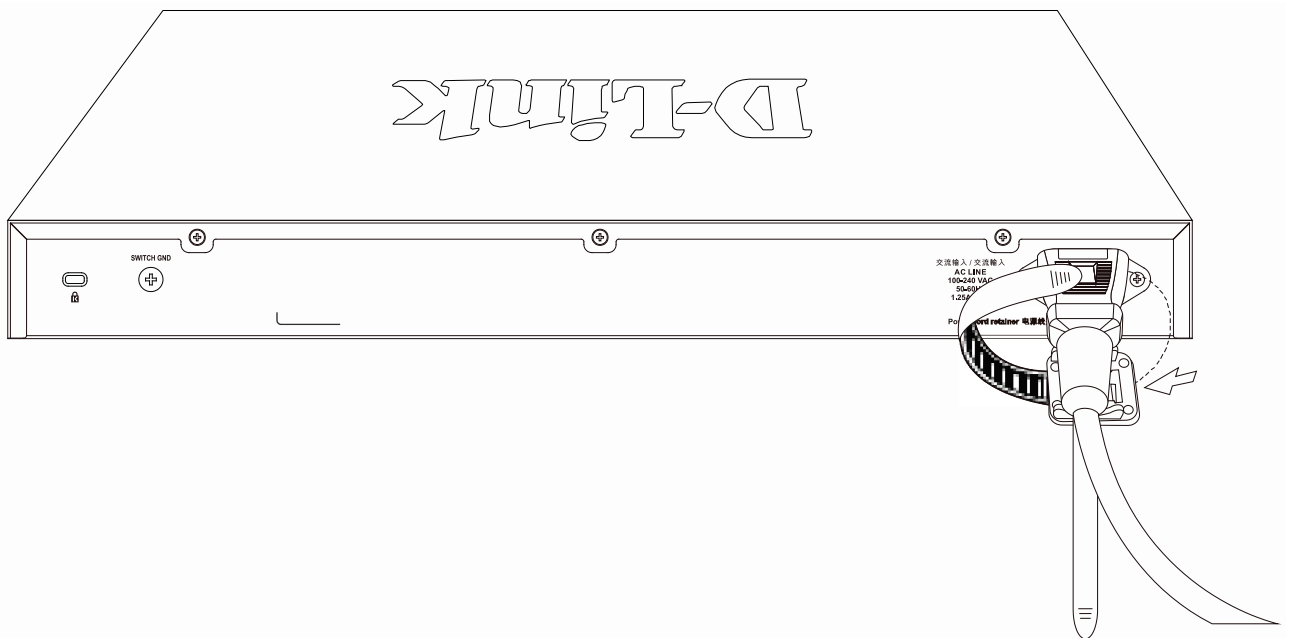


Figure 2.7 – Circle around the power cord

E) Fasten the tie of the Retainer until the power cord is secured.

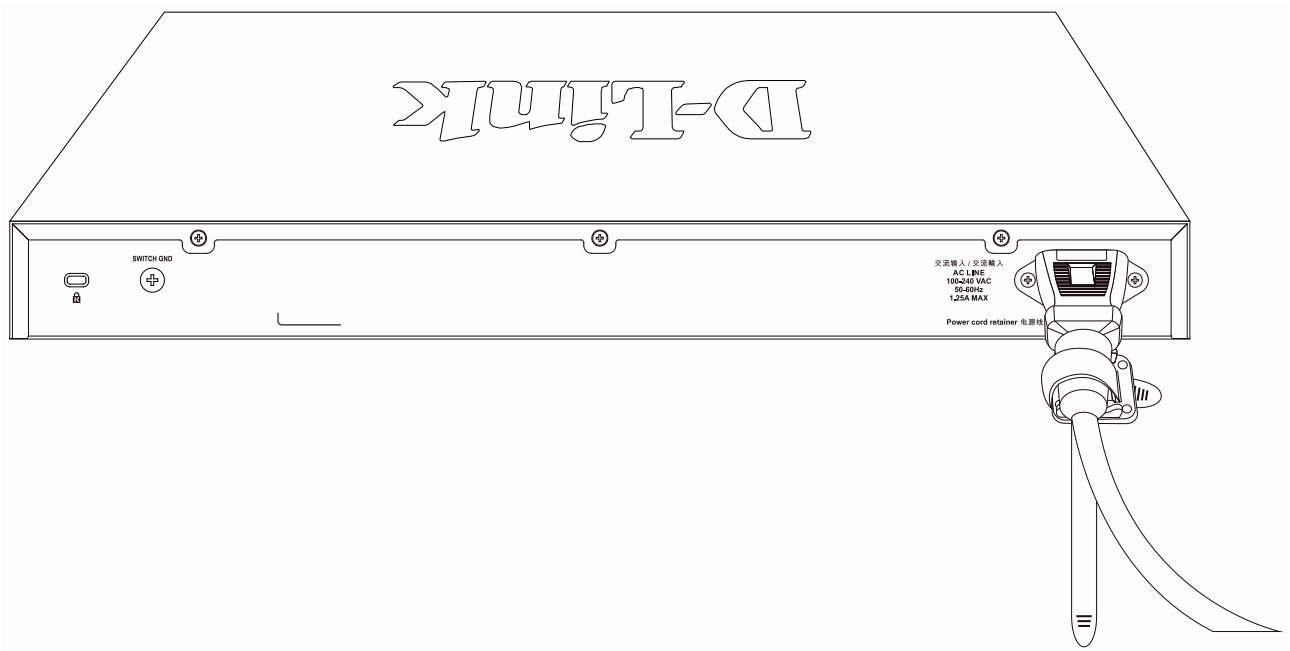


Figure 2.8 – Secure the power cord

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

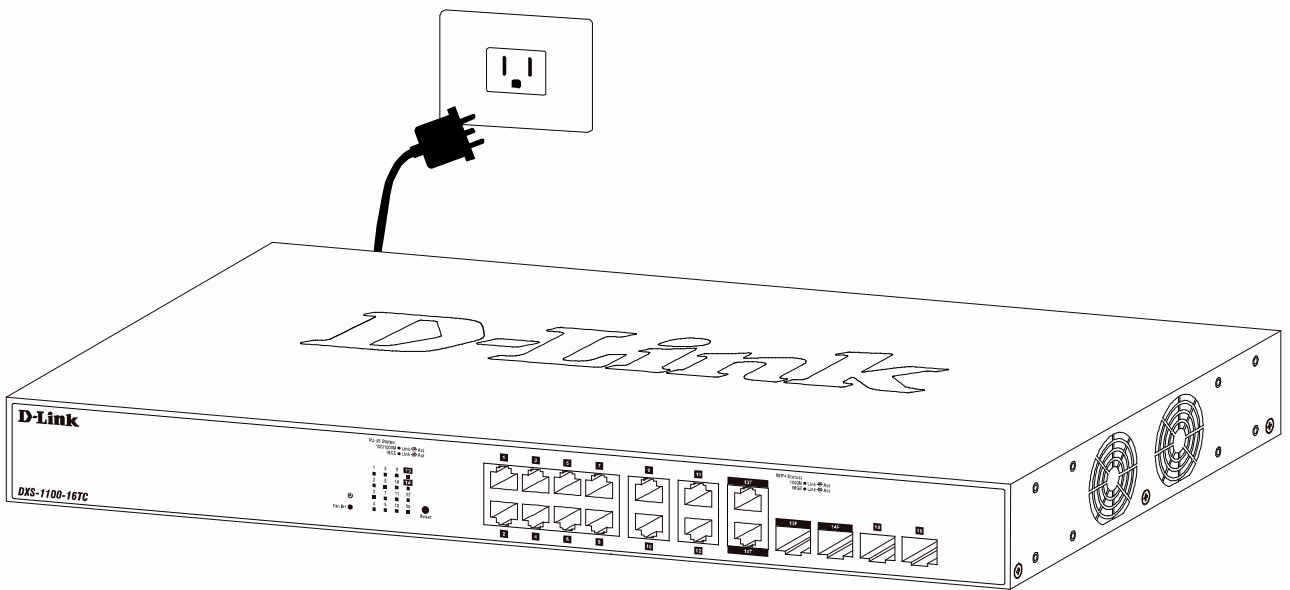


Figure 2.9 – Plugging the switch into an outlet

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 the Switch.

Management Options

The D-Link Switch can be managed through any port on the device by using the Web-based Management.

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 range 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 and the D-Link Network Assistant (DNA).

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 (version 7 and later)
- Firefox
- Google Chrome
- Safari

Connecting to the Switch

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

1. A PC with a RJ45 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.

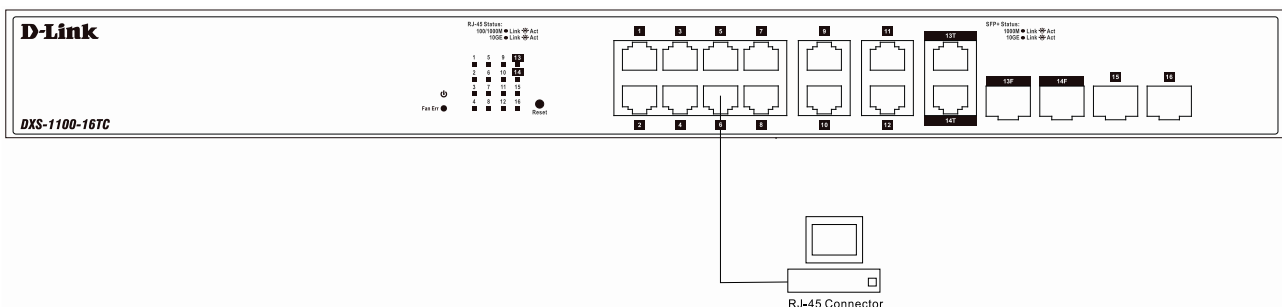


Figure 3.1 – Connected Ethernet cable

Login Web-based Management

In order to login and configure the switch via an Ethernet connection, 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 and 254 and z is a number between 1 and 254), and a subnet mask of **255.0.0.0**. Open the web browser and enter **10.90.90.90** (the factory-default IP address) in the address bar. Then press <Enter>.

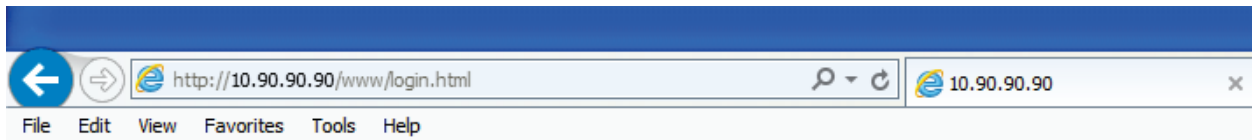


Figure 3.2 – Enter the IP address 10.90.90.90 in the web browser



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 logon dialog box appears, enter the **User Name** and **Password** in the corresponding fields and click **Login**.

A screenshot of a logon dialog box titled "Connect to 10.90.90.90". It features a key icon. There are two input fields: "User Name" with the text "admin" and "Password" with five dots. Below the fields are two buttons: "Login" and "Reset".

Figure 3.3 – Logon Dialog Box



NOTE: The Switch's factory default username is admin and the default password is admin.

Smart Wizard

After a successful login, the Smart Wizard will guide you through essential settings of the 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 [Configuration](#) for detailed instructions.

D-Link Network Assistant (DNA)

The D-Link Network Assistant (DNA), included in the installation CD, is a program that allows administrators to quickly discover all D-Link smart switches and D-Link Discover Protocol (DDP) supported devices (for a list of supported models, refer to the *D-Link Network Assistant (DNA) User Guide*), that are in the same subnet as the PC, collect traps and log messages, and provide quick access to basic configurations of the switch. This tool is only for computers running Windows 7, Vista, XP, or 2000 on both 32/64bit systems. There are two options for the installation of the DNA; one is through the Autorun program on the installation CD and the other is manual installation.



NOTE: Please be sure to uninstall any existing DNA from your PC before installing the latest DNA.

For detailed explanations of the DNA functions, please refer to *D-Link Network Assistant (DNA) User Guide*.

4 Configuration

The features and functions of the 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 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 **Ignore the wizard next time** for the next time you logon to the Web-based Management.

System IP Information

IP Information will guide you to do basic configurations in 3 steps for the IP Information, access password, and SNMP. Select **Static**, **DHCP** or **BOOTP**, and enter the desired new **IP Address**, select the **Netmask** and enter the **Gateway** address, then click the **Next** button to enter the next User Accounts Settings window. (No need to enter IP Address, Netmask and Gateway if DHCP and BOOTP are selected.) The Smart Wizard is for the quick setting in IPv4 environment. If you are not changing the settings, click the **Exit** button to go to the main page of Web-based Management. You can also tick **Ignore the wizard next time** check box to skip wizard setting when the Switch boots up.

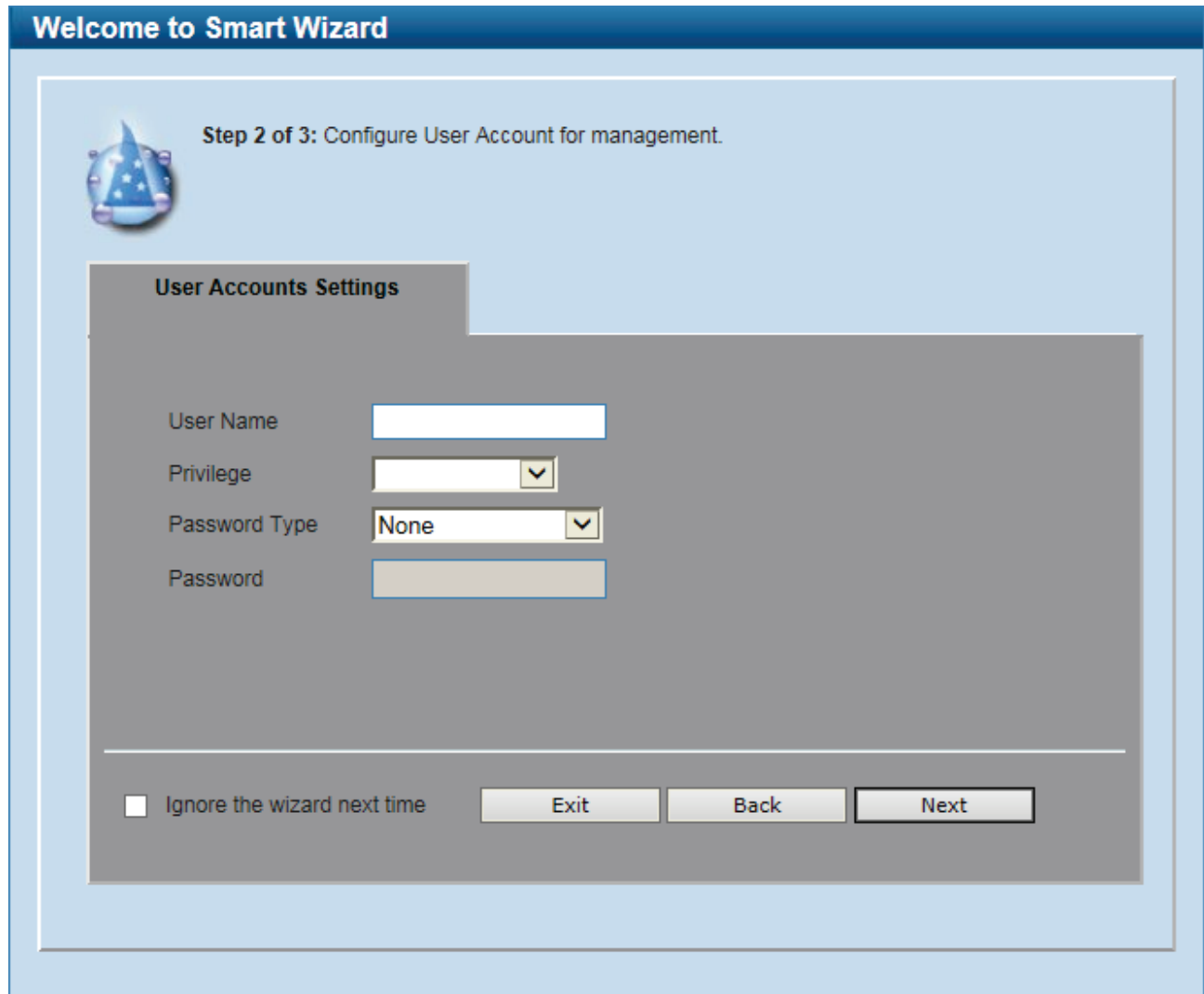
Figure 4.1 – System IP Information in Smart Wizard



NOTE: The Smart Wizard supports quick settings for IPv4 network.

User Accounts Settings

Type the desired new username in the **User Name** field and select the **Privilege** between **User** and **Administrator**. Select **Password Type** among **None**, **Plain Text** and **Encrypted**, and type the desired password in the **Password** field. Click the **Next** button to the SNMP window.



Welcome to Smart Wizard

Step 2 of 3: Configure User Account for management.

User Accounts Settings

User Name

Privilege

Password Type

Password

Ignore the wizard next time

Figure 4.2 – User Accounts Settings in Smart Wizard

SNMP

The SNMP Setting allows you to quickly enable or disable the SNMP function. The default SNMP Setting is *Disabled*. Click **Enabled** and then click **Apply & Save** to make it effective.

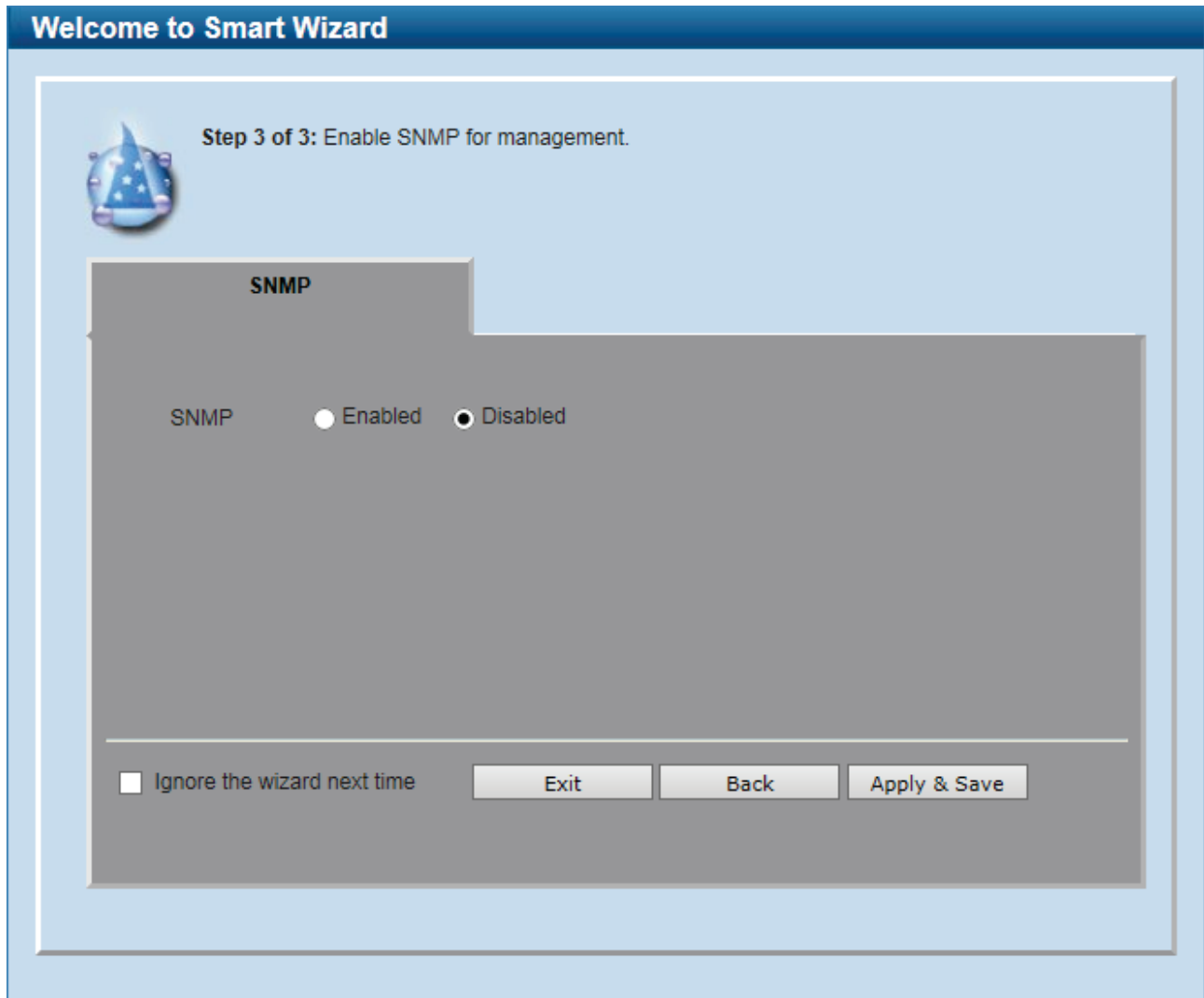


Figure 4.3 – SNMP in Smart Wizard



NOTE: Changing the system IP address will disconnect you from the current connection. Please enter the correct IP address in the Web browser again and make sure your PC is in the same subnet with the switch. See Login Web-based Management for a detailed description.

Web-based Management

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

The screenshot shows the D-Link web-based management interface for a DXS-1100-16TC switch. The interface is divided into three main sections:

- Tool Bar:** Located at the top, it includes a Save button, Tools, Wizard, Online Help, and a Logout button. The user is logged in as Administrator.
- Function Tree:** Located on the left, it lists various configuration categories such as System, Management, L2 Features, L3 Features, QoS, Security, OAM, Monitoring, and Green.
- Main Configuration Screen:** The central area displaying device information and utilization.

| Device Information | | | |
|--------------------|-------------------------------------|---------------|---------------------|
| Device Type | DXS-1100-16TC 10 Gigabit Etherne... | MAC Address | 00-91-06-11-00-01 |
| System Name | Switch | IP Address | 10.90.90.90 |
| System Location | | Mask | 255.0.0.0 |
| System Contact | | Gateway | 0.0.0.0 |
| Boot PROM Version | Build 1.00.003 | System Time | 01/01/2000 01:24:36 |
| Firmware Version | Build 1.10.002 | Serial Number | |
| Hardware Version | A1 | | |

| Utilization | |
|---------------|-------------------------------------|
| CPU | Average: 40 % Current: 45 % |
| Flash | 79602KB Total, 18190KB Used (19 %) |
| Memory | 182298KB Total, 79846KB Used (30 %) |

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 on the left, and the username with current IP address and the **Logout** button on the right. Click **Logout** 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.

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.

Finally, by clicking the D-Link logo at the upper-left corner of the screen you will be redirected to the D-Link website.

Tool Bar > Save Menu

The Save Menu provides the Save Configuration function.

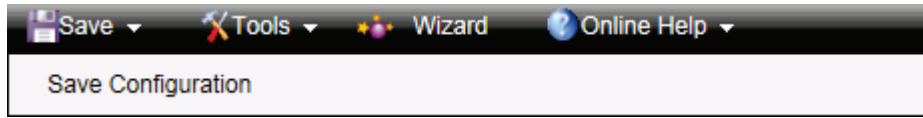


Figure 4.5 – Save Menu

Save Configuration

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

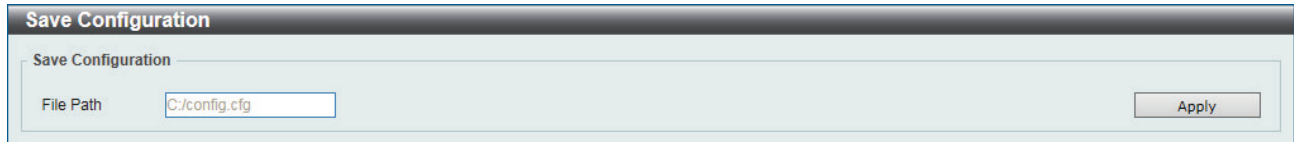


Figure 4.6 – Save Configuration

Tool Bar > Tools Menu

The Tools Menu offers global function controls Firmware Upgrade & Backup, Configuration Restore & Backup, Log Backup, Ping, Reset, and Reboot System.

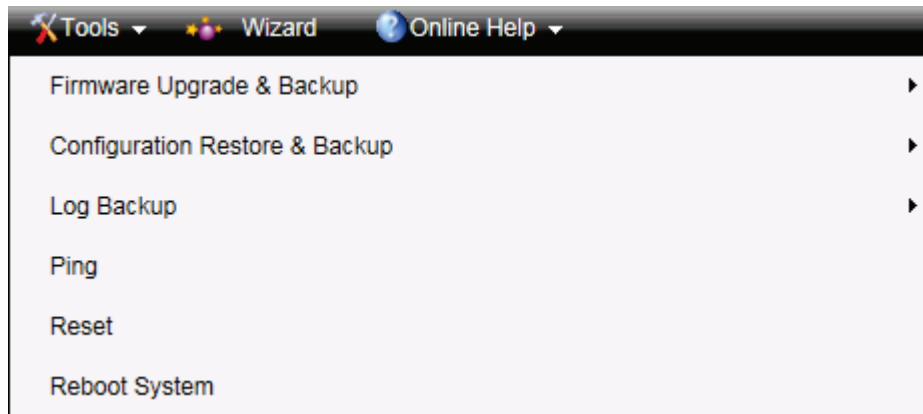


Figure 4.7 – Tools Menu

Firmware Upgrade and Backup

Allow for the firmware to be saved, or for an existing firmware file to be uploaded to the Switch. The Switch can only allow having maximum 2 firmware files saved in the File System. Go to **Management > File System** to delete the old firmware files in order to upgrade firmware successfully. The Two methods can be selected: **HTTP** or **TFTP**.

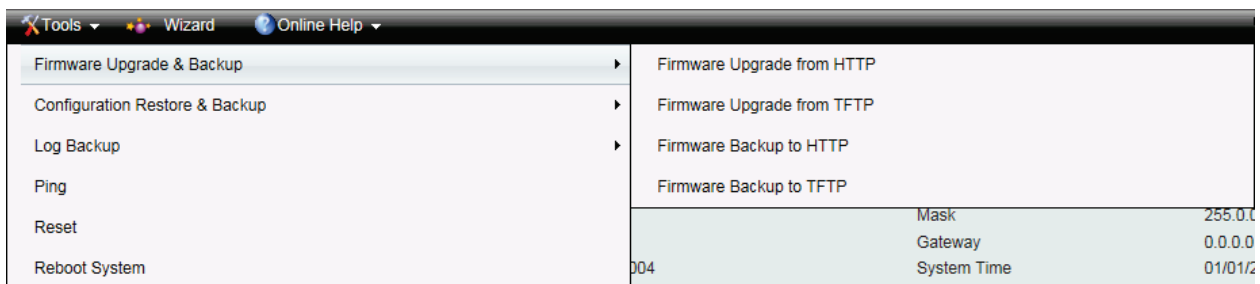


Figure 4.8 – Tools Menu > Firmware Upgrade and Backup

Firmware Upgrade from HTTP

This window is used to upgrade the firmware from HTTP.

Figure 4.9 – Tools Menu > Firmware Upgrade and Backup > Firmware Upgrade from HTTP

The fields that can be configured are described below:

Source File: Click **Browse** to browse your inventories for a saved firmware file.

Destination File: Enter the destination filename and path where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

Click **Upgrade** after selecting the firmware file you want to restore.

Firmware Upgrade from TFTP

This window is used to upgrade the firmware from TFTP.

Figure 4.10 – Tools Menu > Firmware Upgrade and Backup > Firmware Upgrade from TFTP

The fields that can be configured are described below:

TFTP Server IP: Upgrade the firmware from a remote TFTP server. Specify TFTP server IP address with IPv4 or IPv6 address.

Source File: Enter the source filename and path of the firmware file located on the TFTP server here. This field can be up to 64 characters long.

Destination File: Enter the destination filename and path where the new firmware should be stored on the Switch. This field can be up to 64 characters long.

Click **Upgrade** after selecting the firmware file you want to restore.



CAUTION: Do not disconnect the PC or remove the power cord from the Switch until the upgrade completes. The Switch may crash if the firmware upgrade is incomplete.

Firmware Backup to HTTP

This window is used to back up the firmware to HTTP.

Figure 4.11 – Tools Menu > Firmware Upgrade and Backup > Firmware Backup to HTTP

The fields that can be configured are described below:

Source File: Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.

Click **Backup** to save the firmware to your disk.

Firmware Backup to TFTP

This window is used to back up the firmware to TFTP.

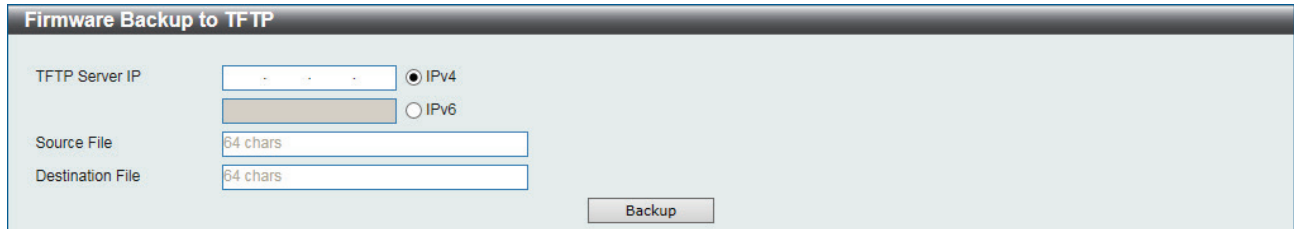


Figure 4.12 – Tools Menu > Firmware Upgrade and Backup > Firmware Backup to TFTP

The fields that can be configured are described below:

TFTP Server IP: Backup the firmware to a remote TFTP server. Specify TFTP server IP address with IPv4 or IPv6 address.

Source File: Enter the source filename and path of the firmware file located on the Switch here. This field can be up to 64 characters long.

Destination File: Enter the destination filename and path where the firmware should be stored on the TFTP server. This field can be up to 64 characters long.

Click **Backup** to save the firmware to the TFTP server.

Configuration Restore and Backup

Allow the current configuration settings to be saved to a file (not including the password), and if necessary, you can restore the configuration settings from this file. The Switch can only allow having maximum 2 configuration files saved in the File System. Go to **Management > File System** to delete the old configuration files in order to restore configurations successfully. Two methods can be selected: **HTTP** or **TFTP**.

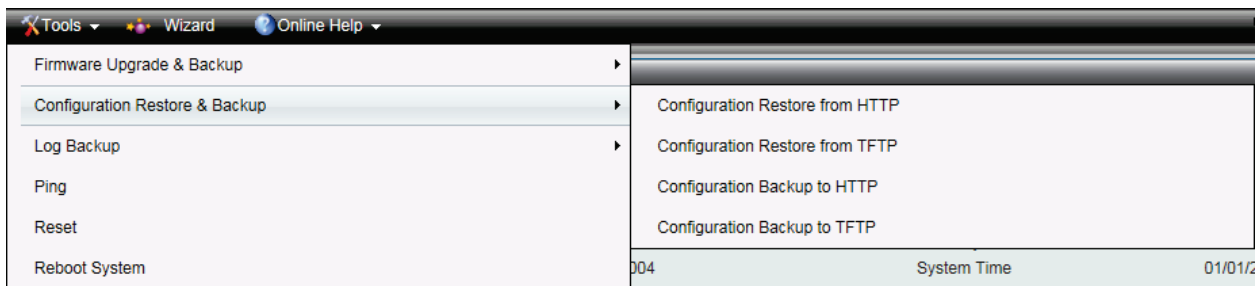


Figure 4.13 – Tools Menu > Configure Restore and Backup

Configuration Restore from HTTP

This window is used to restore the configuration from HTTP.

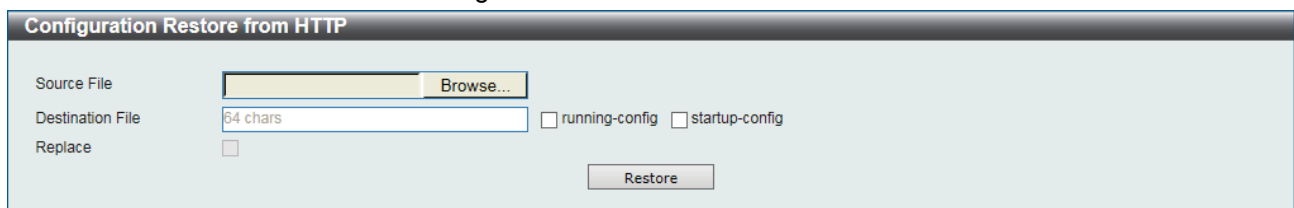


Figure 4.14 – Tools Menu > Configure Restore and Backup > Configuration Restore from HTTP

The fields that can be configured are described below:

Source File: Click **Browse** to browse your inventories for a saved firmware file.

Destination File: Enter the destination filename and path where the configuration file should be stored on the Switch. This field can be up to 64 characters long. Select the **running-config** option to restore and overwrite the running configuration file on the Switch. Select the **startup-config** option to restore and overwrite the start-up configuration file on the Switch.

Replace: Replace the current running configuration.

Click **Restore** after selecting the backup settings file you want to restore.

Configuration Restore from TFTP

This window is used to restore the configuration from TFTP.

Figure 4.15 – Tools Menu > Configure Restore and Backup > Configuration Restore from TFTP

The fields that can be configured are described below:

TFTP Server IP: Restore the configuration from a remote TFTP server. Specify TFTP server IP address with IPv4 or IPv6 address.

Source File: Enter the source filename and path of the configuration file located on the TFTP server here. This field can be up to 64 characters long.

Destination File: Enter the destination filename and path where the configuration file should be stored on the Switch. This field can be up to 64 characters long. Select the **running-config** option to restore and overwrite the running configuration file on the Switch. Select the **startup-config** option to restore and overwrite the start-up configuration file on the Switch.

Replace: Replace the current running configuration.

Click **Restore** after selecting the backup settings file you want to restore.

Configuration Backup to HTTP

This window is used to back up the configuration to HTTP.

Figure 4.16 – Tools Menu > Configure Restore and Backup > Configuration Backup to HTTP

The fields that can be configured are described below:

Source File: Enter the source filename and path of the configuration file located on the Switch here. This field can be up to 64 characters long. Select the **running-config** option to back up the running configuration file from the Switch. Select the **startup-config** option to back up the start-up configuration file from the Switch.

Click **Backup** to save the current settings to your disk.

Configuration Backup to TFTP

This window is used to back up the configuration to TFTP.

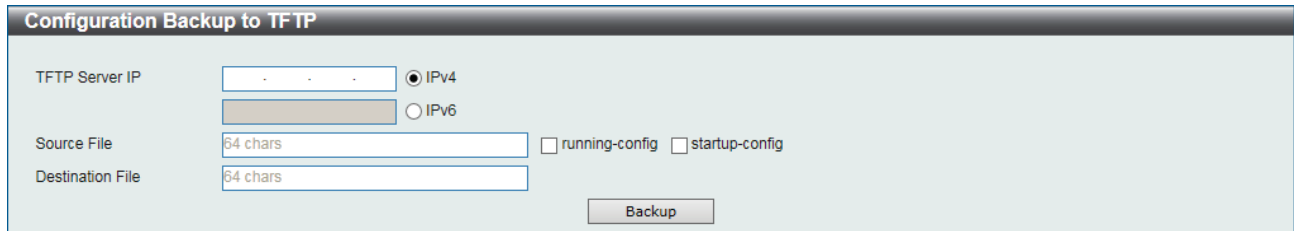


Figure 4.17 – Tools Menu > Configure Restore and Backup > Configuration Backup to TFTP

The fields that can be configured are described below:

TFTP Server IP: Back up the configuration from a remote TFTP server. Specify TFTP server IP address with IPv4 or IPv6 address.

Source File: Enter the source filename and path of the configuration file located on the switch here. This field can be up to 64 characters long. Select the **running-config** option to back up the running configuration file from the Switch. Select the **startup-config** option to back up the start-up configuration file from the Switch.

Destination File: Enter the destination filename and path where the configuration file should be stored on the TFTP server. This field can be up to 64 characters long.

Click **Backup** to save the current settings to the TFTP server.

Log Backup

Allow the logs to be saved to HTTP or TFTP.

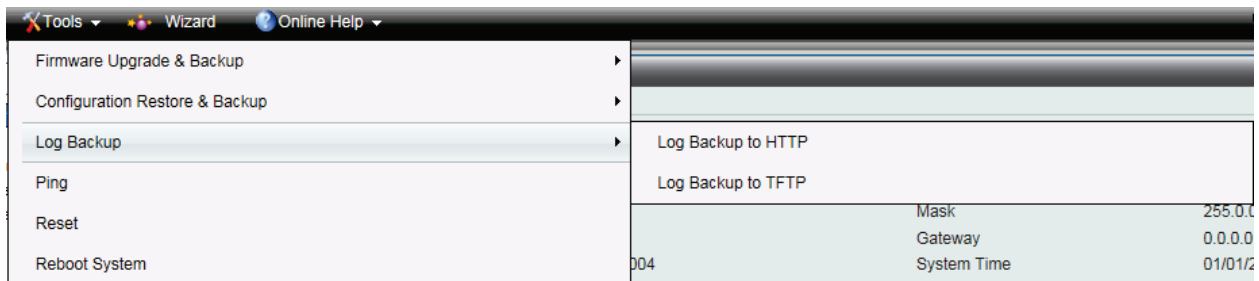


Figure 4.18 – Tools Menu > Log Backup

Log Backup to HTTP

This window is used to back up the logs to HTTP.

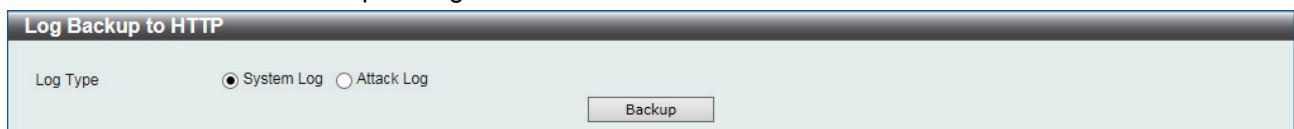


Figure 4.19 – Tools Menu > Log Backup > Log Backup to HTTP

The fields that can be configured are described below:

Log Type: Select the log type that will be backed up to the local PC using HTTP. When the **System Log** option is selected, the system log will be backed up. When the **Attack Log** is selected, the attack log will be backed up.

Click **Backup** to save the current settings to your disk.

Log Backup to TFTP

This window is used to back up the logs to TFTP.

Figure 4.20 – Tools Menu > Log Backup > Log Backup to TFTP

The fields that can be configured are described below:

TFTP Server IP: Back up the log from a remote TFTP server. Specify TFTP server IP address with IPv4 or IPv6 address.

Destination File: Enter the destination filename and path where the log file should be stored on the TFTP server. This field can be up to 64 characters long.

Log Type: Select the log type that will be backed up to the TFTP server. When the **System Log** option is selected, the system log will be backed up. When the **Attack Log** is selected, the attack log will be backed up.

Click **Backup** to save the current settings to the TFTP server.

Ping

Ping is a small program that sends ICMP Echo packets to the IP address you specify. The destination node then responds to or “echoes” the packets sent from the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.

Figure 4.21 – Tools Menu > Ping

The fields that can be configured are described below:

Target IPv4 Address / Target IPv6 Address: Enter an IPv4 or IPv6 address to be pinged. If the IPv6 address is a link-local address or a multicast address, the IP interface name needs to be specified in the following format: *IPV6-ADDRESS%INTERFACE-ID*.

Ping Times: Enter the number of times desired to attempt to Ping the IPv4 or IPv6 address. Users may enter a number of times between 1 and 255. Tick **Infinite** to keep sending ICMP Echo packets to the specified IPv4 or IPv6 address until the program is stopped.

Timeout: Select a timeout period between 1 and 99 seconds for this Ping message to reach its destination. If the packet fails to find the IPv4 or IPv6 address in this specified time, the Ping packet will be dropped.

Click **Start** to initiate the Ping Test for each individual section.

After clicking **Start**, the Ping Result section will appear:

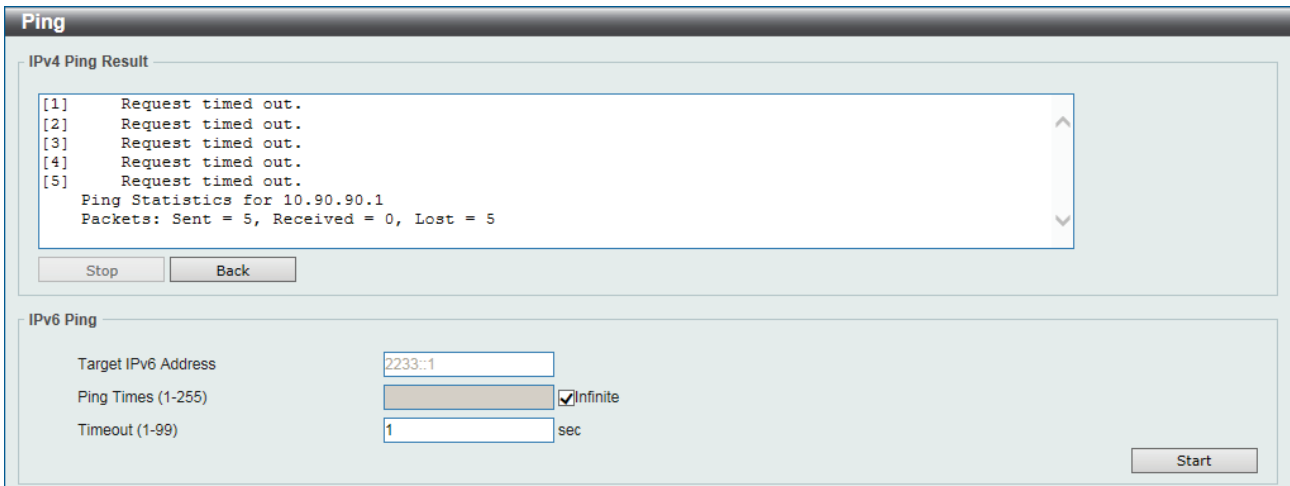


Figure 4.22 – IPv4 Ping Result

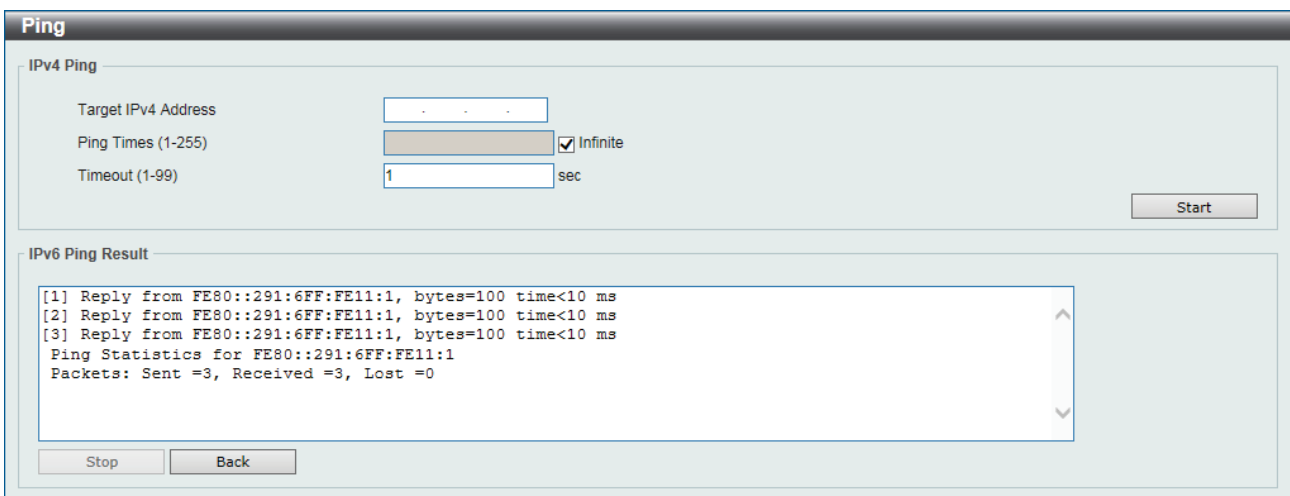


Figure 4.23 – IPv6 Ping Result

Click **Stop** to halt the Ping Test.

Click **Back** to return to the IPv4 or IPv6 Ping section.

Reset

Provide a safe reset option for the Switch.

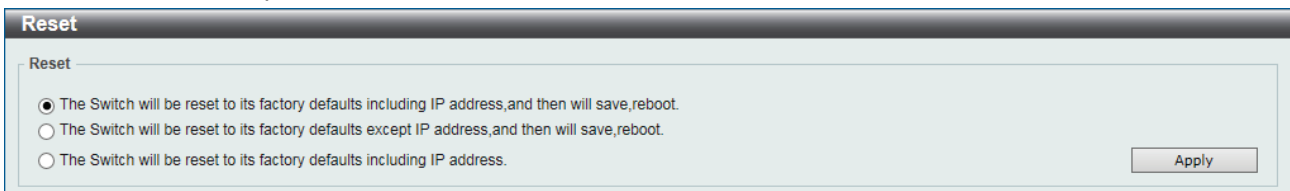


Figure 4.24 – Tools Menu > Reset

Select the **The Switch will be reset to its factory defaults including IP address, and then will save, reboot.** option to reset the Switch’s configuration to its factory default settings.

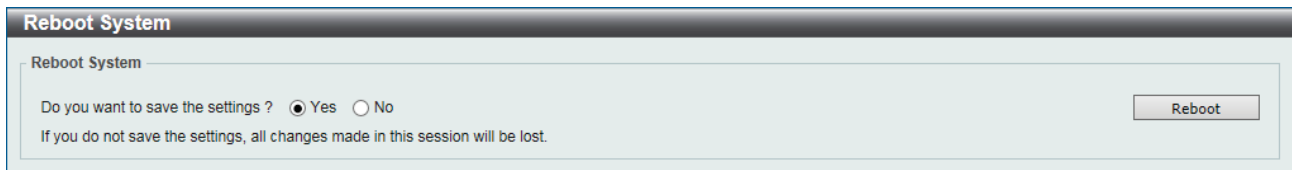
Select the **The Switch will be reset to its factory defaults except IP address, and then will save, reboot** option to reset the Switch’s configuration to its factory default settings. This option will exclude the IP address from being changed.

Select the **The Switch will be reset to its factory defaults including IP address** option to reset the Switch’s configuration to its factory default settings.

Click **Apply** to initiate the factory default reset and reboot the Switch.

Reboot System

Provide a safe way to reboot the system. Click **Yes** and **Apply** to restart the Switch.



Reboot System

Reboot System

Do you want to save the settings ? Yes No

If you do not save the settings, all changes made in this session will be lost.

Reboot

Figure 4.25 – Tools Menu > Reboot Device

Tool Bar > Wizard

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

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 images; **User Guide** can offer an immediate reference for the feature definition or configuration guide.

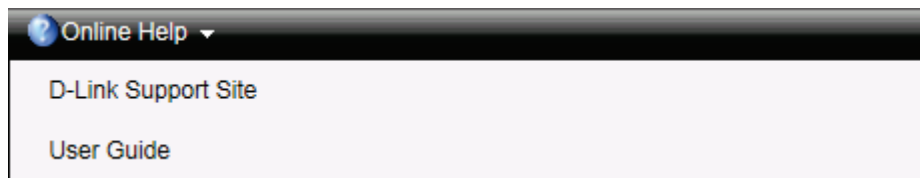


Figure 4.26 – Online Help

Function Tree

All configuration options on the Switch are accessed through the Function Tree. Click the setup item that you want to configure. The following sections provide more detailed description of each feature and function.

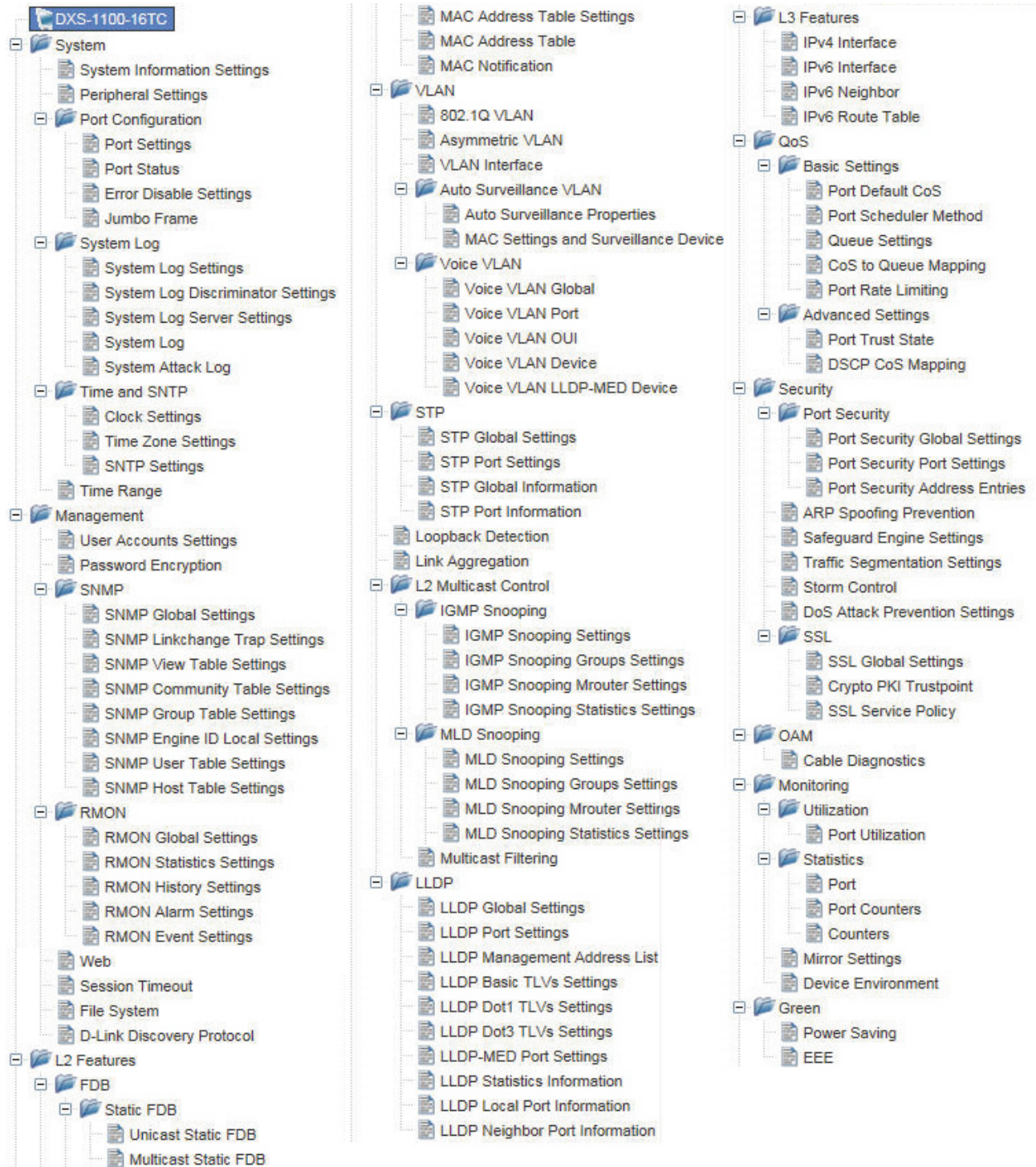


Figure 4.27 – Available settings in the Function Tree

Device Information

In this window, the Device Information, CPU, and Used status are displayed. It appears automatically when you log in the Switch.

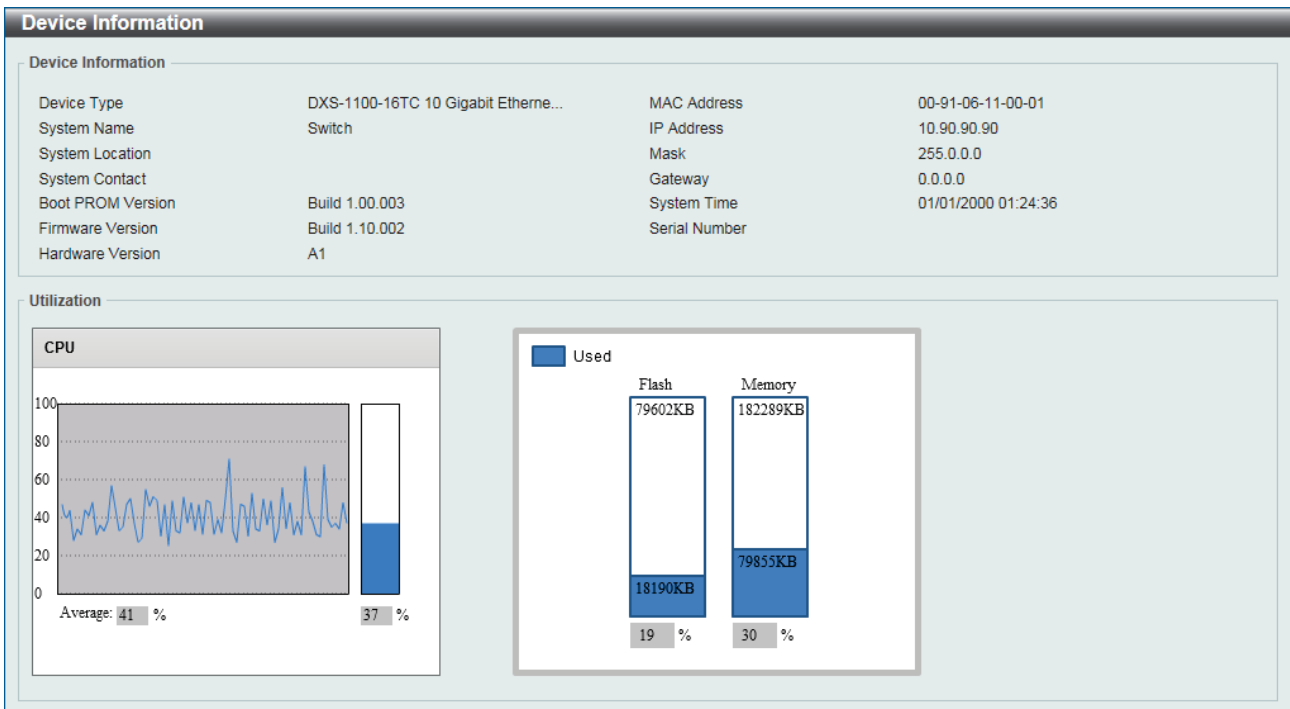


Figure 4.28 – Device Information

System > System Information Settings

The System Information Settings allows the user to configure a System Name, System Location, and System Contact to aid in defining the Switch.

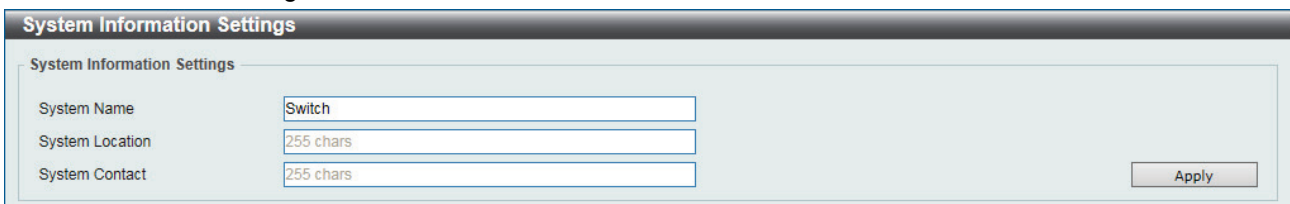


Figure 4.29 – System > System Information Settings

The fields that can be configured are described below:

System Name: Enter a system name for the Switch, if so desired. This name will identify it in the Switch network.

System Location: Enter the location of the Switch, if so desired. This string can be up to 255 characters long.

System Contact: Enter a contact name for the Switch, if so desired. This string can be up to 255 characters long.

System > Peripheral Settings

This window is used to configure the environment trap settings and environment temperature threshold settings.

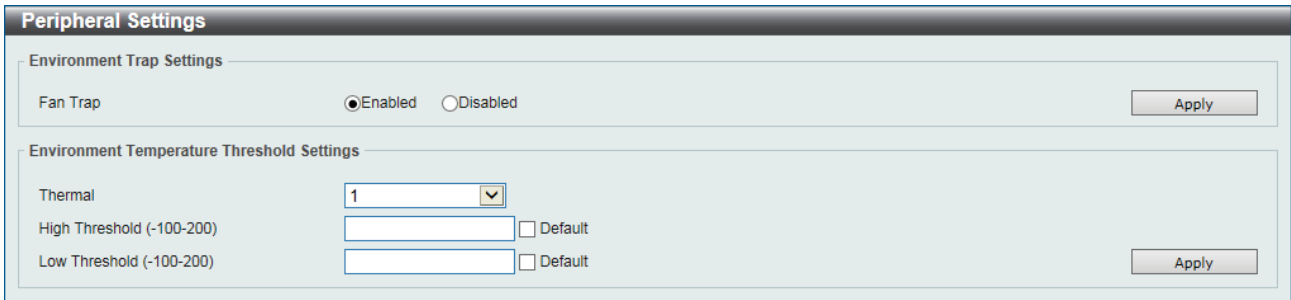


Figure 4.30 – System > Peripheral Settings

The fields that can be configured are described below:

Fan Trap: Enable or disable the fan trap state for warning fan event (fan failed or fan recover).

Thermal: Select the thermal sensor ID.

High Threshold: Enter the high threshold value of the warning temperature setting. The range is from -100 to 200 Celsius degree. Tick **Default** to return to the default value. The default value is 79.

Low Threshold: Enter the low threshold value of the warning temperature setting. The range is from -100 to 200 Celsius degree. Tick **Default** to return to the default value. The default value is 11.

Click **Apply** to accept the changes made for each individual section.

System > Port Configuration > Port Settings

This window is used to view and configure the Switch’s port settings.

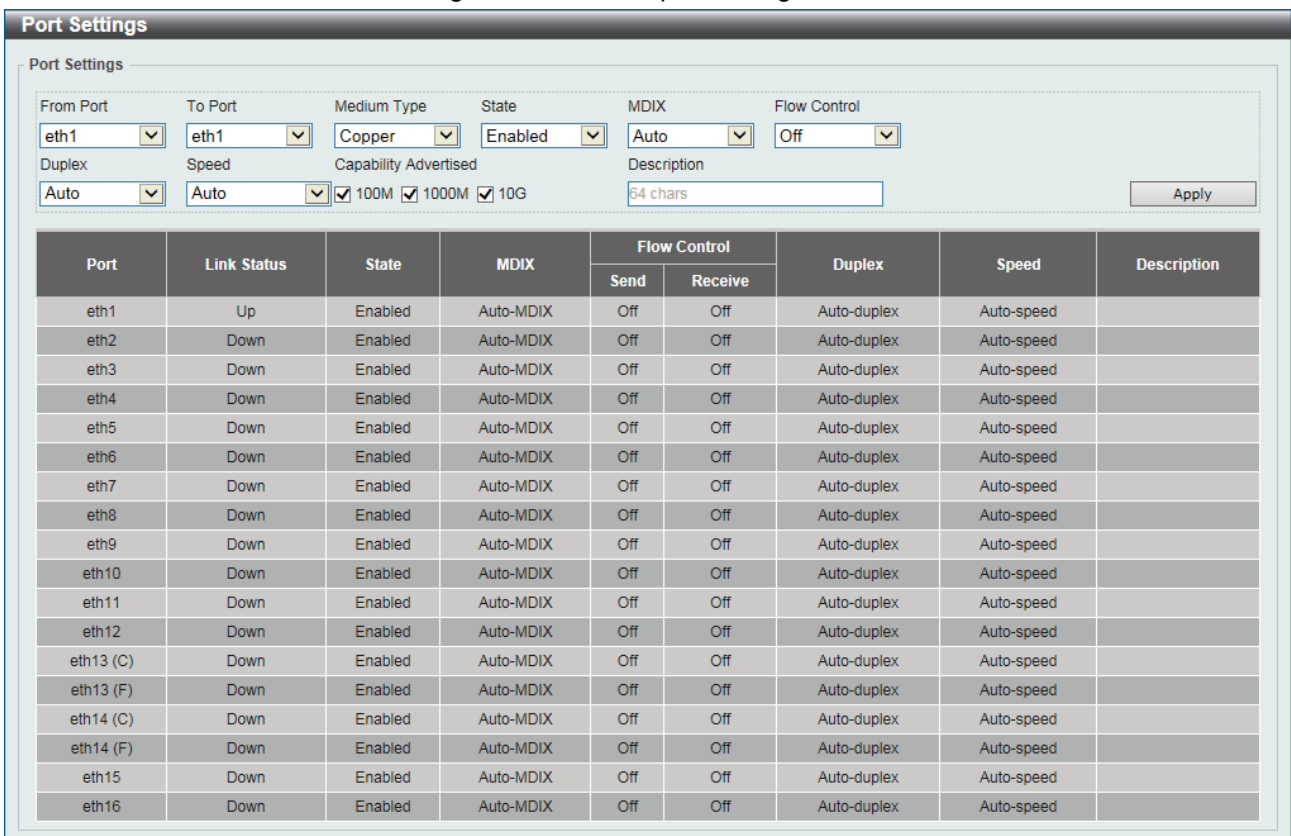


Figure 4.31 – System > Port Configuration > Port Settings

The fields that can be configured are described below:

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

Medium Type: If configuring the Combo ports, this defines the type of transport medium to be used.

State: Select this option to enable or disable the physical port here.

MDIX: Select the Medium Dependent Interface Crossover (MDIX) option here. This is only available when the copper port is selected. Options to choose from are **Auto**, **Normal**, and **Cross**.

Auto - Select this option for auto-sensing of the optimal type of cabling.

Normal - Select this option for normal cabling. If this option is selected, the port is in the MDIX mode and can be connected to a PC's NIC using a straight-through cable or a port (in the MDIX mode) on another switch through a cross-over cable.

Cross - Select this option for cross cabling. If this option is selected, the port is in the MDI mode and can be connected to a port (in the MDIX mode) on another switch through a straight cable.

Flow Control: Select to either turn flow control **On** or **Off** here. 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 here. Options to choose from are **Auto**, and **Full**.

Speed: Select the port speed option here. This option will manually force the connected on the selected port to only connect at the speed specified here. Options to choose from are **Auto**, **100M**, **1000M**, **1000M Master**, **1000M Slave**, and **10G**. The Switch allows users 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** and the copper port is selected, these capabilities are advertised during auto-negotiation.

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

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

System > Port Configuration > Port Status

This window is used to view the Switch's physical port status and settings.

| Port Status | | | | | | | | |
|-------------|---------------|-------------------|------|-----------------------|---------|-----------|-----------|-----------|
| Port | Status | MAC Address | VLAN | Flow Control Operator | | Duplex | Speed | Type |
| | | | | Send | Receive | | | |
| eth1 | Connected | 00-77-93-03-00-01 | 1 | Off | Off | Auto-Full | Auto-100M | 10GBASE-T |
| eth2 | Not-Connected | 00-77-93-03-00-02 | 1 | Off | Off | Auto | Auto | 10GBASE-T |
| eth3 | Not-Connected | 00-77-93-03-00-03 | 1 | Off | Off | Auto | Auto | 10GBASE-T |
| eth4 | Not-Connected | 00-77-93-03-00-04 | 1 | Off | Off | Auto | Auto | 10GBASE-T |
| eth5 | Not-Connected | 00-77-93-03-00-05 | 1 | Off | Off | Auto | Auto | 10GBASE-T |
| eth6 | Not-Connected | 00-77-93-03-00-06 | 1 | Off | Off | Auto | Auto | 10GBASE-T |
| eth7 | Not-Connected | 00-77-93-03-00-07 | 1 | Off | Off | Auto | Auto | 10GBASE-T |
| eth8 | Not-Connected | 00-77-93-03-00-08 | 1 | Off | Off | Auto | Auto | 10GBASE-T |
| eth9 | Not-Connected | 00-77-93-03-00-09 | 1 | Off | Off | Auto | Auto | 10GBASE-T |
| eth10 | Not-Connected | 00-77-93-03-00-0A | 1 | Off | Off | Auto | Auto | 10GBASE-T |
| eth11 | Not-Connected | 00-77-93-03-00-0B | 1 | Off | Off | Auto | Auto | 10GBASE-T |
| eth12 | Not-Connected | 00-77-93-03-00-0C | 1 | Off | Off | Auto | Auto | 10GBASE-T |
| eth13 | Not-Connected | 00-77-93-03-00-0D | 1 | Off | Off | Auto | Auto | 10GBASE-T |
| eth14 | Not-Connected | 00-77-93-03-00-0E | 1 | Off | Off | Auto | Auto | 10GBASE-T |
| eth15 | Not-Connected | 00-77-93-03-00-0F | 1 | Off | Off | Auto | Auto | 10GBASE-R |
| eth16 | Not-Connected | 00-77-93-03-00-10 | 1 | Off | Off | Auto | Auto | 10GBASE-R |

Figure 4.32 – System > Port Configuration > Port Status

System > Port Configuration > Error Disable Settings

This window is used to configure the sending of SNMP notifications for error disable state.

Error Disable Settings

Error Disable Trap Settings

Asserted:

Cleared:

Notification Rate (0-1000):

Error Disable Recovery Settings

ErrDisable Cause: State: Interval (5-86400): sec

| ErrDisable Cause | State | Interval (sec) |
|------------------|----------|----------------|
| Port Security | Disabled | 300 |
| Storm Control | Disabled | 300 |
| Loopback Detect | Disabled | 300 |

Interfaces that will be recovered at the next timeout:

| Interface | VLAN | ErrDisable Cause | Time Left (sec) |
|-----------|------|------------------|-----------------|
|-----------|------|------------------|-----------------|

Figure 4.33 – System > Port Configuration > Error Disable Settings

The fields that can be configured are described below:

Asserted: Select this option to enable or disable the notifications when entering into the error disabled state.

Cleared: Select this option to enable or disable the notifications when exiting from the error disabled state.

Notification Rate: Enter the number of traps per minute. The packets that exceed the rate will be dropped. The value is between 0 and 1000.

ErrDisable Cause: Select the error disable causes here. Options to choose from are All, Port Security, Storm Control, and Loopback Detect.

State: Select this option to enable or disable the auto-recovery for an error port caused by the specified cause.

Interval: Enter the time between 5 and 86400 seconds to recover the port.

Click **Apply** to accept the changes made for each individual section.

System > Port Configuration > Jumbo Frame

This window is used to view and configure the Jumbo Frame size and settings. The Switch supports jumbo frames. Jumbo frames are Ethernet frames with more than 1,536 bytes of payload. The Switch supports jumbo frames with a maximum frame size of up to 9,216 bytes.

Jumbo Frame

Jumbo Frame

From Port: eth1 | To Port: eth1 | Maximum Receive Frame Size (64-9216): 1536 bytes [Apply]

| Port | Maximum Receive Frame Size (bytes) |
|-------|------------------------------------|
| eth1 | 1536 |
| eth2 | 1536 |
| eth3 | 1536 |
| eth4 | 1536 |
| eth5 | 1536 |
| eth6 | 1536 |
| eth7 | 1536 |
| eth8 | 1536 |
| eth9 | 1536 |
| eth10 | 1536 |
| eth11 | 1536 |
| eth12 | 1536 |
| eth13 | 1536 |
| eth14 | 1536 |
| eth15 | 1536 |
| eth16 | 1536 |

Figure 4.34 – System > Port Configuration > Jumbo Frame

The fields that can be configured are described below:

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

Maximum Receive Frame Size: Enter the maximum receive frame size value here. This value must be between 64 and 9216 bytes. By default, this value is 1536 bytes.

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

System > System Log > System Log Settings

This window is used to view and configure the system’s log settings. System logs record and manage events, as well as report errors and informational messages.

System Log Settings

Global State

Source Interface State: Enabled [Apply]

Buffer Log Settings

Buffer Log State: Enabled [Apply]

Severity: 4(Warnings)

Discriminator Name: 15 chars

Write Delay (0-65535): 300 sec Infinite [Apply]

Figure 4.35 – System > System Log > System Log Settings

The fields that can be configured are described below:

Source Interface State: Enable or disable the source interface’s global state.

Buffer Log State: Enable or disable the buffer log’s global state here. Options to choose from are Enable, Disabled, and Default. When selecting the Default option, the buffer log’s global state will follow the default behavior.

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).**

Discriminator Name: Enter the discriminator name used here. This name can be up to 15 characters long.

Write Delay: Enter the interval for periodic writing of the logging buffer to FLASH. This value must be between 0 and 65535 seconds. By default, this value is 300 seconds. Tick **Infinite** to disable the write delay feature.

Click **Apply** to accept the changes made for each individual section.

System > System Log > System Log Discriminator Settings

This window is used to view and configure the system log’s discriminator settings.

| Name | Action | Facility List | Severity | Severity List | |
|-----------------|--------|-------------------------|----------|---------------|--------|
| Discriminato... | Drops | VOICE_VLAN,DEVICE,MA... | Drops | 4 | Delete |

Figure 4.36 – System > System Log > System Log Discriminator Settings

The fields that can be configured are described below:

Discriminator Name: Enter the discriminator name here. This name can be up to 15 characters long.

Action: Select the facility’s behavior option and the type of facility that will be associated with the selected behavior here. Behavior options to choose from are **Drops** and **Includes**.

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

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

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

System > System Log > System Log Server Settings

This window is used to view and configure system log’s server settings.

| Server IP | Severity | Facility | Discriminator Name | UDP Port | |
|-------------|----------|----------|--------------------|----------|--------|
| 10.90.90.25 | Warnings | 23 | | 514 | Delete |

Figure 4.37 – System > System Log > System Log Server Settings

The fields that can be configured are described below:

Host IPv4 Address: Specifies the IPv4 address of the system log server.

Host IPv6 Address: Specifies the IPv6 address of the system log server.

UDP Port: Specifies the UDP port to which the server logs are sent. 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 here. Options to choose from are 0 to 23.

Discriminator Name: Enter the discriminator name here. This name can be up to 15 characters long.

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

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

System > System Log > System Log

This window is used to view and clear the system log. The maximum number of entries that will be displayed in this table is 1,000. The index number can go up to 90,000. When this log is full, older entries will be removed and replaced by newer ones.

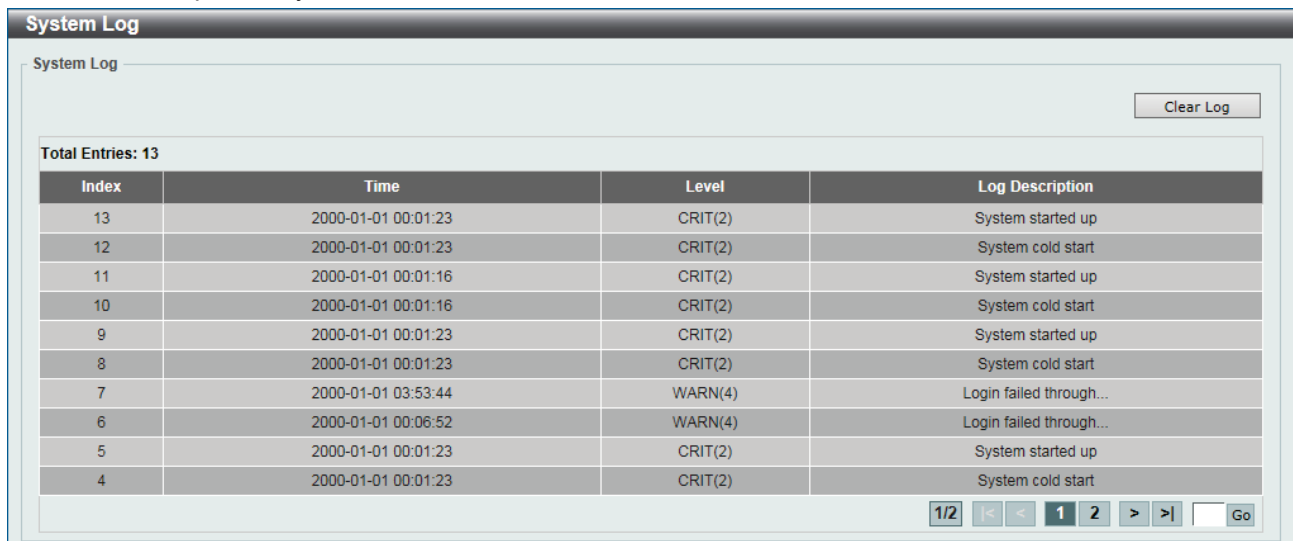


Figure 4.38 – System > System Log > System Log

Click **Clear Log** to clear the system log entries displayed in the table.

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

System > System Log > System Attack Log

This window is used to view and clear the system attack log. The maximum number of entries that will be displayed in this table is 1,000. The index number can go up to 90,000. When this log is full, older entries will be removed and replaced by newer ones.

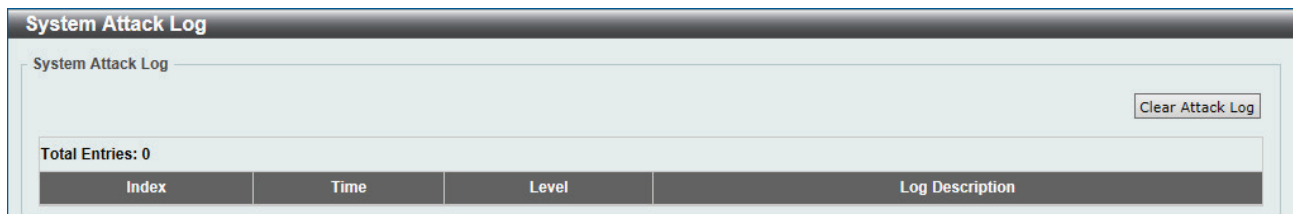


Figure 4.39 – System > System Log > System Attack Log

Click **Clear Attack Log** to clear the system attack log entries displayed in the table.

System > Time and SNTP > Clock Settings

The Simple Network Time Protocol (SNTP) is a protocol for synchronizing computer clocks through the Internet. It provides comprehensive mechanisms to access national time and frequency dissemination services, organize the SNTP subnet of servers and clients, and adjust the system clock in each participant. This window is used to configure the time settings for the Switch.

Figure 4.40 – System > Time and SNTP > Clock Settings

The fields that can be configured are described below:

Time (HH MM:SS): Enter the current time in hours, minutes, and seconds.

Date (DD/MM/YYYY): Enter the current day, month, and year to update the system clock.

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

System > Time and SNTP > Time Zone Settings

This window is used to configure time zones and Daylight Savings Time settings for SNTP.

Figure 4.41 – System > Time and SNTP > Time Zone Settings

The fields that can be configured are described below:

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

Disabled - Select to disable the summer time setting.

Recurring Setting - Select to configure the summer time that should start and end on the specified week day of the specified month.

Date Setting - Select to configure the summer time that should start and end on the specified date of the specified month.

Time Zone: Select to specify your local time zone's offset from Coordinated Universal Time (UTC).

From: Week of the Month: Select week of the month that summer time will start.

From: Day of the Week: Select the day of the week that summer time will start.

From: Month: Select the month that summer time will start.

From: Time (HH:MM): Select the time of the day that summer time will start.

To: Week of the Month: Select week of the month that summer time will end.

To: Day of the Week: Select the day of the week that summer time will end.

To: Month: Select the month that summer time will end.

To: Time (HH:MM): Select the time of the day that summer time will end.

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

From: Date of the Month: Select date of the month that summer time will start.

From: Month: Select the month that summer time will start.

From: Year: Enter the year that the summer time will start.

From: Time (HH:MM): Select the time of the day that summer time will start.

To: Date of the Month: Select date of the month that summer time will end.

To: Month: Select the month that summer time will end.

To: Year: Enter the year that the summer time will end.

To: Time (HH:MM): Select the time of the day that summer time will end.

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

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

System > Time and SNTP > SNTP Settings

This window is used to configure the time settings for the Switch.

| SNTP server | Stratum | Version | Last Receive |
|-------------|---------|---------|--------------|
| 10.90.90.1 | - | - | - |

Figure 4.42 – System > Time and SNTP > SNTP Settings

The fields that can be configured are described below:

SNTP State: Select this option to enable or disable SNTP.

Poll Interval: Enter the synchronizing interval in seconds. The value is from 30 to 99999 seconds. The default interval is 720 seconds.

IPv4 Address: Enter the IP 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 **Apply** to accept the changes made.

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

System > Time Range

This window is used to view and configure the time range settings.

Figure 4.43 – System > Time Range

The fields that can be configured are described below:

Range Name: Enter the name of the time range. This 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 **Daily** to use this time range for every day of the week. Tick **End Weekday** 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 **Apply** to accept the changes made.

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

Click **Delete Periodic** to delete the periodic entry.

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

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

Management > User Accounts Settings

This window is used to create and configure the user accounts. The active user account sessions can be viewed.

There are two user account privilege available, User and Administrator:

- User - This user account level has the lower priority of the user accounts. The purpose of this type of user account level is for basic system checking.
- Administrator - This administrator user account level can monitor all system information and change any of the system configuration settings expressed in this guide.

User Accounts Settings

User Management Settings **Session Table**

User Name: 32 chars Privilege: User
 Password Type: None Password: [] **Apply**

Total Entries: 1

| User Name | Privilege | Password |
|-----------|---------------|----------|
| admin | Administrator | ***** |

1/1 [] [] 1 [] [] **Go**

Figure 4.44 – Management > User Accounts Settings (User Management Settings)

The fields that can be configured are described below:

User Name: Enter the user account name here. This name can be up to 32 characters long.

Privilege: Select the privilege level for this account.

Password Type: Select the password type for this user account here. Options to choose from are **None**, **Plain Text** and **Encrypted**. When selecting Encrypted, the password will not be encrypted from the plain-text format to the encrypted format. Instead, the encrypted password must be entered.

Password: After selecting **Plain Text** or **Encrypted** as the **Password Type**, enter the password for this user account here.

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

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

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

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

User Accounts Settings

User Management Settings **Session Table**

Total Entries: 1

| Type | User Name | Login Time | IP Address |
|-------|-----------|------------|-------------|
| * web | admin | 1H0M9S | 10.90.90.15 |

[] **Go**

Figure 4.45 – Management > User Accounts Settings (Session Table)

A list of active user account session will be displayed.

Management > Password Encryption

This window is used to configure whether to save the encryption of the password in the configuration file.

Password Encryption

Password Encryption Settings

Password Encryption State Enabled Disabled **Apply**

Figure 4.46 – Management > Password Encryption

The fields that can be configured are described below:

Password Encryption State: Enable or disable the encryption of the password before stored in the configuration file.

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

Management > SNMP > SNMP Global Settings

This window is used to configure the SNMP global settings and trap settings.

Figure 4.47 – Management > SNMP > SNMP Global Settings

The fields that can be configured are described below:

SNMP Global State: Enable or disable the SNMP feature.

SNMP Response Broadcast Request: Enable or disable the server to response to broadcast SNMP GetRequest packets.

SNMP UDP Port: Enter the SNMP UDP port number.

Trap Global State: 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 sending of port link up notifications. A linkup trap is generated when the device recognizes that one of the communication links has come up.

Port Link Down: Tick this option to control the sending of port link down notifications. A linkDown trap is generated when the device recognizes a failure in one of the communication links.

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

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

Upload Image: Tick this option to enable the sending of notifications when the image is uploaded successfully.

Download Image: Tick this option to enable the sending of notifications when the image is downloaded successfully.

Upload Configuration: Tick this option to enable the sending of notifications when the configuration is uploaded successfully.

Download Configuration: Tick this option to enable the sending of notifications when the configuration is downloaded successfully.

Save Configuration: Tick this option to enable the sending of notifications when the configuration is saved.

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

Management > SNMP > SNMP Linkchange Trap Settings

This window is used to configure the SNMP link change trap settings.

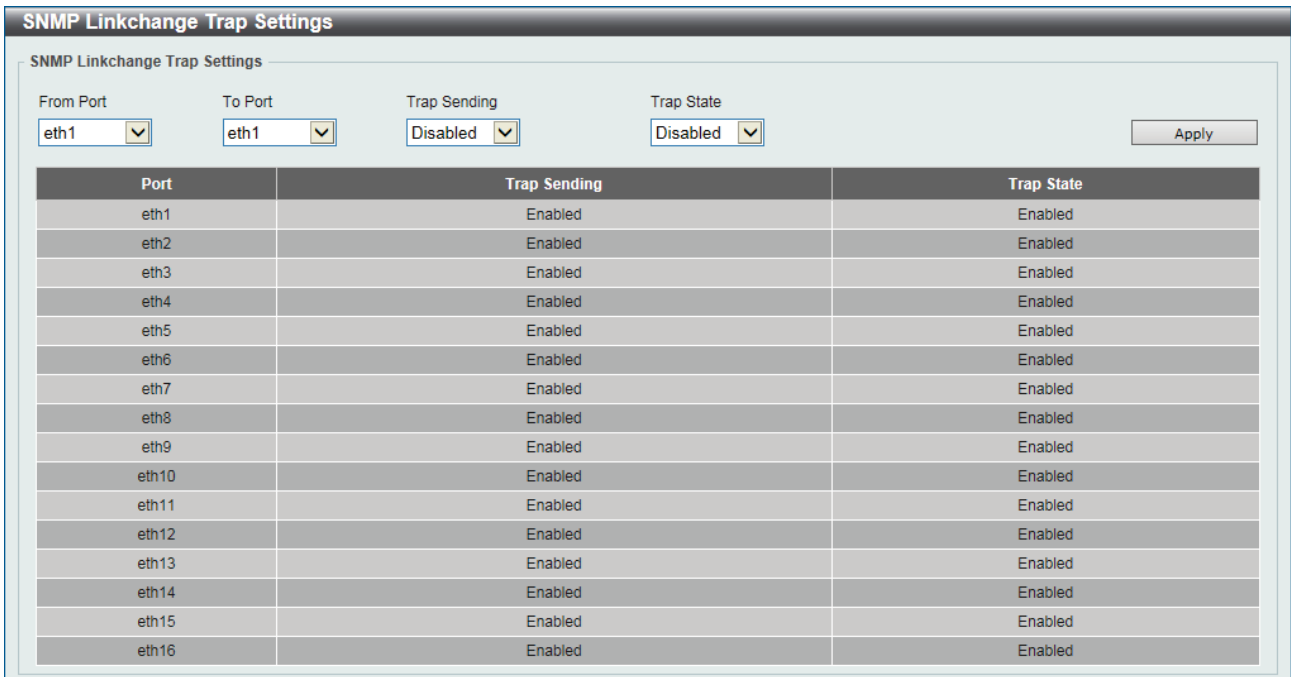


Figure 4.48 – Management > SNMP > SNMP Linkchange Trap Settings

The fields that can be configured are described below:

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

Trap Sending: Enable or disable the sending of the SNMP notification traps that is generated by the system.

Trap State: Enable or disable the SNMP link change trap.

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

Management > SNMP > SNMP View Table Settings

This window is used to assign views to community strings that define which MIB objects can be accessed by a remote SNMP manager. The SNMP Group created with this table maps SNMP users (identified in the SNMP User Table) to the views created in the previous window.

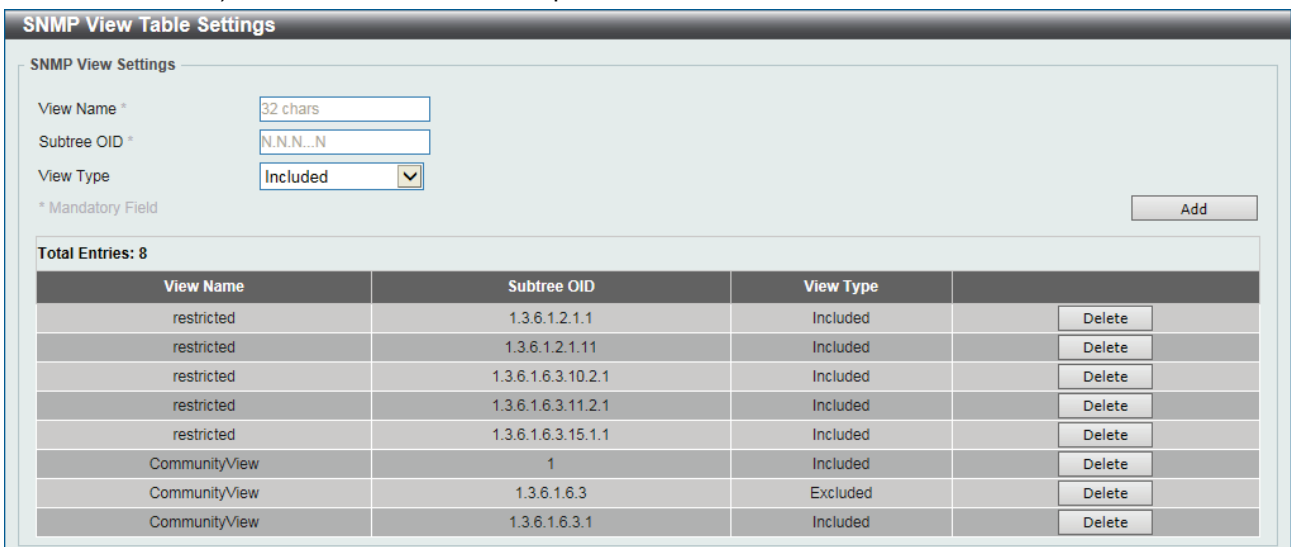


Figure 4.49 – Management > SNMP > SNMP View Table Settings

The fields that can be configured are described below:

View Name: Enter an alphanumeric string of up to 32 characters. This is used to identify the new SNMP view being created.

Subtree OID: Enter 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 view type here. Options to choose from are **Included** and **Excluded**.

Included - Select to include this object in the list of objects that an SNMP manager can access.

Excluded - Select to exclude this object from the list of objects that an SNMP manager can access.

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

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

Management > SNMP > SNMP Community Table Settings

This window is used to create an SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the Switch. One or more of the following characteristics can be associated with the community string:

- An Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the Switch's SNMP agent.
- Any MIB view that defines the subset of all MIB objects will be accessible to the SNMP community.
- Read/write or read-only level permission for the MIB objects accessible to the SNMP community.

| Community Name | View Name | Access Right | |
|----------------|---------------|--------------|--------|
| private | CommunityView | rw | Delete |
| public | CommunityView | ro | Delete |

Figure 4.50 – Management > SNMP > SNMP Community Table Settings

The fields that can be configured are described below:

Key Type: Select the key type for the SNMP community. Options to choose from are **Plain Text** and **Encrypted**.

Community Name: Enter 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 access right here. Options to choose from are **Read Only**, and **Read Write**.

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.

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

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

Management > SNMP > SNMP Group Table Settings

An SNMP Group created with this table maps SNMP users (identified in the SNMP User Table) to the views created in the previous window.

SNMP Group Table Settings

SNMP Group Settings

Group Name * Read View Name

User-based Security Model Write View Name

Security Level Notify View Name

* Mandatory Field Add

Total Entries: 5

| Group Name | Read View Name | Write View Name | Notify View Name | Security Model | Security Level | |
|------------|----------------|-----------------|------------------|----------------|----------------|--------|
| public | CommunityV... | | CommunityV... | v1 | | Delete |
| public | CommunityV... | | CommunityV... | v2c | | Delete |
| initial | restricted | | restricted | v3 | NoAuthNoPriv | Delete |
| private | CommunityV... | CommunityV... | CommunityV... | v1 | | Delete |
| private | CommunityV... | CommunityV... | CommunityV... | v2c | | Delete |

Figure 4.51 – Management > SNMP > SNMP Group Table Settings

The fields that can be configured are described below:

Group Name: Enter the group name of a maximum of 32 characters. The syntax is general string that does not allow space.

User-based Security Model: Select the security model here. Options to choose from are **SNMPv1**, **SNMPv2c**, and **SNMPv3**.

SNMPv1 - Select to allow the group user to use the SNMPv1 security model.

SNMPv2c - Select to allow the group user to use the SNMPv2c security model.

SNMPv3 - Select to allow the group user to use the SNMPv3 security model.

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

NoAuthNoPriv - Specify that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.

AuthNoPriv - Specify that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager.

AuthPriv - Specify that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.

Read View Name: Enter the read view name that the group user can access.

Write View Name: Enter the write view name that the group user can access.

Notify View Name: Enter a write view name that the group user can access. The notify view describes the object that can be reported its status via trap packets to the group user.

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

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

Management > SNMP > SNMP Engine ID Local Settings

The Engine ID is a unique identifier used for SNMP V3 implementations on the Switch.

SNMP Engine ID Local Settings

SNMP Engine ID Local Settings

Engine ID Default Apply

Engine ID length is 24, the accepted character is from 0 to F.

Figure 4.52 – Management > SNMP > SNMP Engine ID Local Settings

The fields that can be configured are described below:

Engine ID: Enter the engine ID string with the maximum of 24 characters.

Click **Default** to revert the engine ID to the default.

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

Management > SNMP > SNMP User Table Settings

SNMP User Table Settings

SNMP User Settings

User Name *

Group Name *

SNMP Version

SNMP V3 Encryption

Auth-Protocol by Password Password (8-16 chars)

Priv-Protocol by Password Password (8-16 chars)

Auth-Protocol by Key Key (32 chars)

Priv-Protocol by Key Key (32 chars)

* Mandatory Field

Total Entries: 1

| User Name | Group Name | Security Model | Authentication Protocol | Privacy Protocol | Engine ID | |
|-----------|------------|----------------|-------------------------|------------------|---------------|---------------------------------------|
| initial | initial | V3 | None | None | 800000ab03... | <input type="button" value="Delete"/> |

Figure 4.53 – Management > SNMP > SNMP User Table Settings

The fields that can be configured are described below:

User Name: Enter an alphanumeric string of up to 32 characters. This is used to identify the SNMP users.

Group Name: Enter the SNMP group name to which the user belongs. The syntax is general string that does not allow spaces.

SNMP Version: Select the SNMP version. Options to choose from 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: When selecting **v3** in the **SNMP Version** drop-down list, and selecting either **Password** or **Key** in the **SNMP V3 Encryption** drop-down list, this option is available. Select the authentication level. Options to choose from are **MD5**, and **SHA**.

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

SHA - Specify that the HMAC-SHA authentication protocol will be used. This field will require the user to enter a password or a key.

Priv-Protocol: When selecting **v3** in the **SNMP Version** drop-down list, and selecting either **Password** or **Key** in the **SNMP V3 Encryption** drop-down list, this option is available. Select the private protocol. Options to choose from are **None**, and **DES56**.

None - Specify that no authorization protocol is in use.

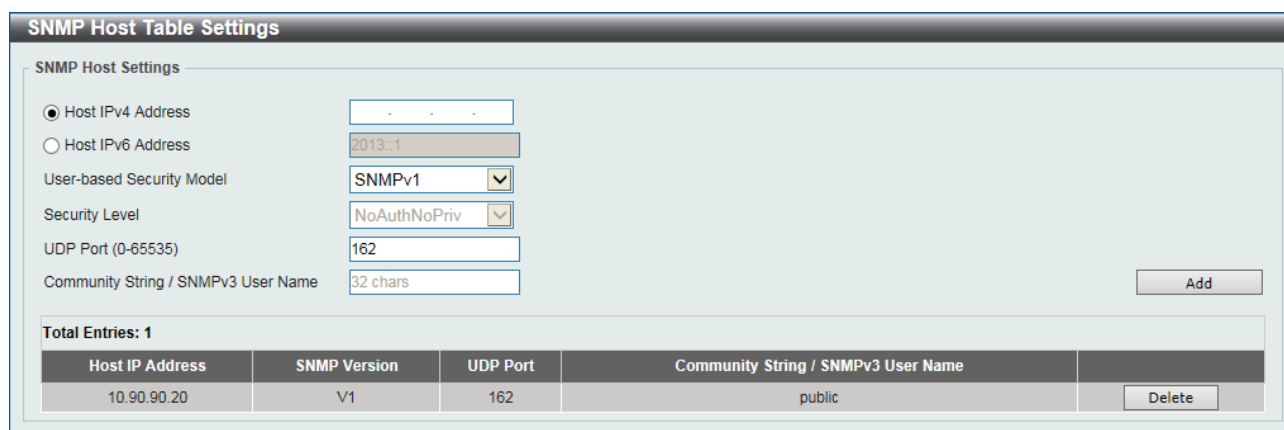
DES56 - Specify that DES 56-bit encryption is in use, based on the CBC-DES (DES-56) standard. This field will require the user to enter a password or a key.

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

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

Management > SNMP > SNMP Host Table Settings

This window is used to configure and display the recipient of the SNMP notification.



SNMP Host Table Settings

SNMP Host Settings

Host IPv4 Address

Host IPv6 Address

User-based Security Model:

Security Level:

UDP Port (0-65535):

Community String / SNMPv3 User Name:

Total Entries: 1

| Host IP Address | SNMP Version | UDP Port | Community String / SNMPv3 User Name | |
|-----------------|--------------|----------|-------------------------------------|---------------------------------------|
| 10.90.90.20 | V1 | 162 | public | <input type="button" value="Delete"/> |

Figure 4.54 – Management > SNMP > SNMP Host Table Settings

The fields that can be configured are described below:

Host IPv4 Address: Enter the IPv4 address of the SNMP notification host.

Host IPv6 Address: Enter the IPv6 address of the SNMP notification host.

User-based Security Model: Select the security model here. Options to choose from are **SNMPv1**, **SNMPv2c**, and **SNMPv3**.

SNMPv1 - Select to allow the group user to use the SNMPv1 security model.

SNMPv2c - Select to allow the group user to use the SNMPv2c security model.

SNMPv3 - Select to allow the group user to use the SNMPv3 security model.

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

NoAuthNoPriv - Specify that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.

AuthNoPriv - Specify that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager.

AuthPriv - Specify that authorization will be required, and that packets sent between the Switch and a remote SNMP manager will be encrypted.

UDP Port: 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.

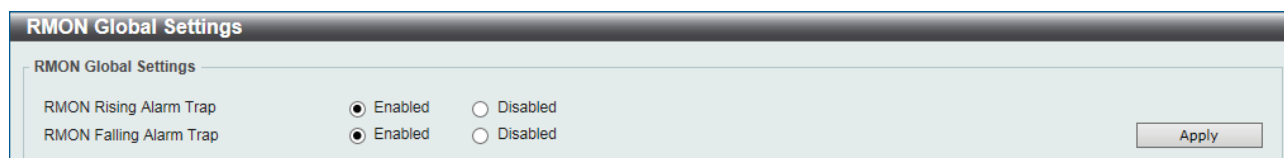
Community String / SNMPv3 User Name: Enter the community string to be sent with the notification packet.

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

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

Management > RMON > RMON Global Settings

This window is used to enable or disable remote monitoring (RMON) for the rising and falling alarm trap feature for the SNMP function on the Switch.



RMON Global Settings

RMON Global Settings

RMON Rising Alarm Trap: Enabled Disabled

RMON Falling Alarm Trap: Enabled Disabled

Figure 4.55 – Management > RMON > RMON Global Settings

The fields that can be configured are described below:

RMON Rising Alarm Trap: Enable or disable the RMON Rising Alarm Trap Feature.

RMON Falling Alarm Trap: Enable or disable the RMON Falling Alarm Trap Feature.

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

Management > RMON > RMON Statistics Settings

This window is used to configure and display the RMON statistics on the specified port.

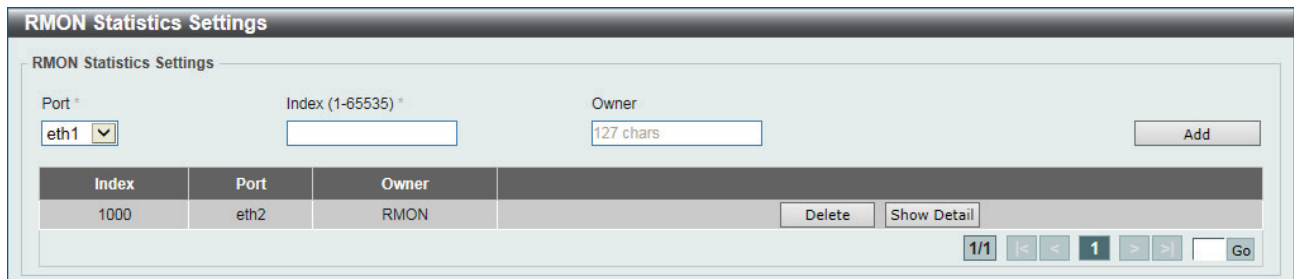


Figure 4.56 – Management > RMON > RMON Statistics Settings

The fields that can be configured are described below:

Port: Select to choose the port.

Index: Enter the RMON table index. The value is from 1 to 65535

Owner: Enter the owner string. The string can be up to 127 characters.

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

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

Click **Show Detail** to see the detail information of the specific port.

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

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

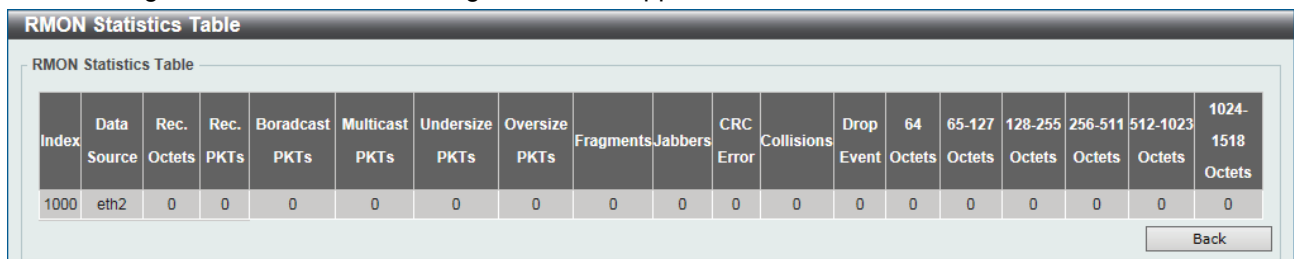


Figure 4.57 – Management > RMON > RMON Statistics Table

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

Management > RMON > RMON History Settings

This window is used to configure and display RMON MIB history statistics gathering on the specified port.

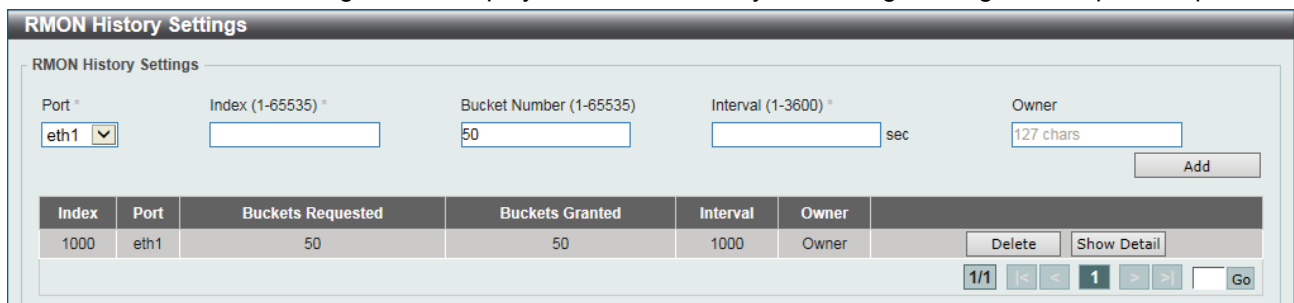


Figure 4.58 – Management > RMON > RMON History Settings

The fields that can be configured are described below:

Port: Select to choose the port.

Index: Enter the history group table index. The value is from 1 to 65535.

Bucket Number: Enter Specifies the number of buckets specified for the RMON collection history group of statistics. The range is from 1 to 65535. The default value is 50.

Interval: Enter the time in seconds in each polling cycle. The range is from 1 to 3600.

Owner: Enter the owner string. The string can be up to 127 characters.

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

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

Click **Show Detail** to see the detail information of the specific port.

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

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

| Index | Sample | Rec. Octets | Rec. PKTs | Broadcast PKTs | Multicast PKTs | Utilization | Undersize PKTs | Oversize PKTs | Fragments | Jabbers | CRC Error | Collisions | Drop Event |
|-------|--------|-------------|-----------|----------------|----------------|-------------|----------------|---------------|-----------|---------|-----------|------------|------------|
|-------|--------|-------------|-----------|----------------|----------------|-------------|----------------|---------------|-----------|---------|-----------|------------|------------|

Figure 4.59 – Management > RMON > RMON History Table

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

Management > RMON > RMON Alarm Settings

This window is used to configure and display alarm entries to monitor an interface.

| Index | Interval (sec) | Variable | Type | Last Value | Rising Threshold | Falling Threshold | Rising Event No. | Falling Event No. | Startup Alarm | Owner |
|-------|----------------|------------------------|----------|------------|------------------|-------------------|------------------|-------------------|------------------|-------|
| 1 | 30 | 1.3.6.1.2.1.2.2.1.12.6 | Absolute | 0 | 20 | 10 | 1 | 1 | Rising or Faling | Owner |

Figure 4.60 – Management > RMON > RMON Alarm Settings

The fields that can be configured are described below:

Index: Enter the alarm index. The range is from 1 to 65535.

Interval: Enter the interval in seconds for the sampling of the variable and checking against the threshold. The valid range is from 1 to 2147483647 seconds.

Variable: Enter the object identifier of the variable to be sampled.

Type: Select the monitoring type. Options to choose from are Absolute and Delta.

Rising Threshold: Enter the rising threshold value between 0 and 2147483647.

Falling Threshold: Enter the falling threshold value between 0 and 2147483647.

Rising Event Number: Enter the index of the event entry that is used to notify the rising threshold crossing event. The valid range is from 1 to 65535. If not specified, no action is taken while crossing the rising threshold.

Falling Event Number: Enter the index of the event entry that is used to notify the falling threshold crossing event. The valid range is from 1 to 65535. If not specified, no action is taken while crossing the falling threshold.

Owner: Enter the owner string up to 127 characters.

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

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

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

Management > RMON > RMON Event Settings

This window is used to configure and display event entries.

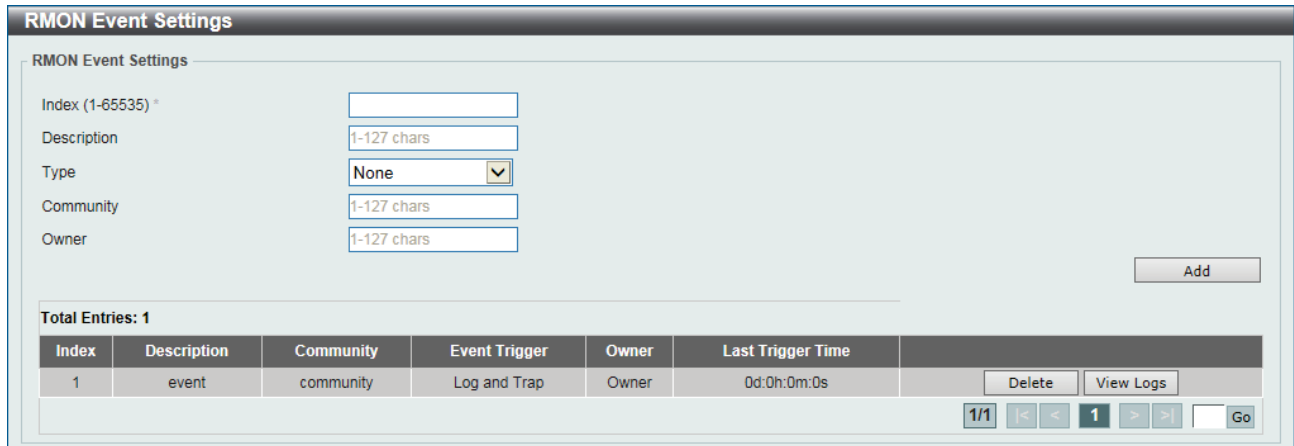


Figure 4.61 – Management > RMON > RMON Event Settings

The fields that can be configured are described below:

Index: Enter the index of the alarm entry between 1 and 65535.

Description: Enter a description for the RMON event entry. The string is up to 127 characters long.

Type: Select the RMON event entry type. Options to choose from are **None**, **Log**, **Trap**, and **Log and Trap**.

Community: Enter the community string. The string can be up to 127 characters.

Owner: Enter the owner string. The string can be up to 127 characters.

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

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

Click **View Logs** to see the detail information of the specific port.

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

After clicking **View Logs**, the following window will appear.

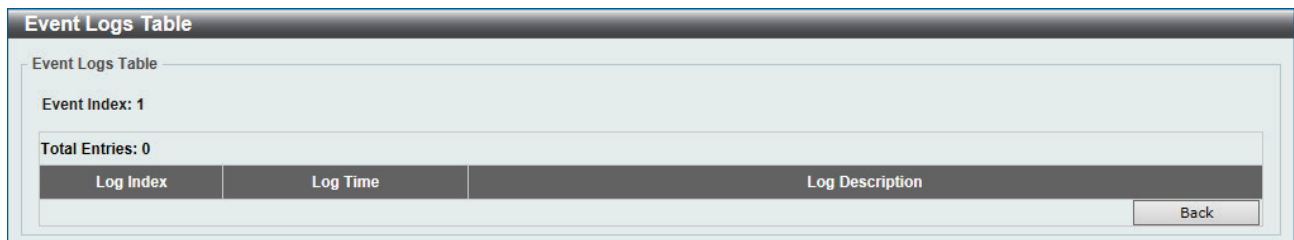


Figure 4.62 – Management > RMON > Event Logs Table

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

Management > Web

This window is used to configure the Web settings on the Switch.

The screenshot shows a web interface titled 'Web' with a sub-section 'Web Settings'. There is a text input field labeled 'Port (1-65535)' containing the number '80'. To the right of the input field is an 'Apply' button.

Figure 4.63 – Management > Web

The fields that can be configured are described below:

Port: Enter the TCP port number used for Web-based management of the Switch. The “well-known” TCP port for the Web-based protocol is 80.

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

Management > Session Timeout

This window is used to configure the session timeout.

The screenshot shows a web interface titled 'Session Timeout'. There is a text input field labeled 'Web Session Timeout (60-36000)' containing the number '180', followed by the unit 'sec'. To the right of the input field is a checked checkbox labeled 'Default'. An 'Apply' button is located at the bottom right.

Figure 4.64 – Management > Session Timeout

The fields that can be configured are described below:

Web Session Timeout: Enter the time in seconds of the web session timeout. Tick **Default** to return to the default setting. The value is from 60 to 36000 seconds. The default value is 180 seconds.

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

Management > File System

The File System is used to provide the user with flexible file operation on the Flash. All the firmware, configuration information and system log information are stored in the Flash as files.

The screenshot shows a web interface titled 'File System'. There is a text input field labeled 'Path' containing 'C:'. To the right of the input field is a 'Go' button. Below the input field is a 'Copy' button. Below the 'Copy' button is a table with the following data:

| Drive | Media Type | Size (MB) | File System Type | Label |
|-------|------------|-----------|------------------|-------|
| C: | Flash | 95 | FFS | |

Figure 4.65 – Management > File System

The fields that can be configured are described below:

Path: Enter the path string

Click **Go** to navigate to the path entered.

Click the [C:](#) hyperlink to navigate the C: drive.

After clicking the [C:](#) hyperlink, the following window will appear:

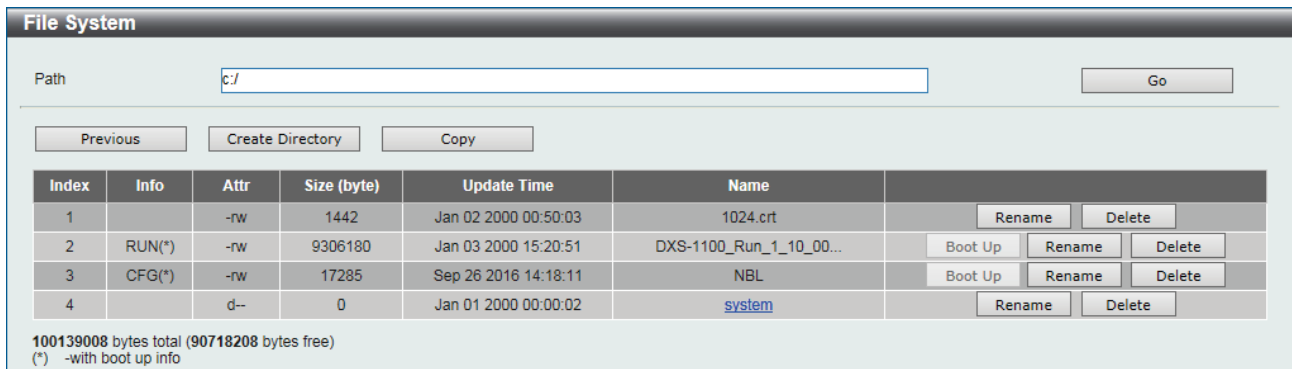


Figure 4.66 – Management > File System (Search for Drive)

Click **Previous** to return to the previous window.

Click **Create Directory** to create a new directory within the file system of the Switch.

Click **Copy** to copy a specific file to the Switch.

Click **Boot Up** to set a specific file as either the boot-up image or boot-up configuration.

Click **Rename** to rename a specific file's name.

Click **Delete** to remove a specific file from the file system.

Click **Copy** to see the following window.

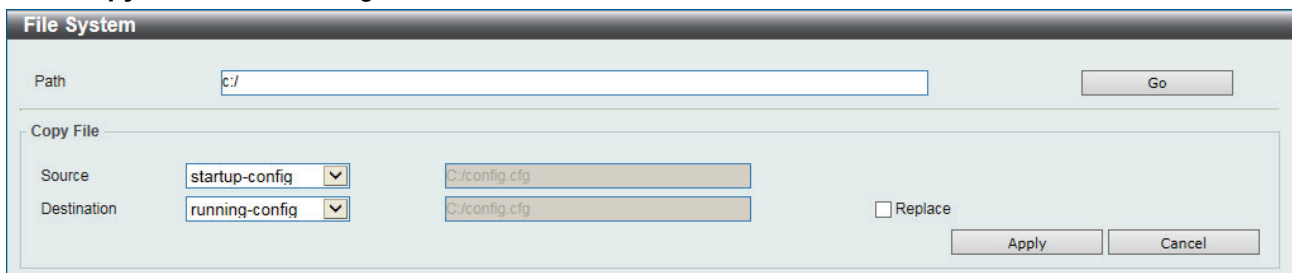


Figure 4.67 – Management > File System (Copy)

When copying a file to the file system of this switch, the user must enter the **Source** and **Destination** path. Tick **Replace** to replace the current running configuration with the indicated configuration file.

Click **Apply** to initiate the copy.

Click **Cancel** to discard the process.



NOTE: / \ : * ? " < > | and space are not allowed in the file name.



NOTE: When renaming the file or folder name, or creating a directory, the forward slash character (/) is used to indicate the file or folder path except if the forward slash character is used at the end of the file name in which it is then considered to be part of the file name thus, in this usage, the forward slash character would not be allowed.

Management > D-Link Discovery Protocol

This window is used to configure and display D-Link Discovery Protocol (DDP).

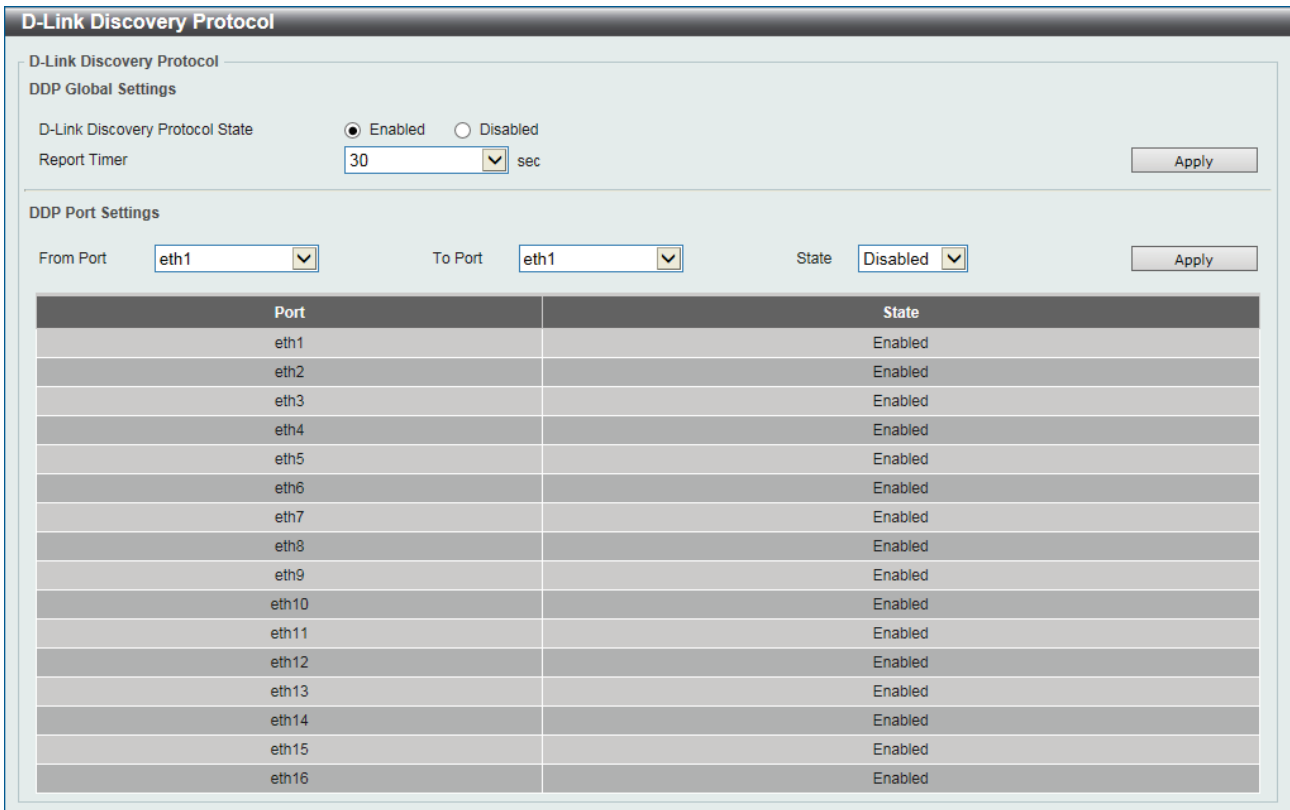


Figure 4.68 – Management > D-Link Discovery Protocol

The fields that can be configured are described below:

D-Link Discovery Protocol State: Enable or disable DDP global state.

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

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

State: Select this option to enable or disable DDP port state.

Click **Apply** to accept the changes made for each individual section.

L2 Features > FDB > Static FDB > Unicast Static FDB

This window is used to view and configure the static unicast forwarding settings on the Switch.

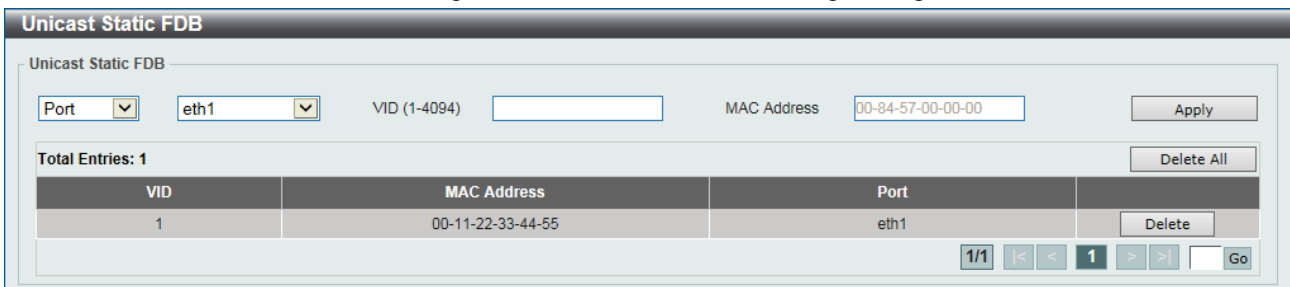


Figure 4.69 – L2 Features > FDB > Static FDB > Unicast Static FDB

The fields that can be configured are described below:

Port / Drop: 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 port number.

Port Number: Select the port number used here, when **Port** is selected in the previous drop-down list.

VID: 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 **Apply** to accept the changes made.

Click **Delete All** to delete all the entries found in the display table.

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

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

L2 Features > FDB > Static FDB > Multicast Static FDB

This window is used to view and configure the multicast static FDB settings.

Multicast Static FDB

Multicast Static FDB

From Port: eth1 | To Port: eth1 | VID (1-4094): | MAC Address: 01-00-00-00-00-02

Total Entries: 1 | Delete All

| VID | MAC Address | Egress Ports |
|-----|-------------------|--------------|
| 1 | 01-00-00-00-00-22 | eth1 |

1/1 | < < 1 > > | Go

Figure 4.70 – L2 Features > FDB > Static FDB > Multicast Static FDB

The fields that can be configured are described below:

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

VID: 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-XX.

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

Click **Delete All** to delete all the entries found in the display table.

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

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

L2 Features > FDB > MAC Address Table Settings

This window is used to view and configure the MAC address table's global settings.

MAC Address Table Settings

Global Settings | MAC Address Learning

Aging Time (0, 10-1000000): 300 sec | Apply

Figure 4.71 – L2 Features > FDB > MAC Address Table Settings (Global Settings)

The fields that can be configured are described below:

Aging Time: Enter the MAC address table's aging time value here. This value must be between 10 and 1000000 seconds. Entering 0 will disable MAC address aging. By default, this value is 300 seconds.

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

After clicking the **MAC Address Learning** tab, at the top of the page, the following page will be available.

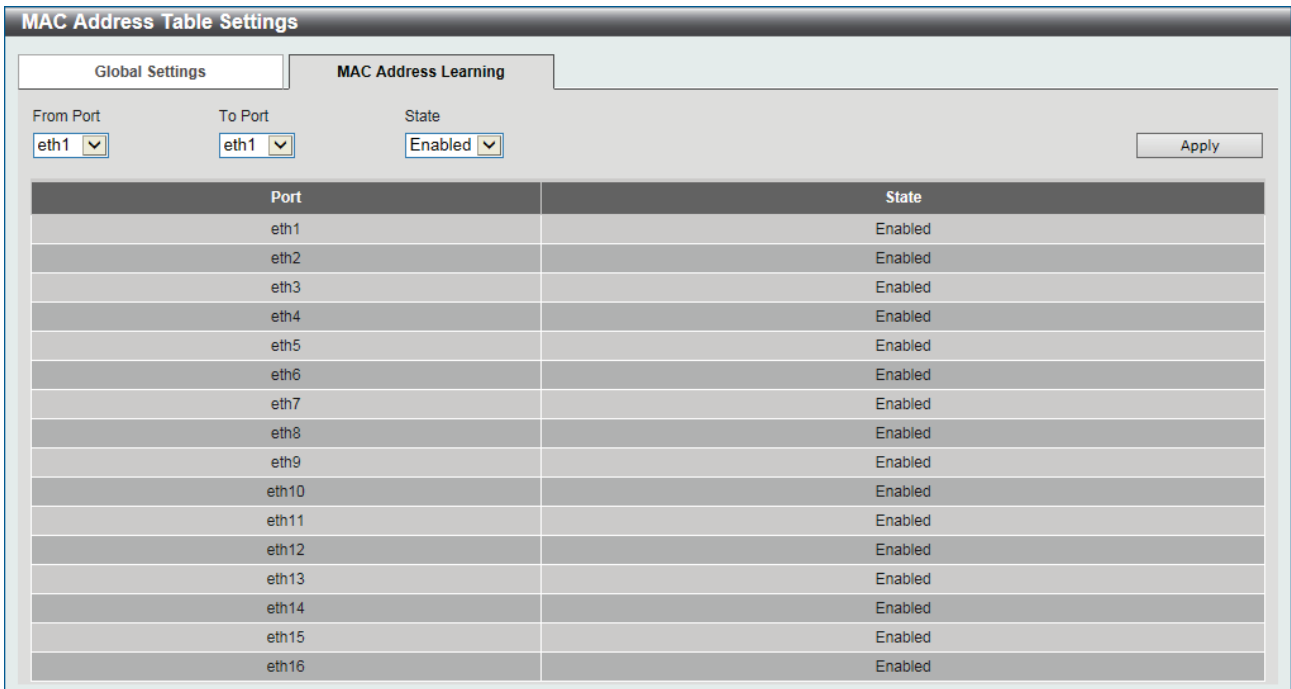


Figure 4.72 – L2 Features > FDB > MAC Address Table Settings (MAC Address Learning)

The fields that can be configured are described below:

From Port / To Port: Select the range of ports that will be used for this configuration here.

State: Enable or disable the MAC address learning function on the ports specified here.

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

L2 Features > FDB > MAC Address Table

This window is used to view the entries listed in the MAC address table.

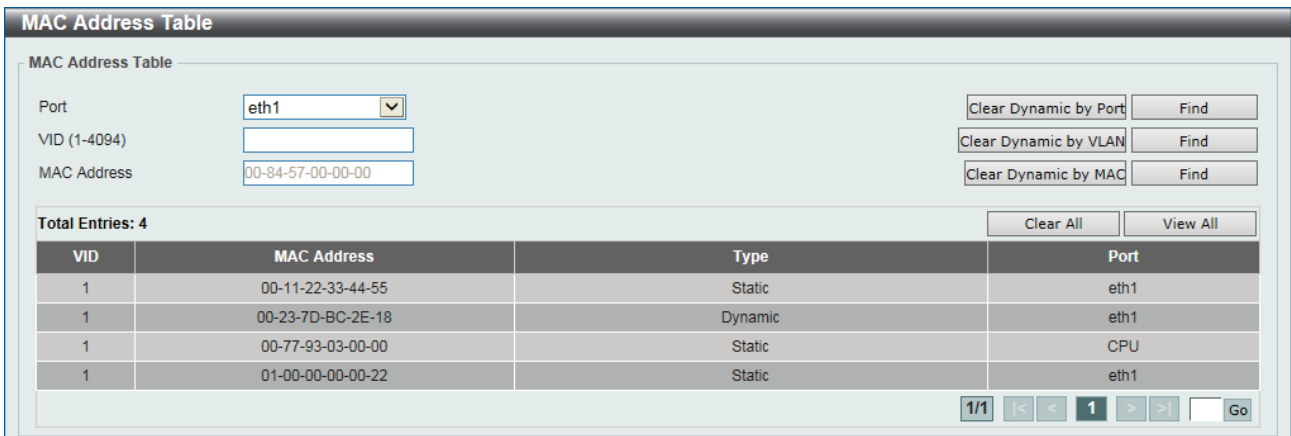


Figure 4.73 – L2 Features > FDB > MAC Address Table

The fields that can be configured are described below:

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

VID: Enter the VLAN ID that will be used for this configuration here.

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

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

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

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

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

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

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

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

L2 Features > FDB > MAC Notification

This window is used to view and configure MAC notification.

| Port | Added Trap | Removed Trap |
|-------|------------|--------------|
| eth1 | Disabled | Disabled |
| eth2 | Disabled | Disabled |
| eth3 | Disabled | Disabled |
| eth4 | Disabled | Disabled |
| eth5 | Disabled | Disabled |
| eth6 | Disabled | Disabled |
| eth7 | Disabled | Disabled |
| eth8 | Disabled | Disabled |
| eth9 | Disabled | Disabled |
| eth10 | Disabled | Disabled |
| eth11 | Disabled | Disabled |
| eth12 | Disabled | Disabled |
| eth13 | Disabled | Disabled |
| eth14 | Disabled | Disabled |
| eth15 | Disabled | Disabled |
| eth16 | Disabled | Disabled |

Figure 4.74 – L2 Features > FDB > MAC Notification (MAC Notification Settings)

The fields that can be configured are described below:

MAC Address Notification: Enable or disable MAC notification globally on the Switch.

Interval: Enter the time value between notifications. This value must be between 1 and 2147483647 seconds. By default, this value is 1 second.

History Size: Enter the maximum number of entries listed in the history log used for notification. This value must be between 0 and 500. By default, this value is 1.

MAC Notification Trap State: Select this option to enable or disable the MAC notification trap state.

From Port / To Port: Select the range of ports that will be used for this configuration here.

Added Trap: Enable or disable the added trap for the port(s) selected.

Removed Trap: Enable or disable the removed trap for the port(s) selected.

Click **Apply** to accept the changes made for each individual section.

L2 Features > VLAN > 802.1Q VLAN

A VLAN is a group of ports that can be anywhere in the network, but communicate as though they were in the same area.

VLANs can be easily organized to reflect department groups (such as R&D, Marketing), usage groups (such as e-mail), or multicast groups (multimedia applications such as video conferencing), and therefore help to simplify network management by allowing users to move devices to a new VLAN without having to change any physical connections.

The IEEE 802.1Q VLAN Settings window provides powerful VID management functions. The original settings have the VID as 1, VLAN Name as default, and all ports as Untagged.

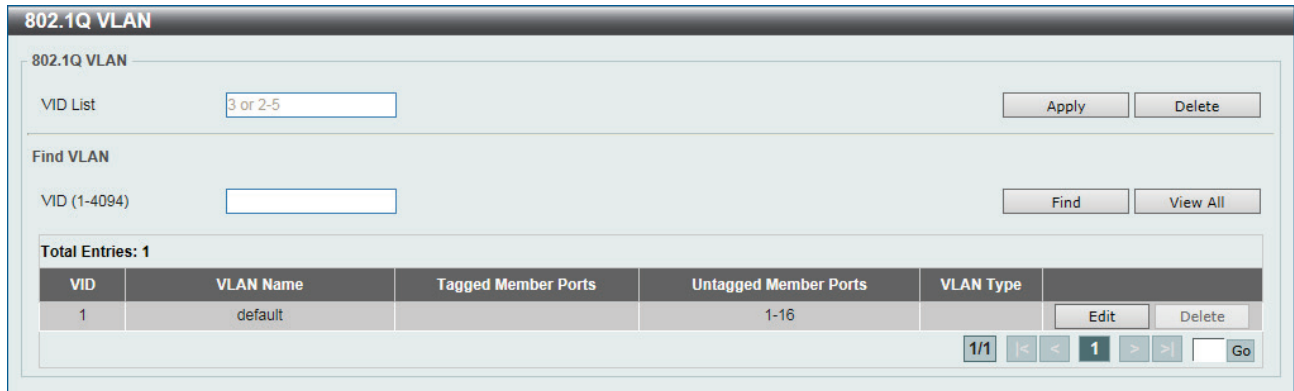


Figure 4.75 – L2 Features > VLAN > 802.1Q VLAN

The fields that can be configured are described below:

VID List: Enter the VLAN ID list that will be created here.

VID: Enter the VLAN ID that will be displayed here.

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

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

Click **View All** to locate all the entries.

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

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

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

L2 Features > VLAN > Asymmetric VLAN

This window is used to configure the asymmetric VLAN function.

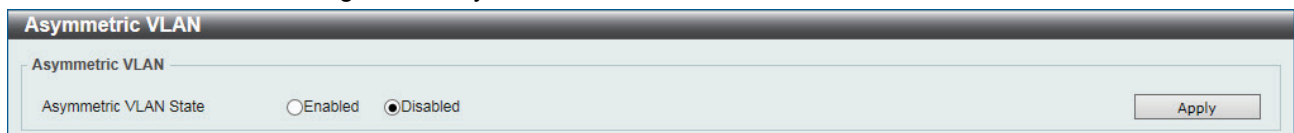


Figure 4.76 – L2 Features > VLAN > Asymmetric VLAN

The fields that can be configured are described below:

Asymmetric VLAN State: Enable or disable the asymmetric VLAN function

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

L2 Features > VLAN > VLAN Interface

This window is used to view and configure VLAN interface settings.

| VLAN Interface | | | | | | |
|----------------|-----------|------------------|-----------------------|-------------|------|--|
| VLAN Interface | | | | | | |
| Port | VLAN Mode | Ingress Checking | Acceptable Frame Type | | | |
| eth1 | Hybrid | Enabled | Admit-All | VLAN Detail | Edit | |
| eth2 | Hybrid | Enabled | Admit-All | VLAN Detail | Edit | |
| eth3 | Hybrid | Enabled | Admit-All | VLAN Detail | Edit | |
| eth4 | Hybrid | Enabled | Admit-All | VLAN Detail | Edit | |
| eth5 | Hybrid | Enabled | Admit-All | VLAN Detail | Edit | |
| eth6 | Hybrid | Enabled | Admit-All | VLAN Detail | Edit | |
| eth7 | Hybrid | Enabled | Admit-All | VLAN Detail | Edit | |
| eth8 | Hybrid | Enabled | Admit-All | VLAN Detail | Edit | |
| eth9 | Hybrid | Enabled | Admit-All | VLAN Detail | Edit | |
| eth10 | Hybrid | Enabled | Admit-All | VLAN Detail | Edit | |
| eth11 | Hybrid | Enabled | Admit-All | VLAN Detail | Edit | |
| eth12 | Hybrid | Enabled | Admit-All | VLAN Detail | Edit | |
| eth13 | Hybrid | Enabled | Admit-All | VLAN Detail | Edit | |
| eth14 | Hybrid | Enabled | Admit-All | VLAN Detail | Edit | |
| eth15 | Hybrid | Enabled | Admit-All | VLAN Detail | Edit | |
| eth16 | Hybrid | Enabled | Admit-All | VLAN Detail | Edit | |

Figure 4.77 – L2 Features > VLAN > VLAN Interface

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

After clicking **VLAN Detail**, the following page will appear.

| VLAN Interface Information | |
|----------------------------|-----------|
| VLAN Interface Information | |
| Port | eth1 |
| VLAN Mode | Hybrid |
| Native VLAN | 1 |
| Hybrid Untagged VLAN | 1 |
| Hybrid Tagged VLAN | |
| Ingress Checking | Enabled |
| Acceptable Frame Type | Admit-All |

Back

Figure 4.78 – L2 Features > VLAN > VLAN Interface Information (View Detail)

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

After click the **Edit** button, the following page will appear. This is a dynamic page that will change when a different **VLAN Mode** was selected.

When **Access** was selected as the **VLAN Mode**, the following page will appear.

| Configure VLAN Interface | |
|--------------------------|---|
| Configure VLAN Interface | |
| Port | eth1 |
| VLAN Mode | Access |
| Acceptable Frame | Admit All |
| Ingress Checking | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled |
| VID (1-4094) | <input type="text"/> |

Back Apply

Figure 4.79 – L2 Features > VLAN > VLAN Interface Information (Access)

The fields that can be configured are described below:

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

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

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

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

Click **Apply** to accept the changes made for each individual section.

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

When **Hybrid** was selected as the **VLAN Mode**, the following page will appear.

The screenshot shows a web interface titled "Configure VLAN Interface". The configuration is for port "eth1". The "VLAN Mode" is set to "Hybrid". The "Acceptable Frame" is set to "Admit All". "Ingress Checking" is set to "Enabled". The "Native VLAN" checkbox is unchecked. The "VID (1-4094)" field is empty. The "Action" is set to "Add". The "Add Mode" is set to "Untagged". The "Allowed VLAN Range" field is empty. At the bottom right, there are "Back" and "Apply" buttons.

Figure 4.80 – L2 Features > VLAN > VLAN Interface Information (Hybrid)

The fields that can be configured are described below:

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

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

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

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

Action: Select the action that will be taken here. Options to choose from are **Add**, **Remove**, **Tagged**, and **Untagged**.

Add Mode: Select whether to add an **Untagged** or **Tagged** parameters.

Allowed VLAN Range: Enter the allowed VLAN range information here.

Click **Apply** to accept the changes made for each individual section.

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

When **Trunk** was selected as the **VLAN Mode**, the following page will appear.

The screenshot shows a web interface for configuring a VLAN interface. The title is "Configure VLAN Interface". The form has the following fields and values:

- Port: eth1
- VLAN Mode: Trunk
- Acceptable Frame: Admit All
- Ingress Checking: Enabled Disabled
- Native VLAN: Native VLAN Untagged Tagged
- VID (1-4094): (empty text box)
- Action: All
- Allowed VLAN Range: (empty text box)

At the bottom right, there are two buttons: "Back" and "Apply".

Figure 4.81 – L2 Features > VLAN > VLAN Interface Information (Trunk)

The fields that can be configured are described below:

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

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

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

Native VLAN: Tick this option to enable the native VLAN function. Also select if this VLAN supports **Untagged** or **Tagged** frames.

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

Action: Select the action that will be taken here. Options to choose from are **All**, **Add**, **Remove**, **Except**, and **Replace**.

Allowed VLAN Range: Enter the allowed VLAN range information here.

Click **Apply** to accept the changes made for each individual section.

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

L2 Features > VLAN > Auto Surveillance VLAN > Auto Surveillance Properties

This window is used to configure the auto surveillance VLAN global settings and display the ports surveillance VLAN information.

Auto Surveillance Properties

Global Settings

Surveillance VLAN Enabled Disabled

Surveillance VLAN ID (2-4094)

Surveillance VLAN CoS ▼

Aging Time (1-65535) min

Port Settings

From Port ▼ To Port ▼ State ▼

| Port | State |
|-------|----------|
| eth1 | Disabled |
| eth2 | Disabled |
| eth3 | Disabled |
| eth4 | Disabled |
| eth5 | Disabled |
| eth6 | Disabled |
| eth7 | Disabled |
| eth8 | Disabled |
| eth9 | Disabled |
| eth10 | Disabled |
| eth11 | Disabled |
| eth12 | Disabled |
| eth13 | Disabled |
| eth14 | Disabled |
| eth15 | Disabled |
| eth16 | Disabled |

Figure 4.82 – L2 Features > VLAN > Auto Surveillance VLAN> Auto Surveillance Properties

The fields that can be configured are described below:

Surveillance VLAN: Enable or disable the surveillance VLAN state

Surveillance VLAN ID: Enter the surveillance VLAN ID. The range is from 2 to 4094.

Surveillance VLAN CoS: Select the priority of the surveillance VLAN from 0 to 7.

Aging Time: Enter the aging time of surveillance VLAN. The range is from 1 to 65535 minutes. The default value is 720 minutes. The aging time is used to remove a port from surveillance VLAN if the port is an automatic surveillance VLAN member. When the last surveillance device stops sending traffic and the MAC address of this surveillance device is aged out, the surveillance VLAN aging timer will be started. The port will be removed from the surveillance VLAN after expiration of surveillance VLAN aging timer. If the surveillance traffic resumes during the aging time, the aging timer will be reset and stop.

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

State: Enable or disable the state of the port.

Click **Apply** to accept the changes made for each individual section.

L2 Features > VLAN > Auto Surveillance VLAN > MAC Settings and Surveillance Device

This window is used to configure the user-defined surveillance device OUI and display the surveillance VLAN information.

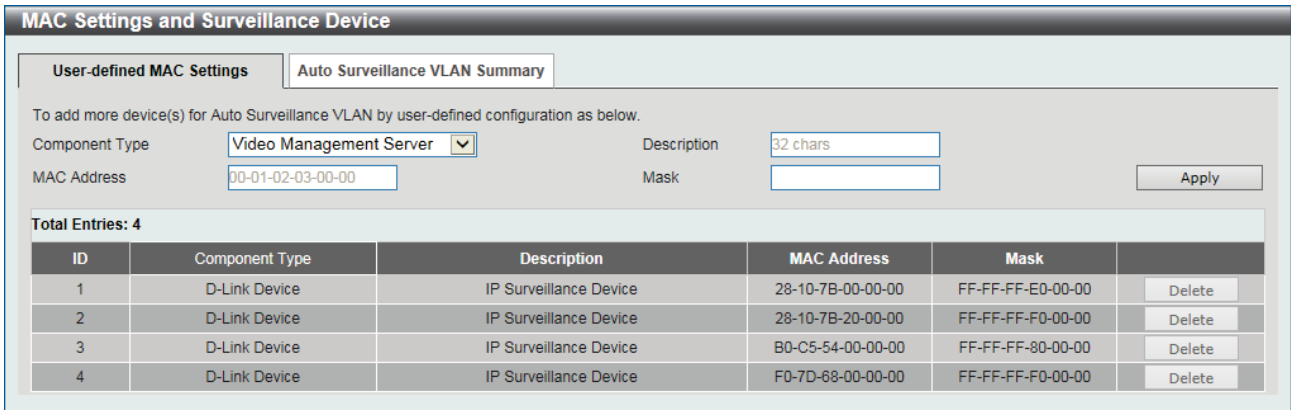


Figure 4.83 – L2 Features > VLAN > Auto Surveillance VLAN> MAC Settings and Surveillance Device (User-defined MAC Settings)

The fields that can be configured are described below:

Component Type: Select the surveillance component type. Options to choose from are **Video Management Server**, **VMS Client/Remote Viewer**, **Video Encoder**, **Network Storage**, and **Other IP Surveillance Device**.

Description: Enter the description for the user-defined OUI with a maximum of 32 characters.

MAC Address: Enter the OUI MAC address.

Mask: Enter the OUI MAC address matching bitmask.

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

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

After clicking the **Auto Surveillance VLAN Summary** tab, the following page will appear.

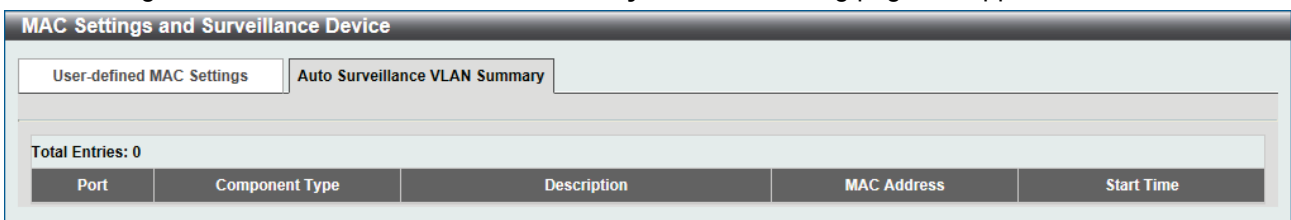


Figure 4.84 – L2 Features > VLAN > Auto Surveillance VLAN> MAC Settings and Surveillance Device (Auto Surveillance VLAN Summary)

L2 Features > VLAN > Voice VLAN > Voice VLAN Global

Voice VLAN is a VLAN used to carry voice traffic from IP phone. Because the sound quality of an IP phone call will be deteriorated if the data is unevenly sent, the quality of service (QoS) for voice traffic shall be configured to ensure the transmission priority of voice packet is higher than normal traffic.

The switches determine whether a received packet is a voice packet by checking its source MAC address. If the source MAC addresses of packets comply with the organizationally unique identifier (OUI) addresses configured by the system, the packets are determined as voice packets and transmitted in voice VLAN.

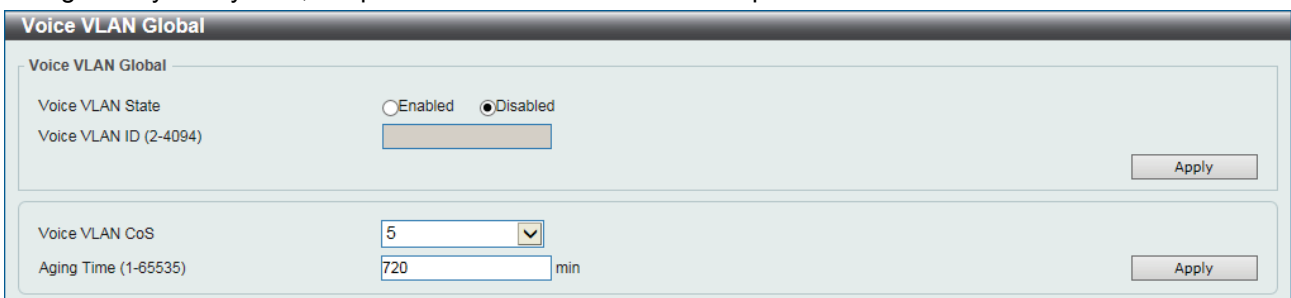


Figure 4.85 – L2 Features > VLAN > Voice VLAN > Voice VLAN Global

The fields that can be configured are described below:

Voice VLAN State: Enable or disable voice VLAN.

Voice VLAN ID: Enter the voice VLAN ID. The value is range from 2 to 4094.

Voice VLAN CoS: Select the priority of voice VLAN from 0 to 7.

Aging Time: Enter the aging time of voice VLAN. The range is from 1 to 65535 minutes. The default value is 720 minutes. The aging time is used to remove a port from voice VLAN if the port is an automatic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after expiration of voice VLAN aging timer. If the voice traffic resumes during the aging time, the aging timer will be reset and stop.

Click **Apply** to accept the changes made for each individual section.

L2 Features > VLAN > Voice VLAN > Voice VLAN Port

This window is used to show the ports voice VLAN information.

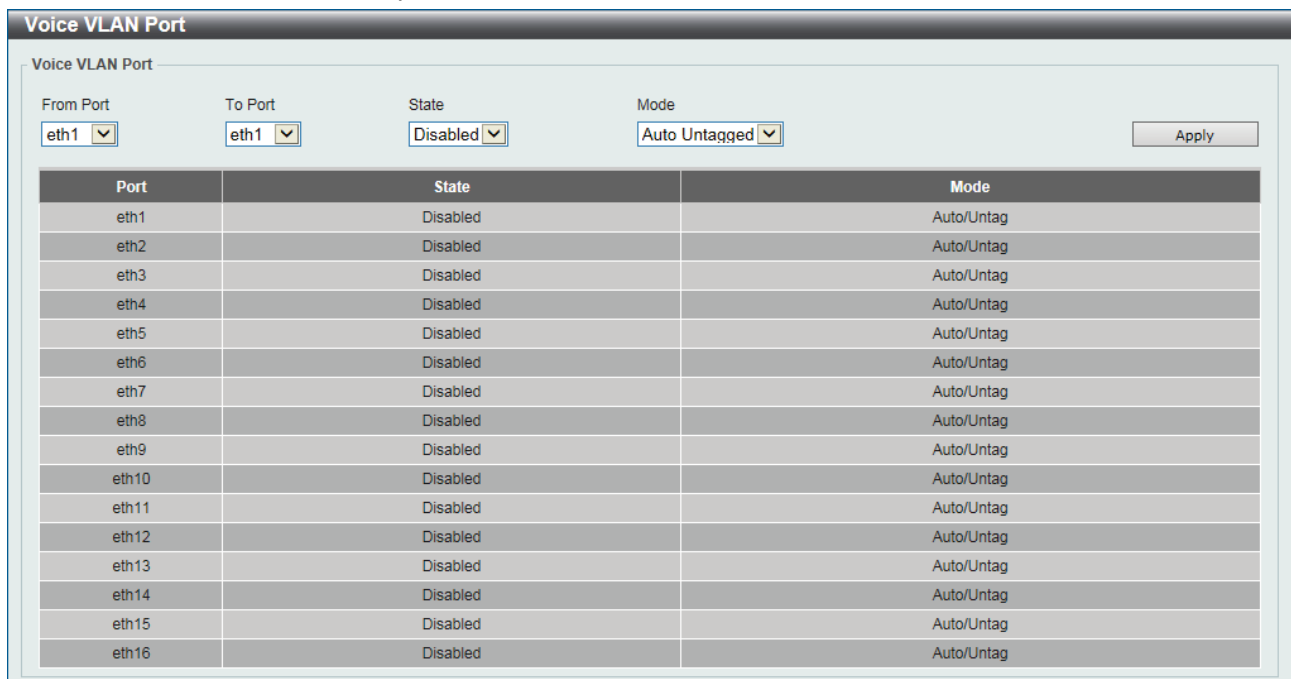


Figure 4.86 – L2 Features > VLAN > Voice VLAN > Voice VLAN Port

The fields that can be configured are described below:

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

State: Enable or disable the state of the port.

Mode: Select the mode of the port. Options to choose from are Auto Untagged, Auto Tagged, and Manual.

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

L2 Features > VLAN > Voice VLAN > Voice VLAN OUI

This window is used to configure the user-defined voice traffic's OUI. The OUI is used to identify the voice traffic. There are a number of pre-defined OUIs. The user can further define the user-defined OUIs if needed. The user-defined OUI cannot be the same as the pre-defined OUI.

Voice VLAN OUI

Voice VLAN OUI

OUI Address: Mask: Description:

Total Entries: 8

| OUI Address | Mask | Description | |
|-------------------|-------------------|-------------|---------------------------------------|
| 00-01-E3-00-00-00 | FF-FF-FF-00-00-00 | Siemens | <input type="button" value="Delete"/> |
| 00-03-6B-00-00-00 | FF-FF-FF-00-00-00 | Cisco | <input type="button" value="Delete"/> |
| 00-09-6E-00-00-00 | FF-FF-FF-00-00-00 | Avaya | <input type="button" value="Delete"/> |
| 00-0F-E2-00-00-00 | FF-FF-FF-00-00-00 | Huawei&3COM | <input type="button" value="Delete"/> |
| 00-60-B9-00-00-00 | FF-FF-FF-00-00-00 | NEC&Philips | <input type="button" value="Delete"/> |
| 00-D0-1E-00-00-00 | FF-FF-FF-00-00-00 | Pingtel | <input type="button" value="Delete"/> |
| 00-E0-75-00-00-00 | FF-FF-FF-00-00-00 | Veritel | <input type="button" value="Delete"/> |
| 00-E0-BB-00-00-00 | FF-FF-FF-00-00-00 | 3COM | <input type="button" value="Delete"/> |

Figure 4.87 – L2 Features > VLAN > Voice VLAN > Voice VLAN OUI

The fields that can be configured are described below:

OUI Address: Enter the OUI MAC address.

Mask: Enter the OUI MAC address matching bitmask.

Description: Enter the description for the user-defined OUI with a maximum of 32 characters.

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

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

L2 Features > VLAN > Voice VLAN > Voice VLAN Device

This window is used to show voice devices that are connected to the ports. The start time is the time when the device is detected on this port.

Voice VLAN Device

Voice VLAN Device Table

Total Entries: 0

| Port | Voice Device Address | Start Time | Status |
|------|----------------------|------------|--------|
|------|----------------------|------------|--------|

Figure 4.88 – L2 Features > VLAN > Voice VLAN > Voice VLAN Device

L2 Features > VLAN > Voice VLAN > Voice VLAN LLDP-MED Device

This window displays the voice VLAN LLDP-MED voice devices connected to the Switch.

Voice VLAN LLDP-MED Device

Voice VLAN LLDP-MED Device Table

Total Entries: 0

| Index | Port | Chassis ID Subtype | Chassis ID | Port ID Subtype | Port ID | Create Time | Remain Time (sec) |
|-------|------|--------------------|------------|-----------------|---------|-------------|-------------------|
|-------|------|--------------------|------------|-----------------|---------|-------------|-------------------|

Figure 4.89 – L2 Features > VLAN > Voice VLAN > Voice VLAN LLDP-MED Device

L2 Features > STP > STP Global Settings

The Switch implements two versions of the Spanning Tree Protocol, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1D-2004 specification and a version compatible with the IEEE 802.1D-98 STP. RSTP can operate with legacy equipment implementing IEEE 802.1D-98, however the advantages of using RSTP will be lost.

The IEEE 802.1D-2004 Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1D-98 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.

By default, Spanning Tree Protocol 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.

The screenshot shows the 'STP Global Settings' configuration page. It is organized into five sections, each with an 'Apply' button:

- STP State:** Radio buttons for 'Disabled' (selected) and 'Enabled'.
- STP Traps:** Radio buttons for 'STP New Root Trap' (Disabled) and 'STP Topology Change Trap' (Disabled).
- STP Mode:** A dropdown menu set to 'RSTP'.
- STP Priority:** A dropdown menu set to '32768'.
- STP Configuration:** Four input fields: 'Bridge Max Age (6-40)' (20 sec), 'Bridge Hello Time (1-2)' (2 sec), 'Bridge Forward Time (4-30)' (15 sec), and 'TX Hold Count (1-10)' (6 times).

Figure 4.90 – L2 Functions > STP > STP Global Settings

The fields that can be configured are described below:

Spanning Tree State: Enable or disable the STP global state here.

STP New Root Trap: Enable or disable the STP new root trap option here.

STP Topology Change Trap: Enable or disable the STP topology change trap option here.

STP Mode: Select the STP mode used here. Options to choose from are **RSTP** and **STP**.

Priority: Select the STP priority value here. This value is between 0 and 61440. By default, this value is 32768. The lower the value, the higher the priority.

Bridge Max Age: 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 Hello Time: 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.

Bridge Forward Time: Enter the bridge's forwarding time value here. 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.

TX Hold Count: Enter the transmit hold count value here. 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 **Apply** to accept the changes made for each individual section.

L2 Features > STP > STP Port Settings

This window allows the user to configure STP parameters for individual ports or a range of ports. In addition to setting Spanning Tree parameters for use on the switch level, the Switch allows for the configuration of the

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.

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

| Port | State | Cost | Guard Root | Link Type | Port Fast | TCN Filter | BPDU Forward | Priority |
|-------|---------|-------------|------------|-----------|---------------|------------|--------------|----------|
| eth1 | Enabled | 0/0 | Disabled | Auto/P2P | Edge/Non-Edge | Disabled | Disabled | 128 |
| eth2 | Enabled | 0/200000000 | Disabled | Auto/P2P | Edge/Non-Edge | Disabled | Disabled | 128 |
| eth3 | Enabled | 0/200000000 | Disabled | Auto/P2P | Edge/Non-Edge | Disabled | Disabled | 128 |
| eth4 | Enabled | 0/200000000 | Disabled | Auto/P2P | Edge/Non-Edge | Disabled | Disabled | 128 |
| eth5 | Enabled | 0/200000000 | Disabled | Auto/P2P | Edge/Non-Edge | Disabled | Disabled | 128 |
| eth6 | Enabled | 0/200000000 | Disabled | Auto/P2P | Edge/Non-Edge | Disabled | Disabled | 128 |
| eth7 | Enabled | 0/200000000 | Disabled | Auto/P2P | Edge/Non-Edge | Disabled | Disabled | 128 |
| eth8 | Enabled | 0/200000000 | Disabled | Auto/P2P | Edge/Non-Edge | Disabled | Disabled | 128 |
| eth9 | Enabled | 0/200000000 | Disabled | Auto/P2P | Edge/Non-Edge | Disabled | Disabled | 128 |
| eth10 | Enabled | 0/200000000 | Disabled | Auto/P2P | Edge/Non-Edge | Disabled | Disabled | 128 |
| eth11 | Enabled | 0/200000000 | Disabled | Auto/P2P | Edge/Non-Edge | Disabled | Disabled | 128 |
| eth12 | Enabled | 0/200000000 | Disabled | Auto/P2P | Edge/Non-Edge | Disabled | Disabled | 128 |
| eth13 | Enabled | 0/200000000 | Disabled | Auto/P2P | Edge/Non-Edge | Disabled | Disabled | 128 |
| eth14 | Enabled | 0/200000000 | Disabled | Auto/P2P | Edge/Non-Edge | Disabled | Disabled | 128 |
| eth15 | Enabled | 0/200000000 | Disabled | Auto/P2P | Edge/Non-Edge | Disabled | Disabled | 128 |
| eth16 | Enabled | 0/200000000 | Disabled | Auto/P2P | Edge/Non-Edge | Disabled | Disabled | 128 |

Figure 4.91 – L2 Functions > STP > STP Port Settings

The fields that can be configured are described below:

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

Cost: Enter the cost value here. This value must be between 1 and 200000000. This value 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). 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. The default port cost for a 100Mbps port is 200000 and the default port cost for a Gigabit port is 20000. The lower the number, the greater the probability the port will be chosen to forward packets.

State: Enable or disable the STP port state.

Guard Root: Enable or disable the guard root function.

Link Type: Select the link type option here. 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 here. 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 **Disabled** 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: 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**.

Priority: Select the priority value here. Options to choose from are 0 to 240. By default this option is 128. A lower value has higher priority.

BPDU Forward: Enable or disable BPDU forwarding. If enabled, the received STP BPDU will be forwarded to all VLAN member ports in the untagged form. By default, this option is **Disabled**.

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

L2 Features > STP > STP Global Information

This window is used to display the STP global information.

| STP Global Information | |
|---|-----------------------|
| STP Global Information[Mode RSTP] | |
| Bridge Address | 00-77-93-03-00-00 |
| Designated Root Address / Priority | 00-00-00-00-00-00 / 0 |
| Regional Root Bridge Address / Priority | 00-00-00-00-00-00 / 0 |
| Designated Bridge Address / Priority | 00-00-00-00-00-00 / 0 |

Figure 4.92 – L2 Functions > STP > STP Global Info

L2 Features > STP > STP Port Information

This window is used to view and configure the STP port information settings.

| STP Port Information | | | | |
|----------------------|----------|-------------------------|--------|------------------|
| STP Port Information | | | | |
| Port | eth1 | Clear Detected Protocol | | Find |
| eth1 Settings | | | | |
| Cost | Priority | Status | Role | |
| 200000 | 128 | Forwarding | NonStp | Edit |
| | | | | 1/1 < > 1 > > Go |

Figure 4.93 – L2 Functions > STP > STP Port Information

The fields that can be configured are described below:

Port: Select the port number that will be cleared here.

Click **Clear Detected Protocol** to clear the detected protocol settings for the port selected.

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

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

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

L2 Features > Loopback Detection

The Loopback Detection function is used to detect the loop created by a specific port. This feature is used to temporarily shut down a port on the Switch when a CTP (Configuration Testing Protocol) packet has been looped back to the Switch. When the Switch detects CTP packets received from a port, this signifies a loop on the network. The Switch will automatically block the port and send an alert to the administrator. The Loopback Detection function can be implemented on a range of ports at a time. The user may enable or disable this function using the drop-down menu.

Loopback Detection

Loopback Detection Global Settings

Loopback Detection State: Mode:

Trap State: Interval (1-32767): sec

Loopback Detection Port Settings

From Port: To Port: State:

| Port | Loopback Detection State | Result | Time Left (sec) |
|-------|--------------------------|--------|-----------------|
| eth1 | Disabled | Normal | - |
| eth2 | Disabled | Normal | - |
| eth3 | Disabled | Normal | - |
| eth4 | Disabled | Normal | - |
| eth5 | Disabled | Normal | - |
| eth6 | Disabled | Normal | - |
| eth7 | Disabled | Normal | - |
| eth8 | Disabled | Normal | - |
| eth9 | Disabled | Normal | - |
| eth10 | Disabled | Normal | - |
| eth11 | Disabled | Normal | - |
| eth12 | Disabled | Normal | - |
| eth13 | Disabled | Normal | - |
| eth14 | Disabled | Normal | - |
| eth15 | Disabled | Normal | - |
| eth16 | Disabled | Normal | - |

Figure 4.94 – L2 Features > Loopback Detection

The fields that can be configured are described below:

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

Mode: The loopback detection mode is **Port-based**.

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

Interval: Enter the interval in seconds that the device will transmit all the CTP (Configuration Test Protocol) packets to detect a loop-back event. The valid range is from 1 to 32767 seconds. The default setting is 10 seconds.

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

State: Enable or disable the state of the port.

Click **Apply** to accept the changes made for each individual section.

L2 Features > Link Aggregation

Understanding Port Trunk Groups

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

The DXS-1100-10TS supports up to 5 port trunk groups with 1 to 4 ports in each group. The DXS-1100-16TC supports up to 8 port trunk groups with 1 to 8 ports in each group.

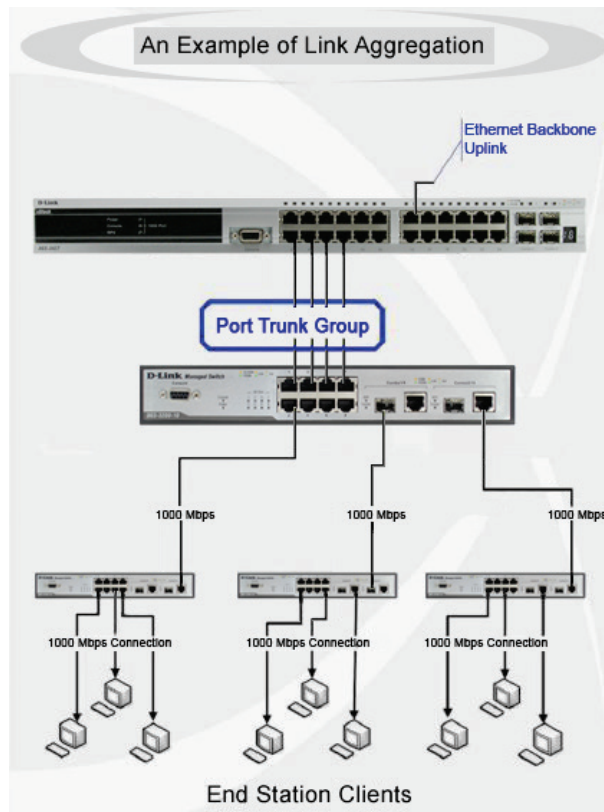


Figure 4.95 – Example of Port Trunk Group

The Switch treats all ports in a trunk group as a single port. Data transmitted to a specific host (destination address) will always be transmitted over the same port in a trunk group. This allows packets in a data stream to arrive in the same order they were sent.

Link aggregation allows several ports to be grouped together and to act as a single link. This gives a bandwidth that is a multiple of a single link's bandwidth.

Link aggregation is most commonly used to link a bandwidth intensive network device or devices, such as a server, to the backbone of a network.

The DXS-1100-10TS allows the creation of up to 5 link aggregation groups, each group consisting of 1 to 4 links (ports); and the DXS-1100-16TC allows the creation of up to 8 link aggregation groups, each group consisting of 1 to 8 links (ports). Each port can only belong to a single link aggregation group.

All of the ports in the group must be members of the same VLAN, and their STP status, static multicast, traffic control; traffic segmentation and 802.1p default priority configurations must be identical. Port locking must not be enabled on the trunk group. Further, the LACP aggregated links must all be of the same speed and should be configured as full duplex.

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

The Spanning Tree Protocol will treat a link aggregation group as a single link, on the switch level. On the port level, the STP will use the port parameters of the Master Port in the calculation of port cost and in determining the state of the link aggregation group. If two redundant link aggregation groups are configured on the Switch, STP will block one entire group; in the same way STP will block a single port that has a redundant link.



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

This window is used to view and configure the link aggregation settings.

| Channel Group | Protocol | Max Ports | Member Number | Member Ports |
|---------------|----------|-----------|---------------|--------------|
| Port-channel1 | Static | 8 | 1 | 2 |

Figure 4.96 – L2 Features > Link Aggregation

The fields that can be configured are described below:

System Priority: Enter the system's priority value used here. 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: Select the load balancing algorithm that will be used here. 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**.

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

Group ID: Enter the channel group number here. This value must be between 1 and 8. 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 the mode option here. Options to choose from are **On**, **Active**, and **Passive**. If the mode **On** is specified, the channel group type is static. If the mode **Active** or **Passive** is specified, 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 **Apply** to accept the changes made for each individual section.

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

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

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

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

After clicking **Channel Detail**, the following page will be available.

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

In order to use IGMP Snooping it must first be enabled for the entire Switch under IGMP Global Settings at the top of the window. You may then fine-tune the settings for each VLAN by clicking the corresponding **Edit** button. When enabled for IGMP snooping, the Switch can open or close a port to a specific multicast group member based on IGMP messages sent from the device to the IGMP host or vice versa. The Switch

monitors IGMP messages and discontinues forwarding multicast packets when there are no longer hosts requesting that they continue.

IGMP Snooping Settings

Global Settings
Global State Enabled Disabled Apply

VLAN Status Settings
VID (1-4094) Enabled Disabled Apply

IGMP Snooping Table
VID (1-4094) Find Find All

Total Entries: 1

| VID | VLAN Name | Status | |
|-----|-----------|---------|--|
| 1 | default | Enabled | Show Detail Edit |

1/1 < << 1 >> > Go

Figure 4.97 – L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings

The fields that can be configured are described below:

Global State: Enable or disable IGMP snooping global state.

VID: Enter a VLAN ID from 1 to 4094, and select to enable or disable IGMP snooping on the VLAN.

VID: Enter a VLAN ID from 1 to 4094.

Click **Apply** to accept the changes made for each individual section.

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

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

Click **Show Detail** to see the detail information of the specific VLAN.

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

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

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

IGMP Snooping VLAN Parameters

IGMP Snooping VLAN Parameters

| | |
|----------------------------|-------------|
| VID | 1 |
| Status | Enabled |
| Minimum Version | v1 |
| Querier State | Disabled |
| Querier IP | 0.0.0.0 |
| Querier Expiry Time | 0 seconds |
| Query Version | v3 |
| Query Interval | 125 seconds |
| Max Response Time | 10 seconds |
| Robustness Value | 2 |
| Last Member Query Interval | 1 seconds |
| Rate Limit | 0 |

Modify

Figure 4.98 – L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping VLAN Parameters

The window displays the detail information about IGMP snooping VLAN.
 Click **Modify** to edit the information in the following window.
 Click the **X** button at the upper-right side to close the window.

After clicking **Modify** or **Edit** in IGMP Snooping Settings window, the following window will appear.

Figure 4.99 – L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping VLAN Settings

The fields that can be configured are described below:

Minimum Version: Select the minimum version of IGMP hosts that is allowed on the VLAN.

Querier State: Enable or disable the querier state.

Query Version: Select the general query packet version sent by the IGMP snooping querier. Options to choose from are **1**, **2**, and **3**.

Query Interval: Enter the interval at which the IGMP snooping querier sends IGMP general query messages periodically.

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

Robustness Value: Enter the robustness variable used in IGMP snooping.

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

Rate Limit: Enter the IGMP snooping rate limit used. Tick **No Limit** to ignore the rate limit.

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

Click the **X** button at the upper-right side to close the window.

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

This window is used to configure and view the IGMP snooping static group, and view IGMP snooping group.

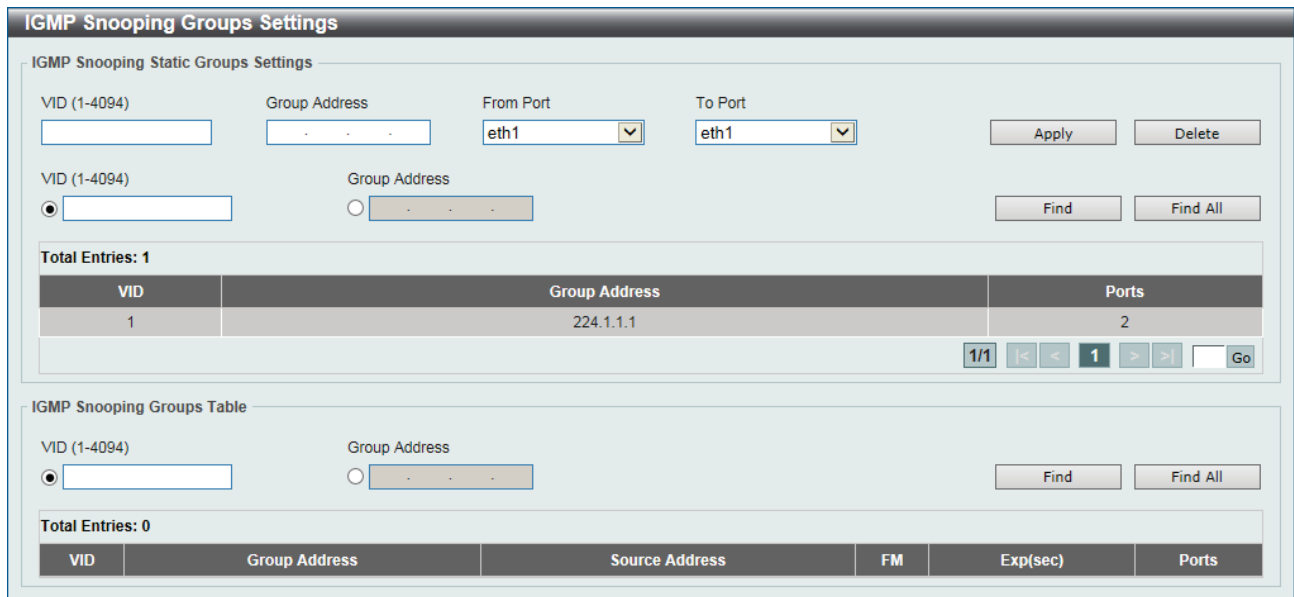


Figure 4.100 – L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Groups Settings

The fields that can be configured are described below:

VID: Enter a VLAN ID of the multicast group.

Group Address: Enter an IP multicast group address.

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

VID: Click the radio button and enter a VLAN ID of the multicast group.

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

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

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

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

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

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

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

This window is used to configure the specified interface(s) as the multicast router ports or as forbidden to be multicast router ports on the Switch.

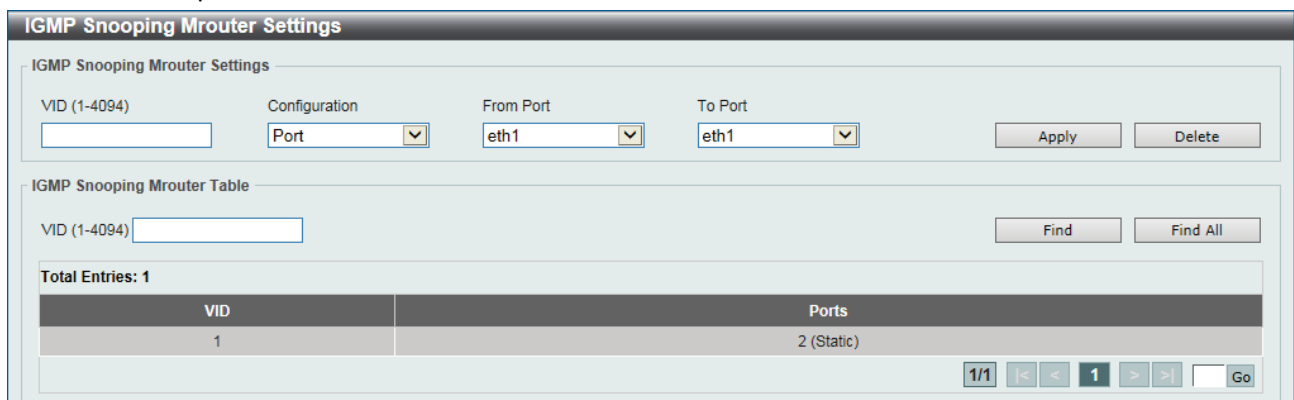


Figure 4.101 – L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Mrouter Settings

The fields that can be configured are described below:

VID: Enter a VLAN ID between 1 and 4094.

Configuration: Select the port configuration. Options to choose from are **Port** and **Forbidden Port**.

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 appropriate port range used for the configuration here.

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

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

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

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

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

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

This window is used to clear and display the IGMP snooping related statistics.

| Port | IGMPv1 | | | | IGMPv2 | | | | | | IGMPv3 | | | |
|------|--------|-------|--------|-------|--------|-------|-------|--------|-------|-------|--------|-------|--------|-------|
| | RX | | TX | | RX | | | TX | | | RX | | TX | |
| | Report | Query | Report | Query | Report | Query | Leave | Report | Query | Leave | Report | Query | Report | Query |
| eth2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Figure 4.102 – L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Statistics Settings

The fields that can be configured are described below:

Statistics: Select the interface here. Options to choose from are **All**, **VLAN**, and **Port**.

VID: Enter a VLAN ID between 1 and 4094. This is available when **VLAN** is selected in the **Statistics** list.

From Port / To Port: Select the appropriate port range used for the configuration here. This is available when **Port** is selected in the **Statistics** list.

Find Type: Select the interface type. Options to choose from are **VLAN** and **Port**.

VID: Enter a VLAN ID between 1 and 4094. This is available when **VLAN** is selected in the **Find Type** list.

From Port / To Port: Select the appropriate port range used for the configuration here. This is available when **Port** is selected in the **Find Type** list.

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

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

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

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

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

Multicast Listener Discovery (MLD) Snooping is an IPv6 function used similarly to IGMP snooping in IPv4. It is used to discover ports on a VLAN that are requesting multicast data. Instead of flooding all ports on a selected VLAN with multicast traffic, MLD snooping will only forward multicast data to ports that wish to receive this data through the use of queries and reports produced by the requesting ports and the source of the multicast traffic.

MLD snooping is accomplished through the examination of the layer 3 part of an MLD control packet transferred between end nodes and a MLD router. When the Switch discovers that this route is requesting multicast traffic, it adds the port directly attached to it into the correct IPv6 multicast table, and begins the process of forwarding multicast traffic to that port. This entry in the multicast routing table records the port, the VLAN ID, and the associated multicast IPv6 multicast group address, and then considers this port to be an active listening port. The active listening ports are the only ones to receive multicast group data.

MLD Control Messages

Three types of messages are transferred between devices using MLD snooping. These three messages are all defined by four ICMPv6 packet headers, labeled 130, 131, 132, and 143.

1. **Multicast Listener Query** - Similar to the IGMPv2 Host Membership Query for IPv4, and labeled as 130 in the ICMPv6 packet header, this message is sent by the router to ask if any link is requesting multicast data. There are two types of MLD query messages emitted by the router. The General Query is used to advertise all multicast addresses that are ready to send multicast data to all listening ports, and the Multicast Specific query, which advertises a specific multicast address that is also ready. These two types of messages are distinguished by a multicast destination address located in the IPv6 header and a multicast address in the Multicast Listener Query Message.
2. **Multicast Listener Report, Version 1** - Comparable to the Host Membership Report in IGMPv2, and labeled as 131 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.
3. **Multicast Listener Done** - Akin to the Leave Group Message in IGMPv2, and labeled as 132 in the ICMPv6 packet header, this message is sent by the multicast listening port stating that it is no longer interested in receiving multicast data from a specific multicast group address, therefore stating that it is "done" with the multicast data from this address. Once this message is received by the Switch, it will no longer forward multicast traffic from a specific multicast group address to this listening port.
4. **Multicast Listener Report, Version 2** - Comparable to the Host Membership Report in IGMPv3, and labeled as 143 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.

This window is used to configure the MLD snooping settings.

MLD Snooping Settings

Global Settings

Global State Enabled Disabled Apply

VLAN Status Settings

VID (1-4094) Enabled Disabled Apply

MLD Snooping Table

VID (1-4094) Find Find All

Total Entries: 1

| VID | VLAN Name | Status |
|-----|-----------|---------|
| 1 | default | Enabled |

Show Detail Edit

1/1 < << 1 >> > Go

Figure 4.103 – L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Settings

The fields that can be configured are described below:

Global State: Enable or disable MLD snooping global state.

VID: Enter a VLAN ID from 1 to 4094, and select to enable or disable MLD snooping on the VLAN.

VID: Enter a VLAN ID from 1 to 4094.

Click **Apply** to accept the changes made for each individual section.

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

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

Click **Show Detail** to see the detail information of the specific VLAN.

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

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

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

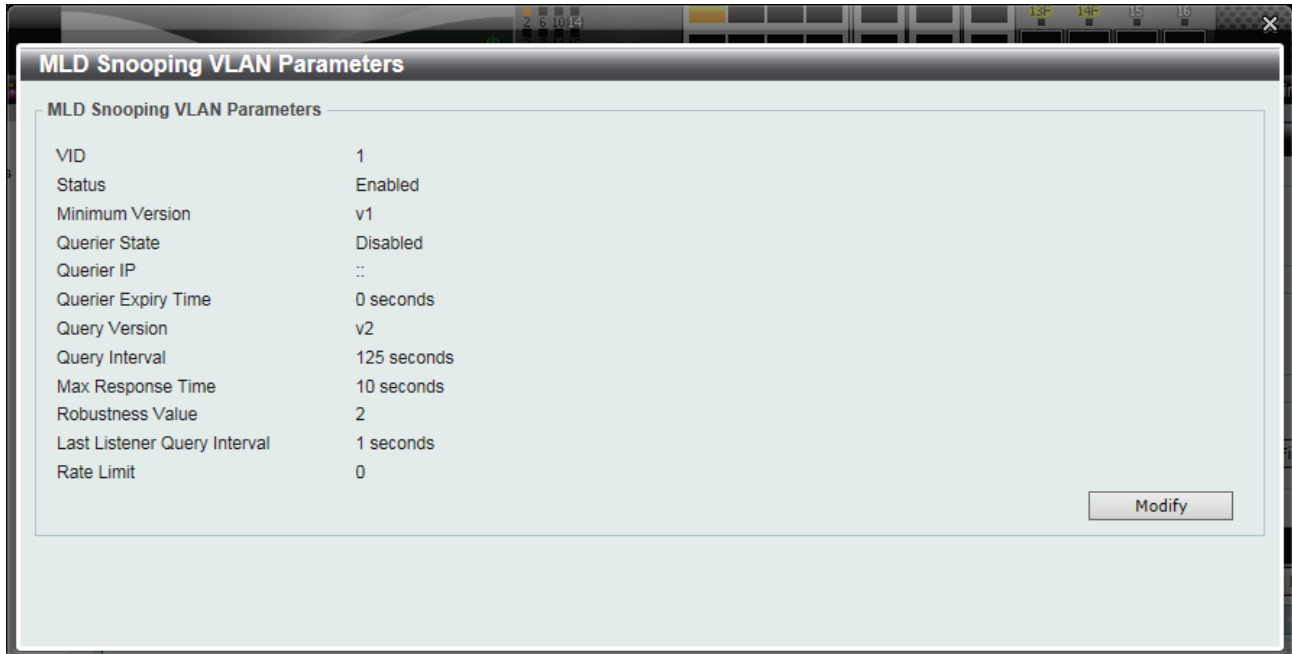


Figure 4.104 – L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping VLAN Parameters

The window displays the detail information about MLD snooping VLAN.

Click **Modify** to edit the information in the following window.

Click the **X** button at the upper-right side to close the window.

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

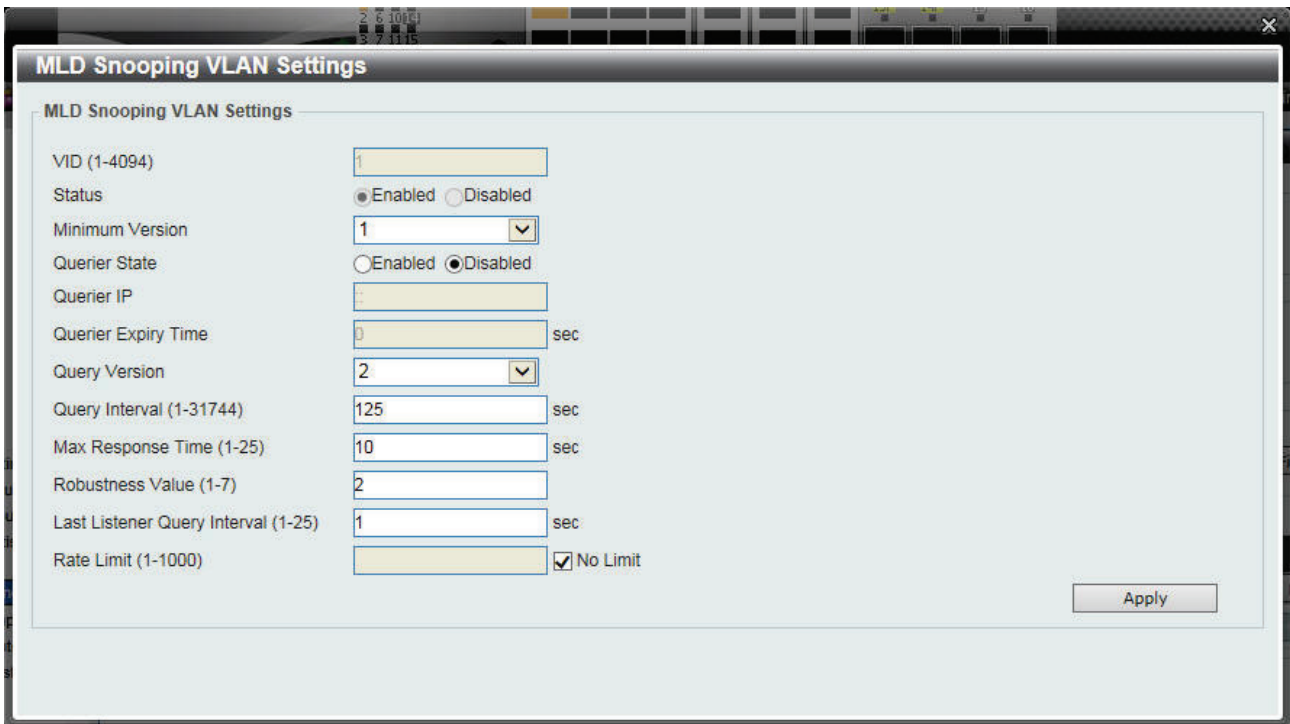


Figure 4.105 – L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping VLAN Settings

The fields that can be configured are described below:

Minimum Version: Select the minimum version of MLD hosts that is allowed on the VLAN.

Querier State: Enable or disable the querier state.

Query Version: Select the general query packet version sent by the MLD snooping querier. Options to choose from are **1** and **2**.

Query Interval: Enter the interval at which the MLD snooping querier sends MLD general query messages periodically.

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

Robustness Value: Enter the robustness variable used in MLD snooping.

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

Rate Limit: Enter the MLD snooping rate limit used. Tick **No Limit** to ignore the rate limit.

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

Click the **X** button at the upper-right side to close the window.

L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Groups Settings

This window is used to configure and view the MLD snooping static group, and view MLD snooping group.

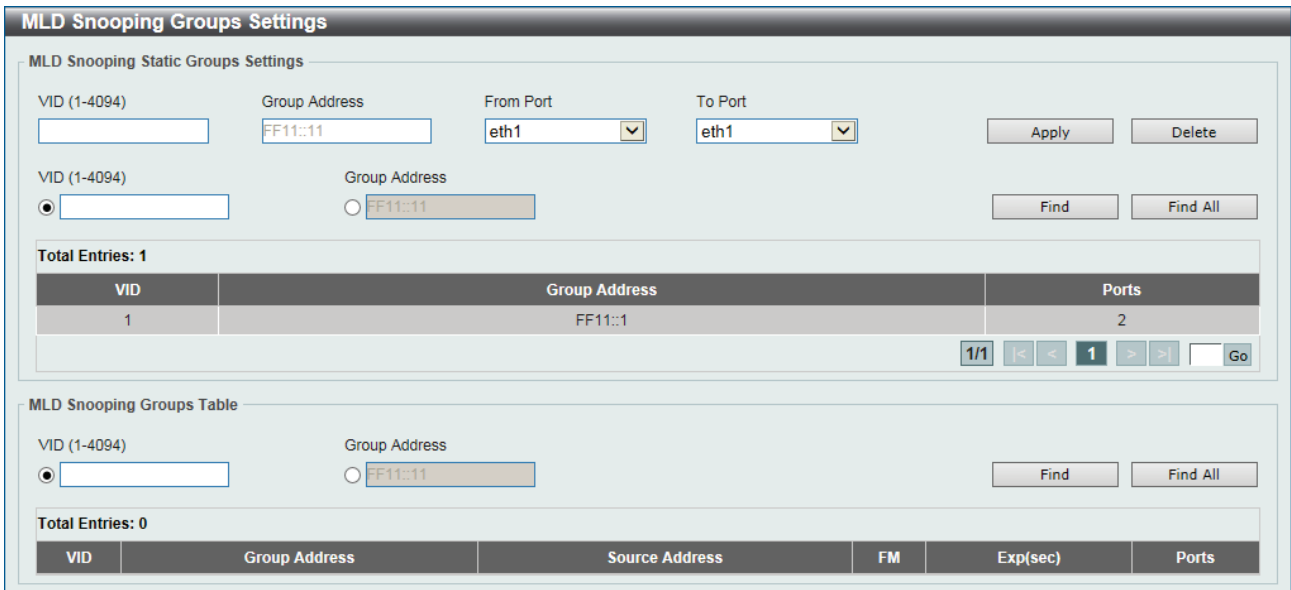


Figure 4.106 – L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Groups Settings

The fields that can be configured are described below:

VID: Enter a VLAN ID of the multicast group.

Group Address: Enter an IPv6 multicast group address.

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

VID: Click the radio button and enter a VLAN ID of the multicast group.

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

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

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

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

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

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

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

This window is used 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.

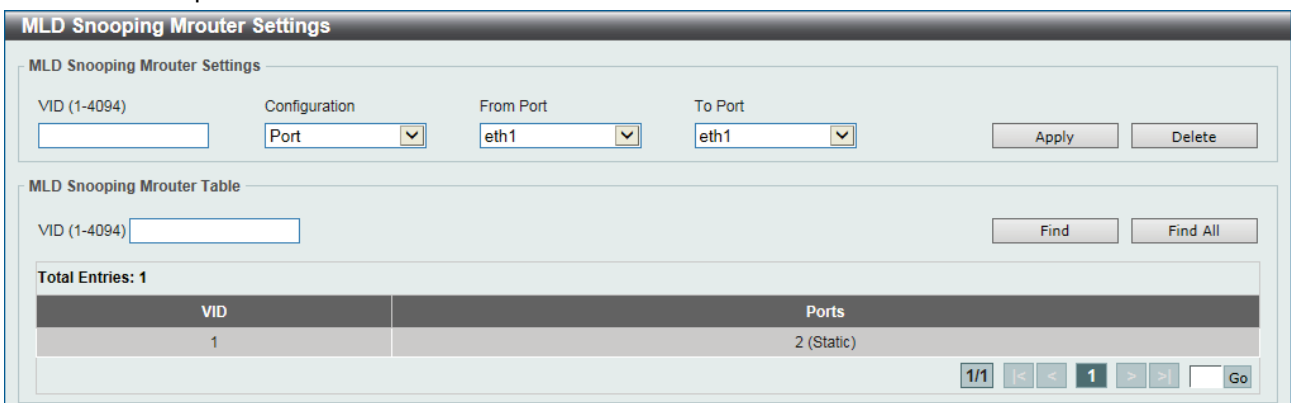


Figure 4.107 – L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Mrouter Settings

The fields that can be configured are described below:

VID: Enter a VLAN ID between 1 and 4094.

Configuration: Select the port configuration. Options to choose from are **Port** and **Forbidden Port**.

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 appropriate port range used for the configuration here.

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

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

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

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

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

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

This window is used to clear and display the MLD snooping related statistics.

MLD Snooping Statistics Settings

MLD Snooping Statistics Settings

Statistics: All | VID (1-4094): | From Port: eth1 | To Port: eth1 | Clear

MLD Snooping Statistics Table

Find Type: VLAN | VID (1-4094): | From Port: eth1 | To Port: eth1 | Find | Find All

Total Entries: 1

| Port | MLDv1 | | | | MLDv2 | | RX | TX |
|------|--------|------|--------|------|--------|--------|-------|-------|
| | RX | | TX | | RX | TX | RX | TX |
| | Report | Done | Report | Done | Report | Report | Query | Query |
| eth2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

1/1 | < < 1 > > | Go

Figure 4.108 – L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Statistics Settings

The fields that can be configured are described below:

Statistics: Select the interface here. Options to choose from are **All**, **VLAN**, and **Port**.

VID: Enter a VLAN ID between 1 and 4094. This is available when **VLAN** is selected in the **Statistics** list.

From Port / To Port: Select the appropriate port range used for the configuration here. This is available when **Port** is selected in the **Statistics** list.

Find Type: Select the interface type. Options to choose from are **VLAN** and **Port**.

VID: Enter a VLAN ID between 1 and 4094. This is available when **VLAN** is selected in the **Find Type** list.

From Port / To Port: Select the appropriate port range used for the configuration here. This is available when **Port** is selected in the **Find Type** list.

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

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

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

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

L2 Features > L2 Multicast Control> Multicast Filtering

This window is used to view and configure the Layer 2 multicast filtering settings.

Multicast Filtering

Multicast Filtering

VID List: Multicast Filter Mode:

Total Entries: 1

| VLAN | Multicast Filter Mode |
|---------|-----------------------------|
| default | Forward Unregistered Groups |

1/1 < < 1 > >

Figure 4.109 – L2 Features > L2 Multicast Control > Multicast Filtering

The fields that can be configured are described below:

VID List: Enter the VLAN ID list that will be used for this configuration here.

Multicast Filter Mode: Select the multicast filter mode here. 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 filtered.

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

Enter a page number and click **Go** 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 disabled by default.

LLDP Global Settings

LLDP State: Enabled Disabled

LLDP Forward State: Enabled Disabled

LLDP Trap State: Enabled Disabled

LLDP-MED Trap State: Enabled Disabled

LLDP-MED Configuration

Fast Start Repeat Count (1-10): times

LLDP Configurations

Message TX Interval (5-32768): sec

Message TX Hold Multiplier (2-10): sec

Reinit Delay (1-10): sec

TX Delay (1-8192): sec

LLDP System Information

| | |
|-------------------------------|----------------------------|
| Chassis ID Subtype | MAC Address |
| Chassis ID | 00-91-06-11-00-01 |
| System Name | Switch |
| System Description | 10 Gigabit Ethernet Switch |
| System Capabilities Supported | Repeater, Bridge |
| System Capabilities Enabled | Repeater, Bridge |

LLDP-MED System Information

| | |
|-------------------|----------------------------------|
| Device Class | Network Connectivity Device |
| Hardware Revision | A1 |
| Firmware Revision | 1.00.003 |
| Software Revision | 1.10.003 |
| Serial Number | |
| Manufacturer Name | D-Link Corporation |
| Model Name | DXS-1100-16TC 10 Gigabit Etherne |
| Asset ID | |

Figure 4.110 – L2 Features > LLDP > LLDP Global Settings

The fields that can be configured are described below:

LLDP State: Select this option to enable or disable the LLDP feature

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

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

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

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

Message TX Interval: Enter the interval between consecutive transmissions of LLDP advertisements on each physical interface. The range is from 5 to 32768 seconds.

Message TX Hold Multiplier: Enter the multiplier on the LLDPDU transmission interval that used to compute the TTL value of an LLDPDU. This value must be between 2 and 10.

Reinit Delay: Enter the delay value for LLDP initialization on an interface. This value must be between 1 and 10 seconds.

TX Delay: Enter the delay value for sending successive LLDPDUs on an interface. The valid values are from 1 to 8192 seconds and should not be greater than one-fourth of the transmission interval timer.

Click **Apply** to accept the changes made for each individual section.

L2 Features > LLDP > LLDP Port Settings

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

LLDP Port Settings

LLDP Port Settings

From Port: To Port: Notification: Subtype: Admin State: IP Subtype: Action: Address:

Note: The address should be the switch's address.

| Port | Notification | Subtype | Admin State | IPv4/IPv6 Address |
|-------|--------------|---------|-------------|-------------------|
| eth1 | Disabled | Local | TX and RX | |
| eth2 | Disabled | Local | TX and RX | |
| eth3 | Disabled | Local | TX and RX | |
| eth4 | Disabled | Local | TX and RX | |
| eth5 | Disabled | Local | TX and RX | |
| eth6 | Disabled | Local | TX and RX | |
| eth7 | Disabled | Local | TX and RX | |
| eth8 | Disabled | Local | TX and RX | |
| eth9 | Disabled | Local | TX and RX | |
| eth10 | Disabled | Local | TX and RX | |
| eth11 | Disabled | Local | TX and RX | |
| eth12 | Disabled | Local | TX and RX | |
| eth13 | Disabled | Local | TX and RX | |
| eth14 | Disabled | Local | TX and RX | |
| eth15 | Disabled | Local | TX and RX | |
| eth16 | Disabled | Local | TX and RX | |

Figure 4.111 – L2 Features > LLDP > LLDP Port Settings

The fields that can be configured are described below:

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

Notification: Select to enable or disable the notification feature here.

Subtype: Select the subtype of LLDP TLV(s). Options to choose from are **MAC Address** and **Local**.

Admin State: Select the local LLDP agent and allow it to send and receive LLDP frames on the port. Options to choose from are **TX**, **RX**, **TX and RX**, and **Disabled**.

TX - The local LLDP agent can only transmit LLDP frames.

RX - The local LLDP agent can only receive LLDP frames.

TX and RX - The local LLDP agent can both transmit and receive LLDP frames. This is the default value.

Disabled - The local LLDP agent can neither transmit nor receive LLDP frames.

IP Subtype: Select the type of the IP address information to be sent. Options to choose from are **Default**, **IPv4** and **IPv6**.

Action: Enable or disable the action field.

Address: Enter the IPv4 or IPv6 address that will be sent.

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



NOTE: The IPv4 or IPv6 address entered here should be an existing LLDP management IP address.

L2 Features > LLDP > LLDP Management Address List

This window is used to view the LLDP management address list.

| Subtype | Address | IF Type | OID | Advertising Ports |
|---------|----------------------|---------|-------------------------|-------------------|
| IPv4 | 10.90.90.90(default) | IfIndex | 1.3.6.1.4.1.171.10.1... | - |
| IPv4 | 10.90.90.90 | IfIndex | 1.3.6.1.4.1.171.10.1... | - |

Figure 4.112 – L2 Features > LLDP > LLDP Management Address List

The fields that can be configured are described below:

All/IPv4/IPv6: Select the subtype. Options to choose from are **All**, **IPv4** and **IPv6**.

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

LLDP Basic TLVs Settings

Type-length-value (TLV) allows the specific sending information as a TLV element within LLDP packets. This window is used to enable the settings for the Basic TLVs Settings. An active LLDP port on the Switch always included mandatory data in its outbound advertisements. There are four optional data types that can be configured for an individual port or group of ports to exclude one or more of these data types from outbound LLDP advertisements. The mandatory data type includes four basic types of information (end of LLDPDU TLV, chassis ID TLV, port ID TLV, and Time to Live TLV). The mandatory data types cannot be disabled. There are also four data types which can be optionally selected. These include Port Description, System Name, System Description and System Capability.

| Port | Port Description | System Name | System Description | System Capabilities |
|-------|------------------|-------------|--------------------|---------------------|
| eth1 | Disabled | Disabled | Disabled | Disabled |
| eth2 | Disabled | Disabled | Disabled | Disabled |
| eth3 | Disabled | Disabled | Disabled | Disabled |
| eth4 | Disabled | Disabled | Disabled | Disabled |
| eth5 | Disabled | Disabled | Disabled | Disabled |
| eth6 | Disabled | Disabled | Disabled | Disabled |
| eth7 | Disabled | Disabled | Disabled | Disabled |
| eth8 | Disabled | Disabled | Disabled | Disabled |
| eth9 | Disabled | Disabled | Disabled | Disabled |
| eth10 | Disabled | Disabled | Disabled | Disabled |
| eth11 | Disabled | Disabled | Disabled | Disabled |
| eth12 | Disabled | Disabled | Disabled | Disabled |
| eth13 | Disabled | Disabled | Disabled | Disabled |
| eth14 | Disabled | Disabled | Disabled | Disabled |
| eth15 | Disabled | Disabled | Disabled | Disabled |
| eth16 | Disabled | Disabled | Disabled | Disabled |

Figure 4.113 – L2 Features > LLDP > LLDP Basic TLVs Settings

The fields that can be configured are described below:

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

Port Description: Enable or disable the Port Description option.

System Name: Enable or disable the System Name option.

System Description: Enable or disable the System Description option.

System Capabilities: Enable or disable the System Capabilities option.

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

L2 Features > LLDP > LLDP Dot1 TLVs Settings

LLDP Dot1 TLVs are organizationally specific TLVs which are defined in IEEE 802.1 and used 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.

LLDP Dot1 TLVs Settings

LLDP Dot1 TLVs Settings

From Port: eth1 | To Port: eth1 | Port VLAN: Disabled | VLAN Name: Disabled | Protocol Identity: Disabled, None

| Port | Port VLAN ID | Enabled VLAN Name | Enabled Protocol Identity |
|-------|--------------|-------------------|---------------------------|
| eth1 | Disabled | | |
| eth2 | Disabled | | |
| eth3 | Disabled | | |
| eth4 | Disabled | | |
| eth5 | Disabled | | |
| eth6 | Disabled | | |
| eth7 | Disabled | | |
| eth8 | Disabled | | |
| eth9 | Disabled | | |
| eth10 | Disabled | | |
| eth11 | Disabled | | |
| eth12 | Disabled | | |
| eth13 | Disabled | | |
| eth14 | Disabled | | |
| eth15 | Disabled | | |
| eth16 | Disabled | | |

Figure 4.114 – L2 Features > LLDP > LLDP Dot1 TLVs Settings

The fields that can be configured are described below:

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

Port VLAN: 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.

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

Protocol Identity: Enable or disable the Protocol Identity TLV to send, and the protocol name. Options for protocol name to choose from are **None**, **LACP**, **STP**, and **All**.

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

L2 Features > LLDP > LLDP Dot3 TLVs Settings

This window is used 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.

LLDP Dot3 TLVs Settings

LLDP Dot3 TLVs Settings

From Port

To Port

MAC/PHY
Configuration/Status

Link Aggregation

Maximum Frame Size

| Port | MAC/PHY Configuration/Status | Link Aggregation | Maximum Frame Size |
|-------|------------------------------|------------------|--------------------|
| eth1 | Disabled | Disabled | Disabled |
| eth2 | Disabled | Disabled | Disabled |
| eth3 | Disabled | Disabled | Disabled |
| eth4 | Disabled | Disabled | Disabled |
| eth5 | Disabled | Disabled | Disabled |
| eth6 | Disabled | Disabled | Disabled |
| eth7 | Disabled | Disabled | Disabled |
| eth8 | Disabled | Disabled | Disabled |
| eth9 | Disabled | Disabled | Disabled |
| eth10 | Disabled | Disabled | Disabled |
| eth11 | Disabled | Disabled | Disabled |
| eth12 | Disabled | Disabled | Disabled |
| eth13 | Disabled | Disabled | Disabled |
| eth14 | Disabled | Disabled | Disabled |
| eth15 | Disabled | Disabled | Disabled |
| eth16 | Disabled | Disabled | Disabled |

Figure 4.115 – L2 Features > LLDP > LLDP Dot3 TLVs Settings

The fields that can be configured are described below:

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

MAC/PHY Configuration/Status: Enable or disable the MAC/PHY Configuration/Status TLV to send. The MAC/PHY Configuration/Status TLV is an optional TLV that identifies (1) the duplex and bit-rate capability of the sending IEEE 802.3 LAN node, and (2) the current duplex and bit-rate settings of the sending IEEE 802.3 LAN node.

Link Aggregation: Enable or disable the Link Aggregation TLV to send. The Link Aggregation TLV indicates contains the following information. Whether the link is capable of being aggregated, whether the link is currently in an aggregation, and the aggregated port channel ID of the port. If the port is not aggregated, then the ID is 0.

Maximum Frame Size: Enable or disable the Maximum Frame Size TLV to send. The Maximum Frame Size TLV indicates the maximum frame size capability of the implemented MAC and PHY.

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

L2 Features > LLDP > LLDP-MED Port Settings

This window is used to enable or disable transmitting LLDP-MED TLVs.

LLDP-MED Port Settings

LLDP-MED Port Settings

From Port: eth1 ▼ To Port: eth1 ▼ Notification: Disabled ▼ Capabilities: Disabled ▼ Network Policy: Disabled ▼ Inventory: Disabled ▼ Apply

| Port | Notification | Capabilities | Network Policy | Inventory |
|-------|--------------|--------------|----------------|-----------|
| eth1 | Disabled | Disabled | Disabled | Disabled |
| eth2 | Disabled | Disabled | Disabled | Disabled |
| eth3 | Disabled | Disabled | Disabled | Disabled |
| eth4 | Disabled | Disabled | Disabled | Disabled |
| eth5 | Disabled | Disabled | Disabled | Disabled |
| eth6 | Disabled | Disabled | Disabled | Disabled |
| eth7 | Disabled | Disabled | Disabled | Disabled |
| eth8 | Disabled | Disabled | Disabled | Disabled |
| eth9 | Disabled | Disabled | Disabled | Disabled |
| eth10 | Disabled | Disabled | Disabled | Disabled |
| eth11 | Disabled | Disabled | Disabled | Disabled |
| eth12 | Disabled | Disabled | Disabled | Disabled |
| eth13 | Disabled | Disabled | Disabled | Disabled |
| eth14 | Disabled | Disabled | Disabled | Disabled |
| eth15 | Disabled | Disabled | Disabled | Disabled |
| eth16 | Disabled | Disabled | Disabled | Disabled |

Figure 4.116 – L2 Features > LLDP > LLDP-MED Port Settings

The fields that can be configured are described below:

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

Notification: Select this option to enable or disable transmitting the LLDP-MED notification TLV.

Capabilities: Enable or disable transmitting the LLDP-MED capabilities TLV.

Network Policy: Enable or disable transmitting the LLDP-MED network policy TLV.

Inventory: Select this option to enable or disable transmitting the LLDP-MED inventory management TLV.

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

L2 Features > LLDP > LLDP Statistics Information

This window is used to view the neighbor detection activity, LLDP Statistics and the settings for individual ports on the Switch.

LLDP Statistics Information

LLDP Statistics Information

| | | |
|------------------|---|--|
| Last Change Time | 0 | <input type="button" value="Clear Counter"/> |
| Total Inserts | 0 | |
| Total Deletes | 0 | |
| Total Drops | 0 | |
| Total Ageouts | 0 | |

LLDP Statistics Ports

Port:

| Port | Total Transmits | Total Discards | Total Errors | Total Receives | Total TLV Discards | Total TLV Unknowns | Total Ageouts |
|-------|-----------------|----------------|--------------|----------------|--------------------|--------------------|---------------|
| eth1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| eth2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| eth3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| eth4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| eth5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| eth6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| eth7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| eth8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| eth9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| eth10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| eth11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| eth12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| eth13 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| eth14 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| eth15 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| eth16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Figure 4.117 – L2 Features > LLDP > LLDP Statistics Information

The fields that can be configured are described below:

Port: Select the port number that will be displayed.

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

Click **Clear All** to clear all the counter information displayed.

L2 Features > LLDP > LLDP Local Port Information

This window is used to display the information on a per port basis currently available for populating outbound LLDP advertisements in the local port brief table shown below.

LLDP Local Port Information

LLDP Local Port Brief Table

Port:

| Port | Port ID Subtype | Port ID | Port Description |
|-------|-----------------|---------|-----------------------------------|
| eth1 | Local | eth1 | D-Link Corporation DXS-1100-16... |
| eth2 | Local | eth2 | D-Link Corporation DXS-1100-16... |
| eth3 | Local | eth3 | D-Link Corporation DXS-1100-16... |
| eth4 | Local | eth4 | D-Link Corporation DXS-1100-16... |
| eth5 | Local | eth5 | D-Link Corporation DXS-1100-16... |
| eth6 | Local | eth6 | D-Link Corporation DXS-1100-16... |
| eth7 | Local | eth7 | D-Link Corporation DXS-1100-16... |
| eth8 | Local | eth8 | D-Link Corporation DXS-1100-16... |
| eth9 | Local | eth9 | D-Link Corporation DXS-1100-16... |
| eth10 | Local | eth10 | D-Link Corporation DXS-1100-16... |
| eth11 | Local | eth11 | D-Link Corporation DXS-1100-16... |
| eth12 | Local | eth12 | D-Link Corporation DXS-1100-16... |
| eth13 | Local | eth13 | D-Link Corporation DXS-1100-16... |
| eth14 | Local | eth14 | D-Link Corporation DXS-1100-16... |
| eth15 | Local | eth15 | D-Link Corporation DXS-1100-16... |
| eth16 | Local | eth16 | D-Link Corporation DXS-1100-16... |

Figure 4.118 – L2 Features > LLDP > LLDP Local Port Information

The fields that can be configured are described below:

Port: Select the port number that will be displayed.

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

Click **Show Detail** to view detailed information of the specific port.

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

LLDP Local Port Information

LLDP Local Information Table

| | |
|---------------------------------|--|
| Port | eth1 |
| Port ID Subtype | Local |
| Port ID | eth1 |
| Port Description | D-Link Corporation DXS-1100-16TC 1.10.003 Port 1 |
| Port PVID | 1 |
| Management Address Count | 2 |
| VLAN Name Entries Count | 1 |
| Protocol Identity Entries Count | 0 |
| MAC/PHY Configuration/Status | Show Detail |
| Link Aggregation | Show Detail |
| Maximum Frame Size | 1536 |
| LLDP-MED Capabilities | Show Detail |
| Network Policy | Show Detail |

Figure 4.119 – L2 Features > LLDP > LLDP Local Port Information (Show Detail)

To view more details about, for example, the **MAC/PHY Configuration/Status**, click the [Show Detail](#) hyperlink.

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

After clicking the [Show Detail](#) hyperlink, a new section will appear at the bottom of the window.



Figure 4.120 – L2 Features > LLDP > LLDP Local Port Information (Show Detail)

L2 Features > LLDP > LLDP Neighbor Port Information

This window is used to display the information learned from the neighbors. The switch receives packets from a remote station but is able to store the information as local.



Figure 4.121 – L2 Features > LLDP > LLDP Neighbor Port Information

Port: Select the port number that will be displayed.

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

Click **Clear** to clear the specific port information.

Click **Clear All** to clear all the port information displayed.

L3 Features > IPv4 Interface

This window is used to configure the IPv4 interface settings.

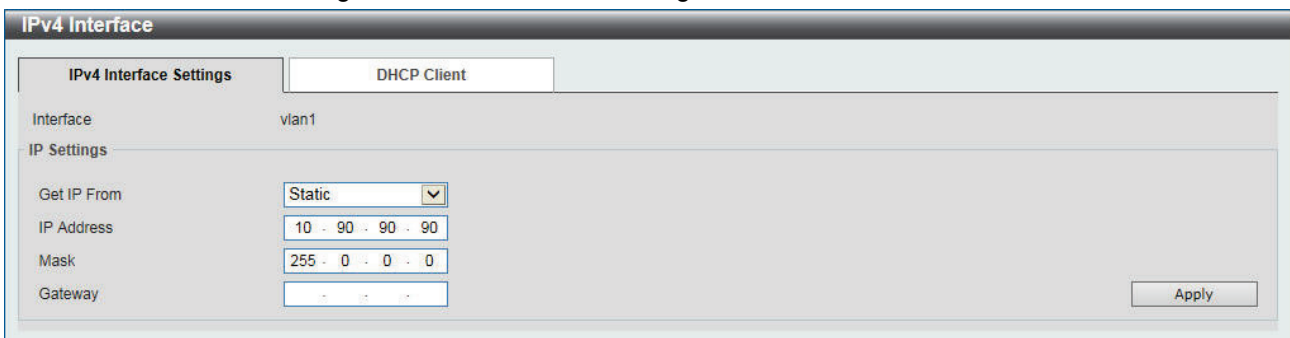


Figure 4.122 – L3 Features > IPV4 Interface (IPv4 Interface Settings)

The fields that can be configured are described below:

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

IP Address: Enter the IPv4 address for this interface here.

Mask: Enter the IPv6 subnet mask for this interface here.

Gateway: Enter the gateway IP address for this interface here.

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

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

The screenshot shows the 'IPv4 Interface Configure' window with the 'DHCP Client' tab selected. The 'DHCP Client Client-ID' is set to '1'. The 'Class ID String' field is set to '32 chars' with a 'Hex' checkbox. The 'Host Name' field is set to '64 chars'. The 'Lease' time is set to '00' Days, '00' Hours, and '00' Minutes. An 'Apply' button is located at the bottom right.

Figure 4.123 – L3 Features > IPV4 Interface (DHCP Client)

The fields that can be configured are described below:

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

Host Name: Enter the host name. The maximum length is 64 characters. The host name must start with a letter, end with a letter or digit, and only with interior characters letters, digits, and hyphens.

Lease: Specify 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 **Apply** to accept the changes made.

L3 Features > IPv6 Interface

This window is used to view and configure the IPv6 interface settings.

The screenshot shows the 'IPv6 Interface' settings window. The 'IPv6 Interface Settings' tab is active. The 'Interface' is 'vlan1' and the 'IPv6 State' is 'Disabled'. The 'Static IPv6 Address Settings' section has an empty 'IPv6 Address' field and checkboxes for 'EUI-64' and 'Link Local'. The 'IPv6 Default Route Settings' section has a 'Next Hop IPv6 Address' of '3FE1::1'. The 'NS Interval Settings' section has an 'NS Interval' of '0' ms. 'Apply' buttons are present for each section.

Figure 4.124 – L3 Features > IPV6 Interface (IPv6 Interface Settings)

The fields that can be configured are described below:

IPv6 State: Select to enable or disable the IPv6 interface's global state here.

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

Next Hop IPv6 Address: Enter the next hop IPv6 address here.

NS Interval: Enter the NS interval between 0 and 3600000 milliseconds.

Click **Apply** to accept the changes made for each individual section.

After clicking the **Interface IPv6 Address** tab, the following page will appear.

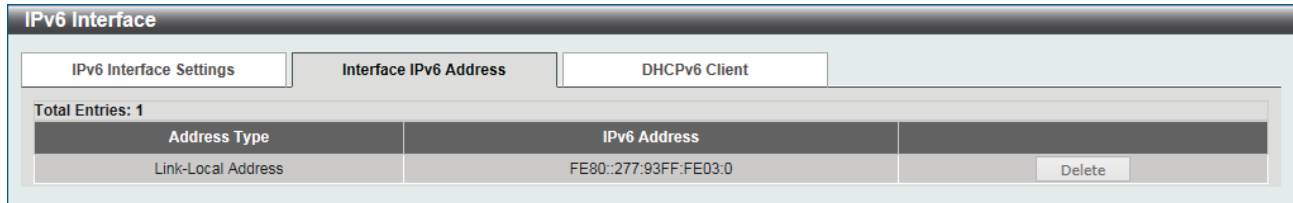


Figure 4.125 – L3 Features > IPV6 Interface (Interface IPv6 Address)

Click **Delete** to delete the specified entry.

After clicking the **DHCPv6 Client** tab, at the top of the page, the following page will be available.

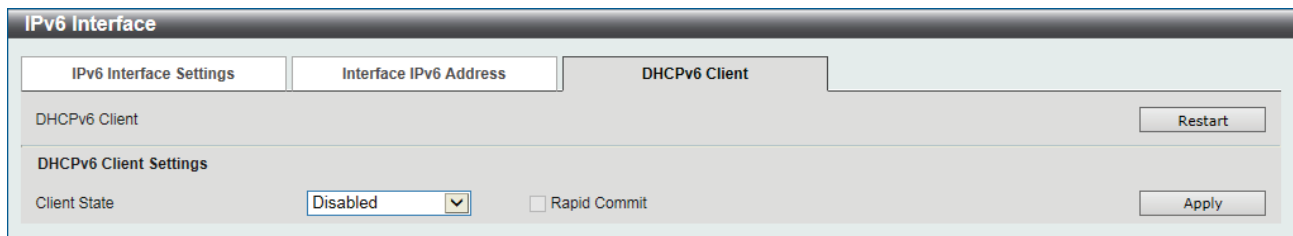


Figure 4.126 – L3 Features > IPV6 Interface (DHCPv6 Client)

The fields that can be configured are described below:

Client State: Select this option to enable or disable the DHCPv6 client state. Tick the Rapid Commit check box to proceed with two-message exchange for prefix delegation.

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

Click **Restart** to restart DHCPv6 client on an interface.

L3 Features > IPv6 Neighbor

This window is used to configure and view the IPv6 neighbor settings.

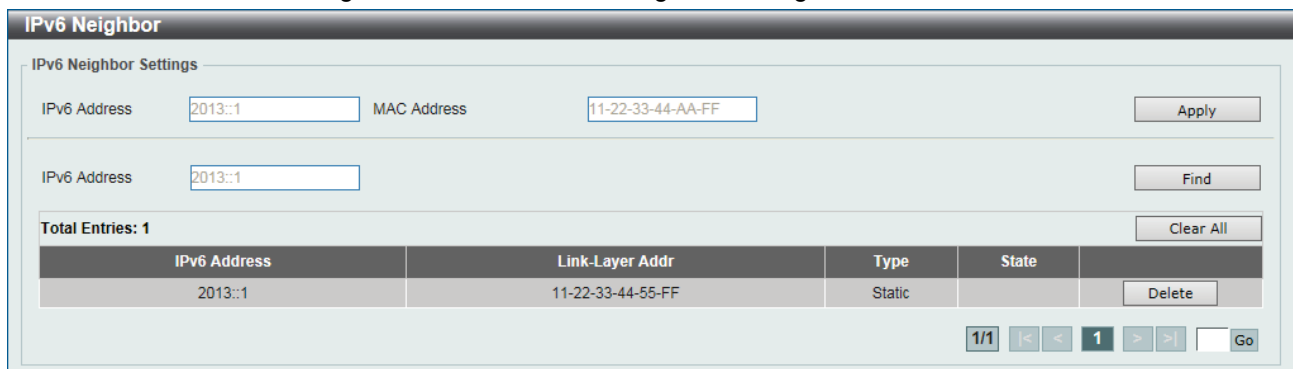


Figure 4.127 – L3 Features > IPV6 Neighbor

The fields that can be configured are described below:

IPv6 Address: Enter the IPv6 address.

MAC Address: Enter the MAC address.

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

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

Click **Clear All** to clear all the information in this table.

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

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

L3 Features > IPv6 Route Table

This window is used to view and configure the IPv6 route table.

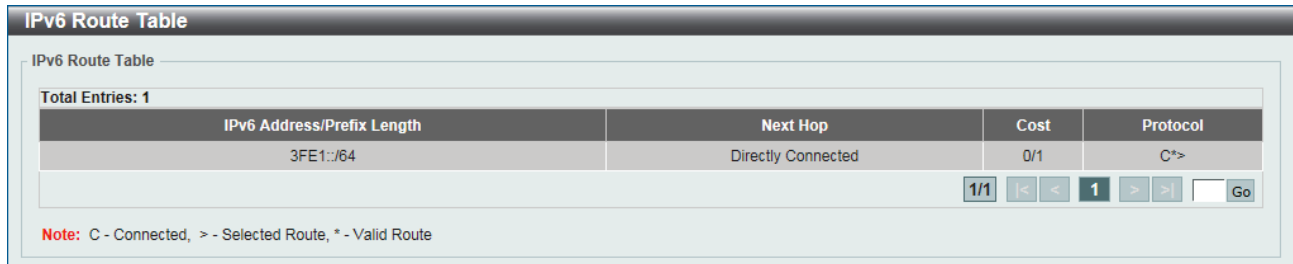


Figure 4.128 – L3 Features > IPV6 Route Table

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

QoS > Basic Settings > Port Default CoS

This window is used to view and configure the port's default CoS settings.

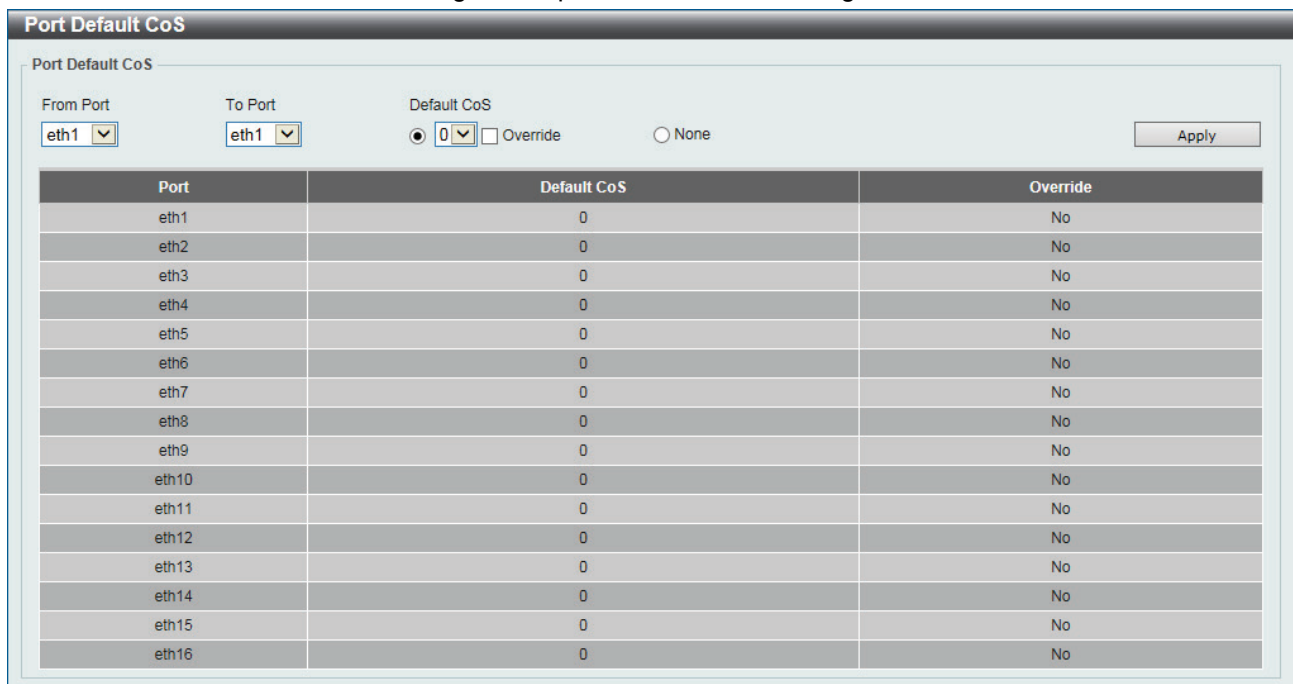


Figure 4.129 – QoS > Basic Settings > Port Default CoS

The fields that can be configured are described below:

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

Default CoS: Select the default CoS option for the port(s) specified here. Options to choose from are **0** to **7**. Select the **Override** option 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 **Apply** to accept the changes made.

QoS > Basic Settings > Port Scheduler Method

This window is used to view and configure the port scheduler method settings.

| Port | Scheduler Method |
|-------|------------------|
| eth1 | WRR |
| eth2 | WRR |
| eth3 | WRR |
| eth4 | WRR |
| eth5 | WRR |
| eth6 | WRR |
| eth7 | WRR |
| eth8 | WRR |
| eth9 | WRR |
| eth10 | WRR |
| eth11 | WRR |
| eth12 | WRR |
| eth13 | WRR |
| eth14 | WRR |
| eth15 | WRR |
| eth16 | WRR |

Figure 4.130 – QoS > Basic Settings > Port Scheduler Method

The fields that can be configured are described below:

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

Scheduler Method: Select the scheduler method that will be applied to the specified port(s). Options to choose from are Strict Priority (**SP**), and Weighted Round-Robin (**WRR**). By default, the output queue scheduling algorithm is **WRR**.

SP - To set a CoS queue in the **SP** mode, any higher priority CoS queue must also be in the strict priority mode.

WRR - **WRR** operates by transmitting permitted packets into the transmit queue in a round robin order. Initially, each queue sets its weight to a configurable weighting. Every time a packet from a higher priority CoS queue is sent, the corresponding weight is subtracted by 1 and the packet in the next lower CoS queue will be serviced. When the weight of a CoS queue reaches zero, the queue will not be serviced until its weight is replenished. When weights of all CoS queues reach 0, the weights get replenished at a time.

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

QoS > Basic Settings > Queue Settings

This window is used to view and configure the queue settings.

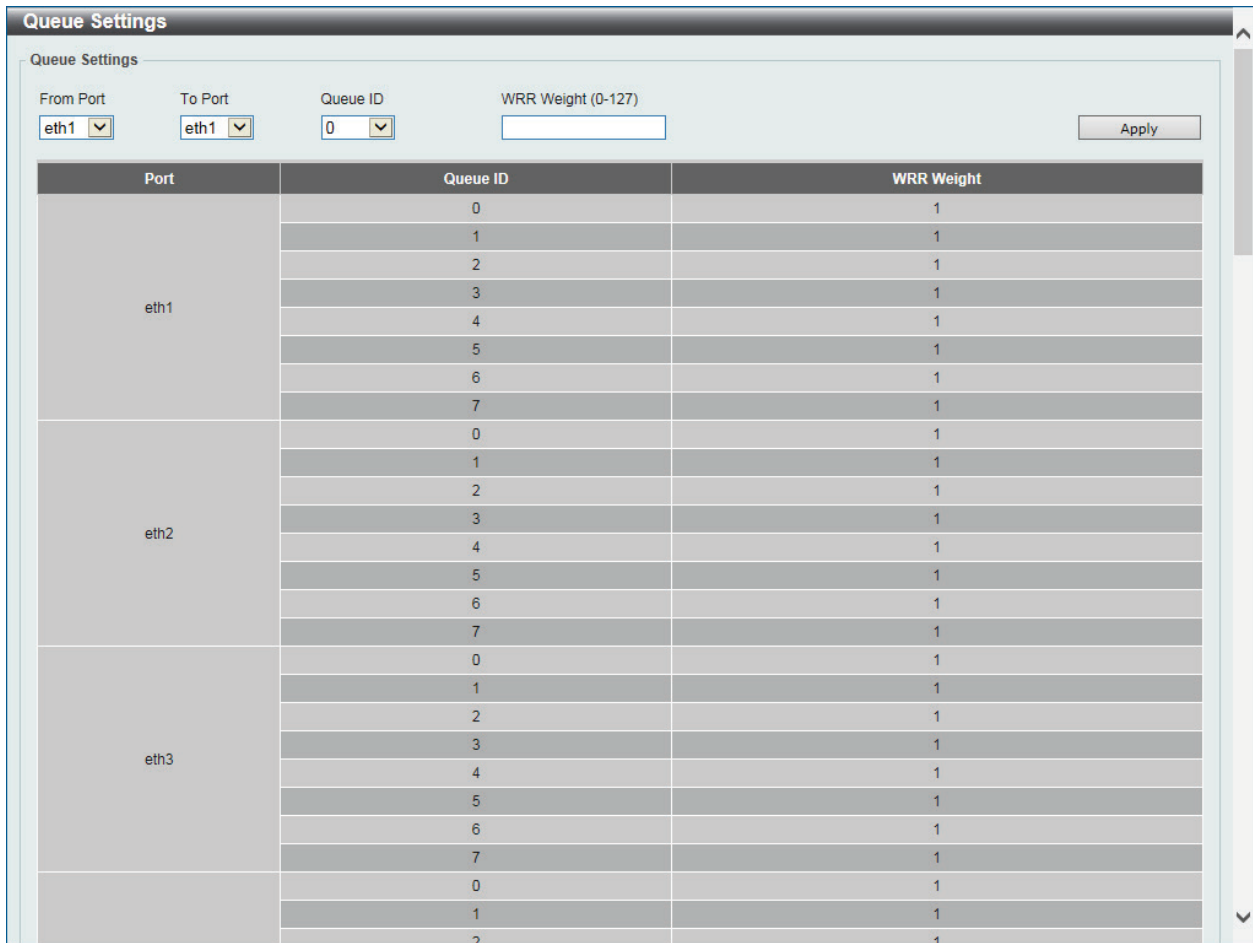


Figure 4.131 – QoS > Basic Settings > Queue Settings

The fields that can be configured are described below:

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

Queue ID: Select the queue ID value here. Options to choose from are 0 to 7.

WRR Weight: Enter the WRR weight value here. This value must be between 0 and 127. To satisfy the behavior requirements of Expedited Forwarding (EF), the highest queue is always selected by the Per-hop Behavior (PHB) EF and the schedule mode of this queue should be strict priority scheduling. So the weight of the last queue should be zero while the Differentiate Service is supported.

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

QoS > Basic Settings > CoS to Queue Mapping

This window is used to view and configure the CoS-to-Queue mapping settings.

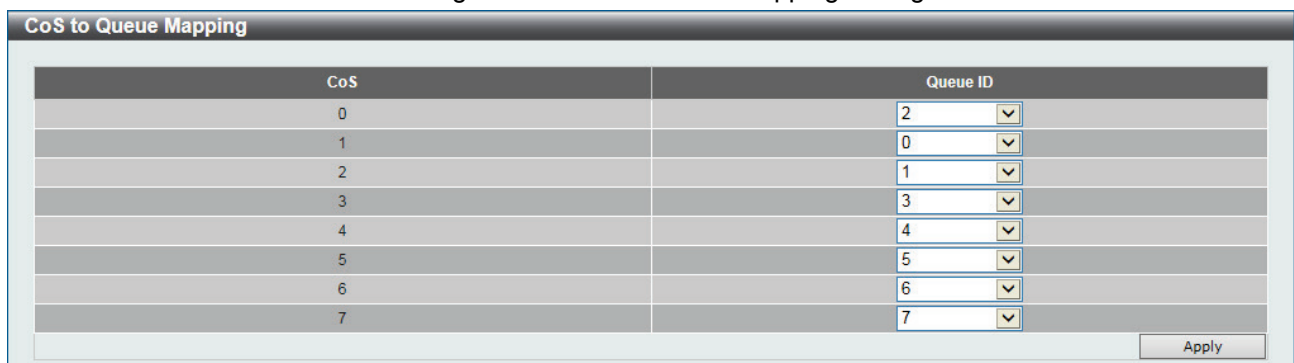


Figure 4.132 – QoS > Basic Settings > CoS to Queue Mapping

The fields that can be configured are described below:

Queue ID: Select the queue ID that will be mapped to the corresponding CoS value. Options to choose from are 0 to 7.

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

QoS > Basic Settings > Port Rate Limiting

This window is used to view and configure the port rate limiting settings.

Port Rate Limiting

Port Rate Limiting

From Port: eth1 | To Port: eth1 | Direction: Input

Rate Limit: Bandwidth (64-10000000) Kbps | Kbps | Burst Size (0-128000) Kbyte

Percent (1-100) % | % | Burst Size (0-128000) Kbyte

None

| Port | Input | | Output | |
|-------|----------|----------|----------|----------|
| | Rate | Burst | Rate | Burst |
| eth1 | No Limit | No Limit | No Limit | No Limit |
| eth2 | No Limit | No Limit | No Limit | No Limit |
| eth3 | No Limit | No Limit | No Limit | No Limit |
| eth4 | No Limit | No Limit | No Limit | No Limit |
| eth5 | No Limit | No Limit | No Limit | No Limit |
| eth6 | No Limit | No Limit | No Limit | No Limit |
| eth7 | No Limit | No Limit | No Limit | No Limit |
| eth8 | No Limit | No Limit | No Limit | No Limit |
| eth9 | No Limit | No Limit | No Limit | No Limit |
| eth10 | No Limit | No Limit | No Limit | No Limit |
| eth11 | No Limit | No Limit | No Limit | No Limit |
| eth12 | No Limit | No Limit | No Limit | No Limit |
| eth13 | No Limit | No Limit | No Limit | No Limit |
| eth14 | No Limit | No Limit | No Limit | No Limit |
| eth15 | No Limit | No Limit | No Limit | No Limit |
| eth16 | No Limit | No Limit | No Limit | No Limit |

Figure 4.133 – QoS > Basic Settings > Port Rate Limiting

The fields that can be configured are described below:

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

Direction: Select the direction option here. Options to choose from 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: Select and enter the rate limit value here.

Bandwidth - Select to 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.

Percent - Select to 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.

None - Select 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 **Apply** to accept the changes made.

QoS > Advanced Settings > Port Trust State

This window is used to view and configure port trust state.

Port Trust State

From Port: eth1 ▼ To Port: eth1 ▼ Trust State: CoS ▼ Apply

| Port | Trust State |
|-------|-------------|
| eth1 | Trust CoS |
| eth2 | Trust CoS |
| eth3 | Trust CoS |
| eth4 | Trust CoS |
| eth5 | Trust CoS |
| eth6 | Trust CoS |
| eth7 | Trust CoS |
| eth8 | Trust CoS |
| eth9 | Trust CoS |
| eth10 | Trust CoS |
| eth11 | Trust CoS |
| eth12 | Trust CoS |
| eth13 | Trust CoS |
| eth14 | Trust CoS |
| eth15 | Trust CoS |
| eth16 | Trust CoS |

Figure 4.134 – QoS > Advanced Settings > Port Trust State

The fields that can be configured are described below:

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

Trust State: Select the port trust state option here. Options to choose from are **CoS** and **DSCP**.

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

QoS > Advanced Settings > DSCP CoS Mapping

DSCP CoS Mapping

DSCP CoS Mapping

From Port: eth1 | To Port: eth1 | CoS: 0 | DSCP List (0-63): | Apply

| Port | CoS | DSCP List |
|------|-----|-----------|
| eth1 | 0 | 0-7 |
| | 1 | 8-15 |
| | 2 | 16-23 |
| | 3 | 24-31 |
| | 4 | 32-39 |
| | 5 | 40-47 |
| | 6 | 48-55 |
| | 7 | 56-63 |
| eth2 | 0 | 0-7 |
| | 1 | 8-15 |
| | 2 | 16-23 |
| | 3 | 24-31 |
| | 4 | 32-39 |
| | 5 | 40-47 |
| | 6 | 48-55 |
| | 7 | 56-63 |
| eth3 | 0 | 0-7 |
| | 1 | 8-15 |
| | 2 | 16-23 |
| | 3 | 24-31 |
| | 4 | 32-39 |
| | 5 | 40-47 |
| | 6 | 48-55 |
| | 7 | 56-63 |

Figure 4.135 – QoS > Advanced Settings > DSCP CoS Mapping

The fields that can be configured are described below:

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

CoS: Select the CoS value. Options to choose from are 0 to 7.

DSCP List: Enter the DSCP list value to map to the CoS value here. This value must be between 0 and 63.

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

Security > Port Security > Port Security Global Settings

This window is used 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.

Port Security Global Settings

Port Security Trap Settings

Trap State: Enabled Disabled | Apply

Port Security Trap Rate Settings

Trap Rate (0-1000): | Apply

Port Security System Settings

System Maximum Address (1-6656): No Limit | Apply

Figure 4.136 – Security > Port Security > Port Security Global Settings

The fields that can be configured are described below:

Trap State: Enable or disable port security traps on the Switch.

Trap Rate: Enter the number of traps per second. The range is from 0 to 1000. The default value 0 indicates an SNMP trap to be generated for every security violation.

System Maximum Address: 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 **No Limit** to allow the maximum number of secure MAC address.

Click **Apply** to accept the changes made for each individual section.

Security > Port Security > Port Security Port Settings

This window is used to view and configure the port security port settings.

| Port | Maximum | Current No. | Violation Action | Violation Count | Security Mode | Admin State | Current State | Aging Time | Aging Type |
|-------|---------|-------------|------------------|-----------------|-------------------|-------------|---------------|------------|------------|
| eth1 | 32 | 0 | Protect | - | Delete-on-Timeout | Disabled | - | 0 | Absolute |
| eth2 | 32 | 0 | Protect | - | Delete-on-Timeout | Disabled | - | 0 | Absolute |
| eth3 | 32 | 0 | Protect | - | Delete-on-Timeout | Disabled | - | 0 | Absolute |
| eth4 | 32 | 0 | Protect | - | Delete-on-Timeout | Disabled | - | 0 | Absolute |
| eth5 | 32 | 0 | Protect | - | Delete-on-Timeout | Disabled | - | 0 | Absolute |
| eth6 | 32 | 0 | Protect | - | Delete-on-Timeout | Disabled | - | 0 | Absolute |
| eth7 | 32 | 0 | Protect | - | Delete-on-Timeout | Disabled | - | 0 | Absolute |
| eth8 | 32 | 0 | Protect | - | Delete-on-Timeout | Disabled | - | 0 | Absolute |
| eth9 | 32 | 0 | Protect | - | Delete-on-Timeout | Disabled | - | 0 | Absolute |
| eth10 | 32 | 0 | Protect | - | Delete-on-Timeout | Disabled | - | 0 | Absolute |
| eth11 | 32 | 0 | Protect | - | Delete-on-Timeout | Disabled | - | 0 | Absolute |
| eth12 | 32 | 0 | Protect | - | Delete-on-Timeout | Disabled | - | 0 | Absolute |
| eth13 | 32 | 0 | Protect | - | Delete-on-Timeout | Disabled | - | 0 | Absolute |
| eth14 | 32 | 0 | Protect | - | Delete-on-Timeout | Disabled | - | 0 | Absolute |
| eth15 | 32 | 0 | Protect | - | Delete-on-Timeout | Disabled | - | 0 | Absolute |
| eth16 | 32 | 0 | Protect | - | Delete-on-Timeout | Disabled | - | 0 | Absolute |

Figure 4.137 – Security > Port Security > Port Security Port Settings

The fields that can be configured are described below:

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

State: Enable or disable the port security feature on the port(s) specified.

Maximum: Enter the maximum number of secure MAC addresses that will be allowed on the port(s) specified. This value must be between 0 and 64. By default, this value is 32.

Violation Action: Select the violation action that will be taken here. Options to choose from are **Protect**, **Restrict**, and **Shutdown**.

Protect - Drop all packets from the insecure hosts at the port-security process level, but does not increment the security-violation count.

Restrict - Drop all packets from the insecure hosts at the port-security process level and increments the security-violation count and record the system log.

Shutdown - Shut down the port if there is a security violation and record the system log.

Security Mode: Select the security mode option here. Options to choose from are **Permanent** and **Delete-on-Timeout**.

Permanent - All learned MAC addresses will not be purged out unless the user manually deletes those entries.

Delete-on-Timeout - All learned MAC addresses will be purged out when an entry is aged out or when the user manually deletes these entries.

Aging Time: Enter the aging time value used for auto-learned dynamic secured addresses on the specified port here. This value must be between 0 and 1440 minutes.

Aging Type: Select the aging type here. Options to choose from are **Absolute** and **Inactivity**.

Absolute - 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.

Inactivity - 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 **Apply** to accept the changes made.

Security > Port Security > Port Security Address Entries

This window is used to view, clear and configure the port security address entries.

Port Security Address Entries

Port Security Address Entries

Port: eth1 MAC Address: 00-84-57-00-00-00 Permanent: VID (1-4094):

Add Delete Clear by Port Clear by MAC

Total Entries: 1 Clear All

| Port | VID | MAC Address | Address Type | Remaining Time (mins) |
|------|-----|-------------------|--------------|-----------------------|
| eth2 | 1 | 00-11-22-33-44-55 | Permanent | - |

1/1 < < 1 > > Go

Figure 4.138 – Security > Port Security > Port Security Address Entries

The fields that can be configured are described below:

Port: Select the port used for the configuration here.

MAC Address: Enter the MAC address here. Tick **Permanent** so that all learned MAC address will not be purged out unless the user manually deletes those entries.

VID: Enter the VLAN ID here. This value must be between 1 and 4094.

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

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

Click **Clear by Port** to clear the information based on the port selected.

Click **Clear by MAC** to clear the information based on the MAC address entered.

Click **Clear All** to clear all the information in this table.

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

Security > ARP Spoofing Prevention

This window is used to view and configure the ARP spoofing prevention settings. When an entry is created, ARP packets whose sender IP address matches the gateway IP address, of an entry, but its sender MAC address field does not match the gateway MAC address, of the entry, will be dropped by the system. The ASP will bypass the ARP packets whose sender IP address doesn't match the configured gateway IP address.

If an ARP address matches a configured gateway's IP address, MAC address, and port list, then bypass the Dynamic ARP Inspection (DAI) check no matter if the receiving port is ARP trusted or untrusted.

ARP Spoofing Prevention

ARP Spoofing Prevention

From Port: eth1

To Port: eth1

Gateway IP: . . .

Gateway MAC: 00-11-22-33-44-aa

Apply

Total Entries: 1

| Gateway IP | Gateway MAC | Port | |
|--------------|-------------------|------|--------|
| 10.90.90.254 | 00-11-22-33-44-55 | eth2 | Delete |

Figure 4.139 – Security > ARP Spoofing Prevention

The fields that can be configured are described below:

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

Gateway IP: Enter the gateway's IP address used here.

Gateway MAC: Enter the gateway's MAC address used here.

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

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

Security > Safeguard Engine Settings

This window is used to view and configure the safeguard engine settings. Periodically, malicious hosts on the network will attack the Switch by utilizing packet flooding (ARP Storm) or other methods. These attacks may increase the switch's CPU load beyond its capability. To alleviate this problem, the Safeguard Engine function was added to the Switch's software.

The Safeguard Engine can help the overall operability of the Switch by minimizing the workload of the Switch while the attack is ongoing, thus making it capable to forward essential packets over its network in a limited bandwidth.

If the CPU load rises above the rising threshold value, the Safeguard Engine function will be activated and the Switch will enter the exhausted mode. In the exhausted mode, the Switch will limit the bandwidth available for ARP and broadcast IP packets. If the CPU load falls below the falling threshold value, the Safeguard Engine will be deactivated and the Switch will exit the exhausted mode and enter the normal mode.

Safeguard Engine Settings

Safeguard Engine Settings

Safeguard Engine State: Disabled

Trap State: Disabled

Safeguard Engine Current Status: Normal

CPU Utilization Settings

Rising Threshold (20% ~ 100%): 70%

Falling Threshold (20% ~ 100%): 20%

Apply

Figure 4.140 – Security > Safeguard Engine Settings

The fields that can be configured are described below:

Safeguard Engine State: Enable or disable the safeguard engine feature here.

Trap State: Select to enable or disable the safeguard engine trap state here.

Rising Threshold: Enter the rising threshold value here. This value must be between 20% and 100%. This value is used to configure the acceptable level of CPU utilization before the Safeguard Engine mechanism is enabled. Once the CPU utilization reaches this percentage level, the Switch will move into Exhausted mode, based on the parameters provided in this window.

Falling Threshold: Enter the falling threshold value here. This value must be between 20% and 100%. This value is used to configure the acceptable level of CPU utilization as a percentage, where the Switch leaves the Safeguard Engine state and returns to normal mode.

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

Security > Traffic Segmentation Settings

This window is used to view and configure the traffic segmentation settings. When the traffic segmentation forwarding domain is specified, packets received by the port will be restricted in Layer 2 packet forwarding to interfaces within the domain. When the forwarding domain of a port is empty, Layer 2 forwarding for packets received by the port is not restricted.

The traffic segmentation member list can be comprised of different interface types, for example port and port-channel in the same forwarding domain. If the interfaces specified by the command include a port-channel, all the member ports of this port-channel will be included in the forwarding domain.

If the forwarding domain of an interface is empty, then there is no restriction on Layer 2 forwarding of packets received by the port.

| Port | Forwarding Domain |
|------|-------------------|
| eth2 | eth3 |

Figure 4.141 – Security > Traffic Segmentation Settings

The fields that can be configured are described below:

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

From Forward Port / To Forward Port: Select the forward port range used for the configuration here.

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

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

Security > Storm Control

This window is used to view and configure the storm control settings.

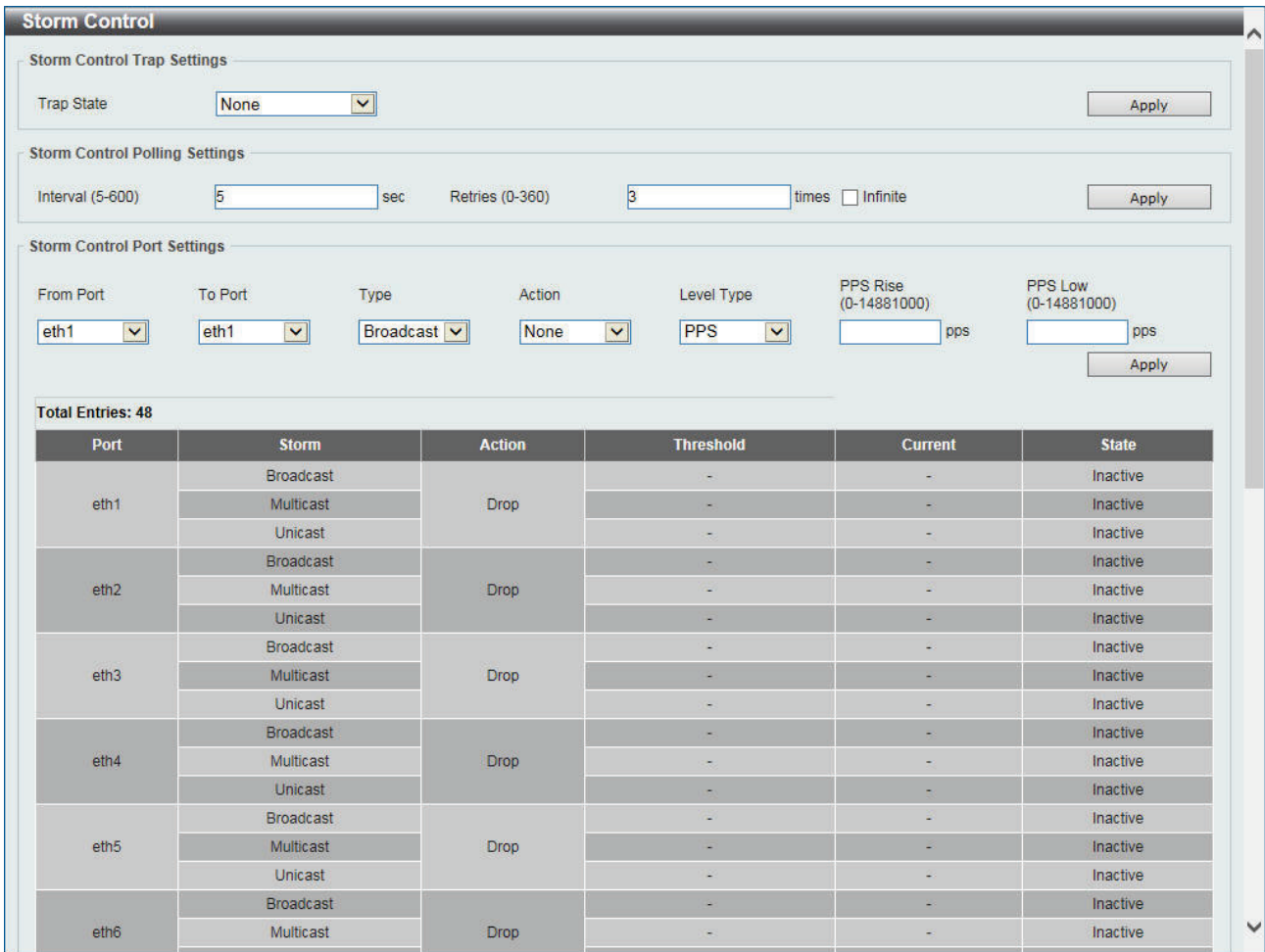


Figure 4.142 – Security > Storm Control

The fields that can be configured are described below:

Trap State: Select the storm control trap option here. Options to choose from are **None**, **Storm Occur**, **Storm Clear**, and **Both**.

None - no traps will be sent.

Storm Occur - A trap notification will be sent when a storm event is detected.

Storm Clear - A trap notification will be sent when a storm event is cleared.

Both - A trap notification will be sent when a storm event is detected or cleared.

Interval: Enter the interval value used here. This value must be between 5 and 600 seconds. By default, this value is 5 seconds.

Retries: Enter the retries value used here. This value must be between 0 and 360. By default, this value is 3. Tick the Infinite option to disable this feature.

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

Type: Select the type of storm attack that will be controlled here. Options to choose from are **Broadcast**, **Multicast**, and **Unicast**. When the action is configured as the shutdown mode, the unicast refers to both known and unknown unicast packets; that is, if the known and unknown unicast packets hit the specified threshold, the port will be shutdown.

Action: Select the action that will be taken here. Options to choose from are **None**, **Shutdown**, and **Drop**.

None - Do not to filter the storm packets.

Shutdown - Shut down the port when the value specified for rise threshold is reached.

Drop - Discard packets that exceed the risen threshold.

Level Type: Select the level type option here. Options to choose from are **PPS** and **Kbps**.

PPS Rise: Enter the rise packets per second value here. This option specifies the rise threshold value in packets count per second. This value must be between 0 and 14881000 packets per second. If the low PPS value is not specified, the default value is 80% of the specified risen PPS.

PPS Low: Enter the low packets per second value here. This option specifies the low threshold value in packets count per second. This value must be between 0 and 14881000 packets per second. If the low PPS value is not specified, the default value is 80% of the specified risen PPS.

Click **Apply** to accept the changes made for each individual section.

After selecting the **Kbps** option as the **Level Type**, the following parameters are available.

Figure 4.143 – Security > Storm Control (Kbps)

The fields that can be configured are described below:

KBPS Rise: Enter the rise KBPS value used here. This option specifies the rise threshold value as a rate of kilobits per second at which traffic is received on the port. This value must be between 0 and 2147483647 Kbps.

KBPS Low: Enter the low KBPS value used here. This option specifies the low threshold value as a rate of kilobits per second at which traffic is received on the port. This value must be between 0 and 2147483647 Kbps. If the low KBPS is not specified, the default value is 80% of the specified risen KBPS.

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

Security > DoS Attack Prevention Settings

This window is used to view and configure the Denial-of-Service (DoS) attack prevention settings. The following well-known DoS types which can be detected by most switches:

- **Land Attack:** This type of attack involves IP packets where the source and destination address are set to the address of the target device. It may cause the target device to reply to itself continuously.
- **Blat Attack:** This type of attack will send packets with the TCP/UDP source port equal to the destination port of the target device. It may cause the target device to respond to itself.
- **TCP-Null:** This type of attack involves port scanning by using specific packets which contain a sequence number of 0 and no flags.
- **TCP-Xmas:** This type of attack involves port scanning by using specific packets which contain a sequence number of 0 and the Urgent (URG), Push (PSH), and FIN flags.
- **TCP SYN-FIN:** This type of attack involves port scanning by using specific packets which contain SYN and FIN flags.
- **TCP SYN SrcPort Less 1024:** This type of attack involves port scanning by using specific packets which contain source port 0 to 1023 and SYN flag.
- **Ping of Death Attack:** A ping of death is a type of attack on a computer that involves sending a malformed or otherwise a malicious ping to a computer. A ping is normally 64 bytes in size (many computers cannot handle a ping larger than the maximum IP packet size) which is 65535 bytes. The sending of a ping of this size can crash the target computer. Traditionally, this bug has been relatively easy to exploit. Generally, sending a 65536 byte ping packet is illegal according to networking protocol, but a packet of such a size can be sent if it is fragmented; when the target computer reassembles the packet, a buffer overflow can occur, which often causes a system crash.
- **TCP Tiny Fragment Attack:** The Tiny TCP Fragment attacker uses IP fragmentation to create extremely small fragments and force the TCP header information into a separate packet fragment to pass through the check function of the router and issue an attack.
- **All Types:** All of above types.

| DoS Type | State | Action |
|---------------------------|----------|--------|
| Land Attack | Disabled | Drop |
| Blat Attack | Disabled | Drop |
| TCP Null | Disabled | Drop |
| TCP Xmas | Disabled | Drop |
| TCP SYN-FIN | Disabled | Drop |
| TCP SYN SrcPort Less 1024 | Disabled | Drop |
| Ping of Death Attack | Disabled | Drop |
| TCP Tiny Fragment Attack | Disabled | Drop |

Figure 4.144 – Security > DoS Attack Prevention Settings

The fields that can be configured are described below:

Trap State: Select to enable or disable the DoS attack prevention trap state here.

DoS Type Selection: Tick the DoS type option that will be prevented here.

State: Enable or disable the DoS attack prevention feature's global state here.

Action: Select the action that will be taken when the DoS attack was detected here. The only option to select here is **Drop**.

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

Security > SSL > SSL Global Settings

Secure Sockets Layer (SSL) is a security feature that will provide a secure communication path between a host and client through the use of authentication, digital signatures and encryption. These security functions are implemented through the use of a cipher suite, which is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session and consists of three levels:

- **Key Exchange:** The first part of the Cipher suite string specifies the public key algorithm to be used. This switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the DHE DSS Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and host as they “exchange keys” in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.
- **Encryption:** The second part of the cipher suite that includes the encryption used for encrypting the messages sent between client and host. The Switch supports two types of cryptology algorithms:
 - **Stream Ciphers** - There are two types of stream ciphers on the Switch, RC4 with 40-bit keys and RC4 with 128-bit keys. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.
 - **CBC Block Ciphers** - CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The Switch supports the 3DES EDE encryption code defined by the Data Encryption Standard (DES) to create the encrypted text and the Advanced Encryption Standard (AES).
- **Hash Algorithm:** This part of the cipher suite allows the user to choose a Message Digest function which will determine a Message Authentication Code. This Message Authentication Code will be encrypted with a sent message to provide integrity and prevent against replay attacks. The Switch

supports three hash algorithms, MD5 (Message Digest 5), SHA (Secure Hash Algorithm), and SHA-256.

These three parameters are uniquely assembled in four choices on the Switch to create a three-layered encryption code for secure communication between the server and the host. The user may implement any one or combination of the cipher suites available, yet different cipher suites will affect the security level and the performance of the secured connection. The information included in the cipher suites is not included with the Switch and requires downloading from a third source in a file form called a certificate. This function of the Switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the Switch by utilizing a TFTP server. The Switch supports SSLv3. Other versions of SSL may not be compatible with this Switch and may cause problems upon authentication and transfer of messages from client to host.

When the SSL function has been enabled, the web will become disabled. To manage the Switch through the web based management while utilizing the SSL function, the web browser must support SSL encryption and the header of the URL must begin with https://. (Ex. https://xx.xx.xx.xx) Any other method will result in an error and no access can be authorized for the web-based management.

Users can download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. Currently, the Switch comes with a certificate pre-loaded though the user may need to download more, depending on user circumstances.

The Switch also supports Transport Layer Security (TLS) versions 1.0, 1.1, and 1.2.

This window is used to view and configure the SSL feature's global settings.

Figure 4.145 – Security > SSL > SSL Global Settings

The fields that can be configured are described below:

SSL Status: Enable or disable the SSL feature's global status here.

Service Policy: Enter the service policy name here. This name can be up to 32 characters long.

File Select: Select the file type that will be loaded here. Options to choose from are **Certificate** and **Private Key**. After selecting the file type, browse to the appropriate file, located on the local computer, by pressing the **Browse** button.

Destination File Name: Enter the destination file name used here. This name can be up to 32 characters long.

Click **Apply** to accept the changes made for each individual section.

Security > SSL > Crypto PKI Trustpoint

This window is used to view and configure the crypto PKI trust point settings.

Crypto PKI Trustpoint

Crypto PKI Trustpoint

Trustpoint

Trustpoint

File System Path Password

TFTP Server Path Type

Total Entries: 1

| Primary | Trustpoint Name | CA | Local Certificate | Local Private Key | |
|--------------------------|-----------------|----|-------------------|-------------------|---------------------------------------|
| <input type="checkbox"/> | Trustpoint | | | | <input type="button" value="Delete"/> |

Figure 4.146 – Security > SSL > Crypto PKI Trustpoint

The fields that can be configured are described below:

Trustpoint: Enter the name of the trust-point that is associated with the imported certificates and key pairs here. This name can be up to 32 characters long.

File System Path: Click and enter the file system path for certificates and key pairs here.

TFTP Server Path: Click and enter the TFTP server's path for certificates and key pairs here.

Password: Enter the encrypted password phrase that is used to undo encryption when the private keys are imported here. The password phrase is a string of up to 64 characters. If the password phrase is not specified, the NULL string will be used.

Type: Select the type of certificate that will be imported here. Options to choose from are **Both**, **CA**, and **Local**. Selecting **Both** specifies to import the CA certificate (*.ca), and local certificate (*.crt) and key (*.prv) pairs. Selecting **CA** specifies to import the CA certificate only. Selecting **Local** specifies to import local certificate and key pairs only.

Click **Apply** to accept the changes made for each individual section.

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

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

Security > SSL > SSL Service Policy

This window is used to view and configure the SSL service policy settings.

SSL Service Policy

SSL Service Policy

Policy Name Apply Find

Policy Name

Version SSL 3.0
 TLS 1.0
 TLS 1.1
 TLS 1.2

Session Cache Timeout (60-86400) sec

Secure Trustpoint

Cipher Suites

DHE_DSS_WITH_3DES_EDE_CBC_SHA
 RSA_WITH_3DES_EDE_CBC_SHA
 RSA_WITH_RC4_128_SHA
 RSA_EXPORT_WITH_RC4_40_MD5
 RSA_WITH_RC4_128_MD5
 RSA_WITH_AES_128_CBC_SHA
 RSA_WITH_AES_256_CBC_SHA
 RSA_WITH_AES_128_CBC_SHA256
 RSA_WITH_AES_256_CBC_SHA256
 DHE_DSS_WITH_AES_256_CBC_SHA
 DHE_RSA_WITH_AES_256_CBC_SHA

Apply

Total Entries: 1

| Policy Name | Version | Cipher Suites | Session Cache Timeout (sec) | Secure Trustpoint | |
|-------------|-------------------------|-------------------------|-----------------------------|-------------------|-------------|
| Policy | SSL 3.0,TLS 1.0,TLS ... | DHE_DSS_WITH_3DES_ED... | 600 | | Edit Delete |

Figure 4.147 – Security > SSL > SSL Service Policy

The fields that can be configured are described below:

Policy Name: Enter the SSL service policy name here. This name can be up to 32 characters long.

Version: Select the SSL or TLS version that will be used here. Options to choose from are **SSL3.0**, **TLS 1.0**, **TLS 1.1**, and **TLS 1.2**.

Session Cache Timeout: Enter the session cache timeout value used here. This value must be between 60 and 86400 seconds. By default, this value is 600 seconds.

Secure Trustpoint: Enter the secure trust point's name here. This name can be up to 32 characters long.

Cipher Suites: Select the cipher suites that will be associated with this profile here.

Click **Apply** to accept the changes made for each individual section.

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

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

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

OAM > Cable Diagnostics

The screenshot shows the 'Cable Diagnostics' interface. At the top, there are two dropdown menus for 'From Port' and 'To Port', both set to 'eth1'. To the right are 'Test' and 'Clear All' buttons. Below is a table with columns: Port, Type, Link Status, Test Result, Cable Length (M), and a 'Clear' button for each row.

| Port | Type | Link Status | Test Result | Cable Length (M) | Clear |
|-------|-----------|-------------|-------------|------------------|-------|
| eth1 | 10GBASE-T | Link Up | - | - | Clear |
| eth2 | 10GBASE-T | Link Down | - | - | Clear |
| eth3 | 10GBASE-T | Link Down | - | - | Clear |
| eth4 | 10GBASE-T | Link Down | - | - | Clear |
| eth5 | 10GBASE-T | Link Down | - | - | Clear |
| eth6 | 10GBASE-T | Link Down | - | - | Clear |
| eth7 | 10GBASE-T | Link Down | - | - | Clear |
| eth8 | 10GBASE-T | Link Down | - | - | Clear |
| eth9 | 10GBASE-T | Link Down | - | - | Clear |
| eth10 | 10GBASE-T | Link Down | - | - | Clear |
| eth11 | 10GBASE-T | Link Down | - | - | Clear |
| eth12 | 10GBASE-T | Link Down | - | - | Clear |
| eth13 | 10GBASE-T | Link Down | - | - | Clear |
| eth14 | 10GBASE-T | Link Down | - | - | Clear |

Figure 4.148 – OAM > Cable Diagnostics

The fields that can be configured are described below:

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

Click **Test** to test the specific port.

Click **Clear All** to clear all the information in this table.

Click **Clear** to clear all the information for the specific port.

Monitoring > Utilization > Port Utilization

This window is used to display the percentage of the total available bandwidth being used on the port.

The screenshot shows the 'Port Utilization' interface. At the top, there are two dropdown menus for 'From Port' and 'To Port', both set to 'eth1'. To the right are 'Find' and 'Refresh' buttons. Below is a table with columns: Port, TX (packets/sec), RX (packets/sec), and Utilization.

| Port | TX (packets/sec) | RX (packets/sec) | Utilization |
|-------|------------------|------------------|-------------|
| eth1 | 5 | 9 | 1 |
| eth2 | 0 | 0 | 0 |
| eth3 | 0 | 0 | 0 |
| eth4 | 0 | 0 | 0 |
| eth5 | 0 | 0 | 0 |
| eth6 | 0 | 0 | 0 |
| eth7 | 0 | 0 | 0 |
| eth8 | 0 | 0 | 0 |
| eth9 | 0 | 0 | 0 |
| eth10 | 0 | 0 | 0 |
| eth11 | 0 | 0 | 0 |
| eth12 | 0 | 0 | 0 |
| eth13 | 0 | 0 | 0 |
| eth14 | 0 | 0 | 0 |
| eth15 | 0 | 0 | 0 |
| eth16 | 0 | 0 | 0 |

Figure 4.149 – Monitoring > Utilization > Port Utilization

The fields that can be configured are described below:

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

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

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

Monitoring > Statistics > Port

This window is used to display the packet statistics of ports.

| Port | RX | | | | TX | | | | |
|-------|-----------|-------------|---------|---------|-----------|-------------|---------|---------|-------------|
| | Rate | | Total | | Rate | | Total | | |
| | bytes/sec | packets/sec | bytes | packets | bytes/sec | packets/sec | bytes | packets | |
| eth1 | 0 | 0 | 5588759 | 44980 | 0 | 0 | 9036195 | 21228 | Show Detail |
| eth2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |
| eth3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |
| eth4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |
| eth5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |
| eth6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |
| eth7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |
| eth8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |
| eth9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |
| eth10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |
| eth11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |
| eth12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |
| eth13 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |
| eth14 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |
| eth15 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |
| eth16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |

Figure 4.150 – Monitoring > Statistics > Port

The fields that can be configured are described below:

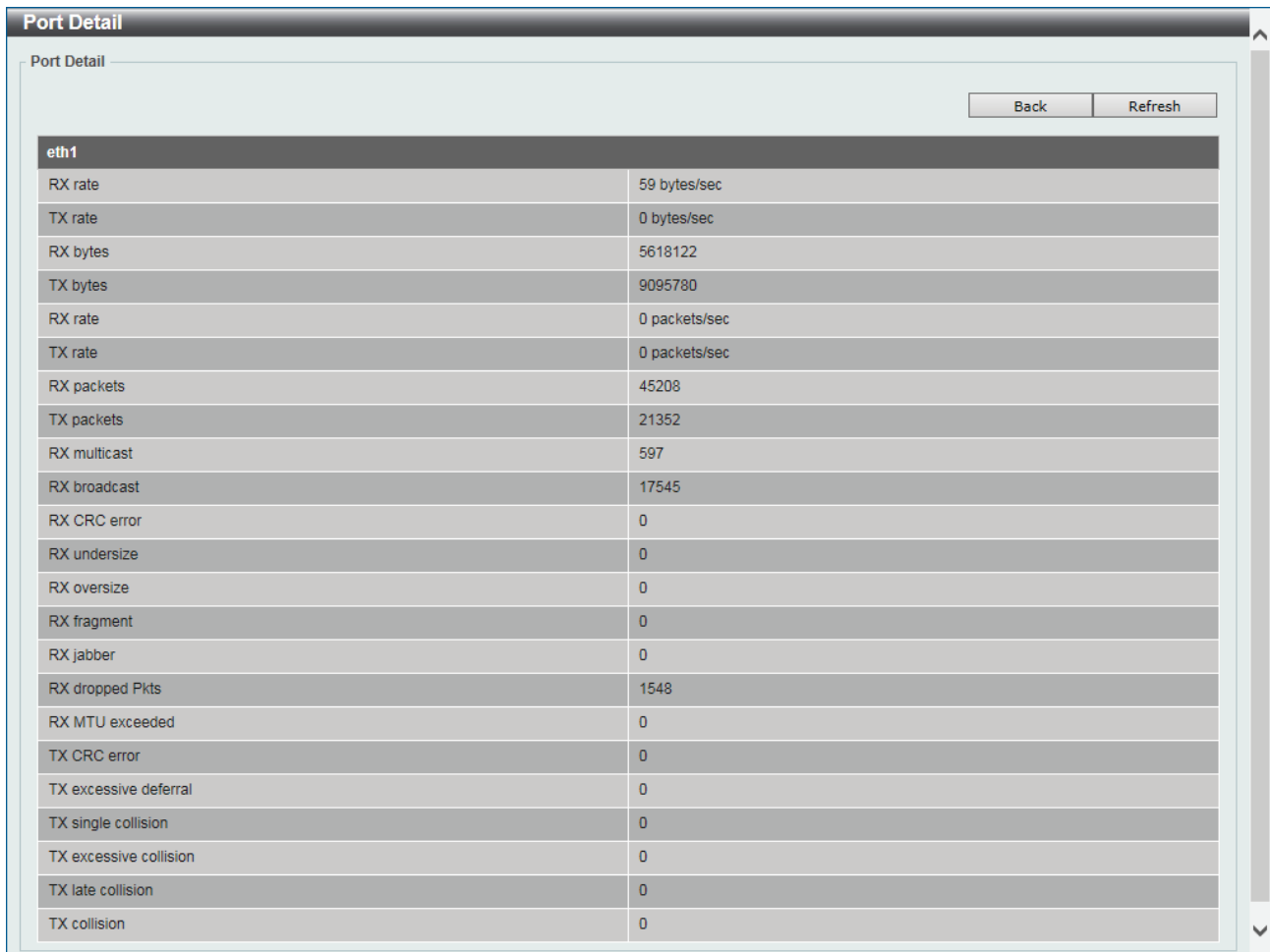
From Port / To Port: Select the appropriate port range used for the configuration here.

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

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

Click **Show Detail** to see the detail information of the specific port.

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



| eth1 | |
|------------------------|---------------|
| RX rate | 59 bytes/sec |
| TX rate | 0 bytes/sec |
| RX bytes | 5618122 |
| TX bytes | 9095780 |
| RX rate | 0 packets/sec |
| TX rate | 0 packets/sec |
| RX packets | 45208 |
| TX packets | 21352 |
| RX multicast | 597 |
| RX broadcast | 17545 |
| RX CRC error | 0 |
| RX undersize | 0 |
| RX oversize | 0 |
| RX fragment | 0 |
| RX jabber | 0 |
| RX dropped Pkts | 1548 |
| RX MTU exceeded | 0 |
| TX CRC error | 0 |
| TX excessive deferral | 0 |
| TX single collision | 0 |
| TX excessive collision | 0 |
| TX late collision | 0 |
| TX collision | 0 |

Figure 4.151 – Monitoring > Statistics > Port Detail

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

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

Monitoring > Statistics > Port Counters

This window is used to display port counter statistics.

| Port | InOctets | InUcastPkts | InMcastPkts | InBcastPkts | OutOctets | OutUcastPkts | OutMcastPkts | OutBcastPkts | Show Errors |
|-------|----------|-------------|-------------|-------------|-----------|--------------|--------------|--------------|-------------|
| eth1 | 5838836 | 28053 | 659 | 18278 | 9397412 | 21337 | 0 | 778 | Show Errors |
| eth2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |
| eth3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |
| eth4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |
| eth5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |
| eth6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |
| eth7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |
| eth8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |
| eth9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |
| eth10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |
| eth11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |
| eth12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |
| eth13 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |
| eth14 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |
| eth15 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |
| eth16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |

Figure 4.152 – Monitoring > Statistics > Port Counters

The fields that can be configured are described below:

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

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

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

Click **Show Errors** to see all error counters of the specific port.

After clicking **Show Errors**, the following page will appear.

| eth1 Counters Errors | |
|----------------------|---|
| Align-Err | 0 |
| Fcs-Err | 0 |
| Rcv-Err | 0 |
| Undersize | 0 |
| Xmit-Err | 0 |
| OutDiscard | 0 |
| Single-Col | 0 |
| Multi-Col | 0 |
| Late-Col | 0 |
| Excess-Col | 0 |
| Carri-Sen | 0 |
| Runts | 0 |
| Giants | 0 |
| Symbol-Err | 0 |
| SQETest-Err | 0 |
| DeferredTx | 0 |
| IntMacTx | 0 |
| IntMacRx | 0 |

Figure 4.153 – Monitoring > Statistics > Counters Errors

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

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

Monitoring > Statistics > Counters

This window is used to display all port counters, and clear the port counters of the specified or all ports.

| Port | linkChange | |
|-------|------------|-------------|
| eth1 | 5 | Show Detail |
| eth2 | 0 | Show Detail |
| eth3 | 0 | Show Detail |
| eth4 | 0 | Show Detail |
| eth5 | 0 | Show Detail |
| eth6 | 0 | Show Detail |
| eth7 | 0 | Show Detail |
| eth8 | 0 | Show Detail |
| eth9 | 0 | Show Detail |
| eth10 | 0 | Show Detail |
| eth11 | 0 | Show Detail |
| eth12 | 0 | Show Detail |
| eth13 | 0 | Show Detail |
| eth14 | 0 | Show Detail |
| eth15 | 0 | Show Detail |
| eth16 | 0 | Show Detail |

Figure 4.154 – Monitoring > Statistics > Counters

The fields that can be configured are described below:

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

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

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

Click **Clear** to clear all the information for the specific ports.

Click **Clear All** to clear all the information in this table.

Click **Show Detail** to see the detail information of the specific port.

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

| eth1 Counters | |
|-------------------------|---------|
| rxHCTotalPkts | 47579 |
| txHCTotalPkts | 22428 |
| rxHCUnicastPkts | 28446 |
| txHCUnicastPkts | 21642 |
| rxHCMulticastPkts | 659 |
| txHCMulticastPkts | 0 |
| rxHCBroadcastPkts | 18474 |
| txHCBroadcastPkts | 786 |
| rxHCOctets | 5914322 |
| txHCOctets | 9538931 |
| rxHCPkt64Octets | 38551 |
| rxHCPkt65to127Octets | 1744 |
| rxHCPkt128to255Octets | 0 |
| rxHCPkt256to511Octets | 6469 |
| rxHCPkt512to1023Octets | 815 |
| rxHCPkt1024to1518Octets | 0 |
| rxHCPkt1519to1522Octets | 0 |
| rxHCPkt1519to2047Octets | 0 |
| rxHCPkt2048to4095Octets | 0 |
| rxHCPkt4096to9216Octets | 0 |
| txHCPkt64Octets | 904 |
| txHCPkt65to127Octets | 790 |
| txHCPkt128to255Octets | 11459 |
| txHCPkt256to511Octets | 4020 |

Figure 4.155 – Monitoring > Statistics > Port Counters Detail

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

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

Monitoring > Mirror Settings

This window is used to view and configure the mirror feature’s settings. The Switch allows users to copy frames transmitted and received on a port and redirect the copies to another port. Attach a monitoring device to the mirroring port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port. This is useful for network monitoring and troubleshooting purposes.

Mirror Settings

Mirror Settings

Session Number: 1

Destination: Port eth1

Source: Port eth1

From Port: eth1 To Port: eth1 Frame Type: Both

Add Delete

Mirror Session Table

| Session Number | Session Type | |
|----------------|---------------|-------------|
| 1 | Local Session | Show Detail |

Figure 4.156 – Monitoring > Mirror Settings

The fields that can be configured are described below:

Session Number: Select the mirror session number for this entry here. This number is 1.

Destination: Tick the checkbox, next to the **Destination** option, to configure the destination for this port mirror entry. In the first drop-down list select the **Port** option. In the second drop-down list select the destination switch’s port number.

Source: Tick the checkbox, next to the Source option, to configure the source for this port mirror entry.

In the first drop-down list select the **Port** option. From the **From Port** drop-down list, select the starting port number and from the **To Port** drop-down list, select the ending port number. Lastly select the **Frame Type** from the corresponding drop-down list. Options to choose from are **Both**, **RX**, and **TX**. When selecting **Both**, traffic in both the incoming and outgoing directions will be mirrored. When selecting **RX**, traffic in only the incoming direction will be mirrored. When selecting **TX**, traffic in only the outgoing direction will be mirrored.

Click **Add** to add the newly configured mirror entry based on the information entered.

Click **Delete** to delete an existing mirror entry based on the information entered.

Click **Show Detail** to see the detail information of the specific session.

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

Mirror Session Detail

Mirror Session Detail

| | |
|------------------|---------------|
| Session Number | 1 |
| Session Type | Local Session |
| Both Port | |
| RX Port | |
| TX Port | |
| Destination Port | eth1 |

Back

Figure 4.157 – Monitoring > Mirror Session Detail

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

Monitoring > Device Environment

The device environment feature displays the Switch internal temperature status.

| Device Environment | |
|--|-------------------------|
| Detail Temperature Status | |
| Temperature Descr/ID | Current/Threshold Range |
| Central Temperature /1 | 22°C/11~79°C |
| Status code: * temperature is out of threshold range | |
| Detail Fan Status | |
| Items | Status |
| Right Fan 1 | (OK) |
| Right Fan 2 | (OK) |
| Detail Power Status | |
| Power Module | Power Status |
| Power 1 | In-operation |

Figure 4.158 – Monitoring > Device Environment

Green > Power Saving

The Power Saving mode feature reduces power consumption automatically when the RJ45 port is link down or the connected devices are turned off. Less power will be consumed also when the short cable is used (less than 10 meters).

| Power Saving | |
|--|---|
| Power Saving Global Settings | Power Saving Shutdown Settings |
| Function Version | 3.00 |
| Link Detection Power Saving | <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled |
| Length Detection Power Saving | <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled |
| Scheduled Port-shutdown Power Saving | <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled |
| Scheduled Hibernation Power Saving | <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled |
| Scheduled Dim-LED Power Saving | <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled |
| <input type="button" value="Apply"/> | |
| Administrative Dim-LED | <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled |
| <input type="button" value="Apply"/> | |
| Time Range Settings | |
| Type | <input type="text" value="Dim-LED"/> <input type="button" value="v"/> |
| Time Range | <input type="text" value="32 chars"/> |
| <input type="button" value="Apply"/> <input type="button" value="Delete"/> | |

Figure 4.159 – Green > Power Saving (Power Saving Global Settings)

The fields that can be configured are described below:

Link Detection Power Saving: Enable or disable the link detection state. When enabled, a port which has a link down status will be turned off to save power to the Switch. This will not affect the port's capabilities when the port status is link up.

Length Detection Power Saving: Enable or disable the length detection state.

Scheduled Port-shutdown Power Saving: Enable or disable applying the power saving by scheduled port shutdown.

Scheduled Hibernation Power Saving: Enable or disable applying the power saving by scheduled hibernation.

Scheduled Dim-LED Power Saving: Enable or disable applying the power saving by scheduled dimming LEDs.

Administrative Dim-LED: Select this option 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: Enter the name of the time range to associate with the power saving type.

Click **Apply** to accept the changes made for each individual section.

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

After clicking the **Power Saving Shutdown Settings** tab, the following page will appear.

Power Saving

Power Saving Global Settings | **Power Saving Shutdown Settings**

From Port: eth1 | To Port: eth1 | Time Range: 32 chars |

| Port | Time Range | |
|-------|------------|---------------------------------------|
| eth1 | | <input type="button" value="Delete"/> |
| eth2 | | <input type="button" value="Delete"/> |
| eth3 | | <input type="button" value="Delete"/> |
| eth4 | | <input type="button" value="Delete"/> |
| eth5 | | <input type="button" value="Delete"/> |
| eth6 | | <input type="button" value="Delete"/> |
| eth7 | | <input type="button" value="Delete"/> |
| eth8 | | <input type="button" value="Delete"/> |
| eth9 | | <input type="button" value="Delete"/> |
| eth10 | | <input type="button" value="Delete"/> |
| eth11 | | <input type="button" value="Delete"/> |
| eth12 | | <input type="button" value="Delete"/> |
| eth13 | | <input type="button" value="Delete"/> |
| eth14 | | <input type="button" value="Delete"/> |
| eth15 | | <input type="button" value="Delete"/> |
| eth16 | | <input type="button" value="Delete"/> |

Figure 4.160 – Green > Power Saving (Power Saving Shutdown Settings)

The fields that can be configured are described below:

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

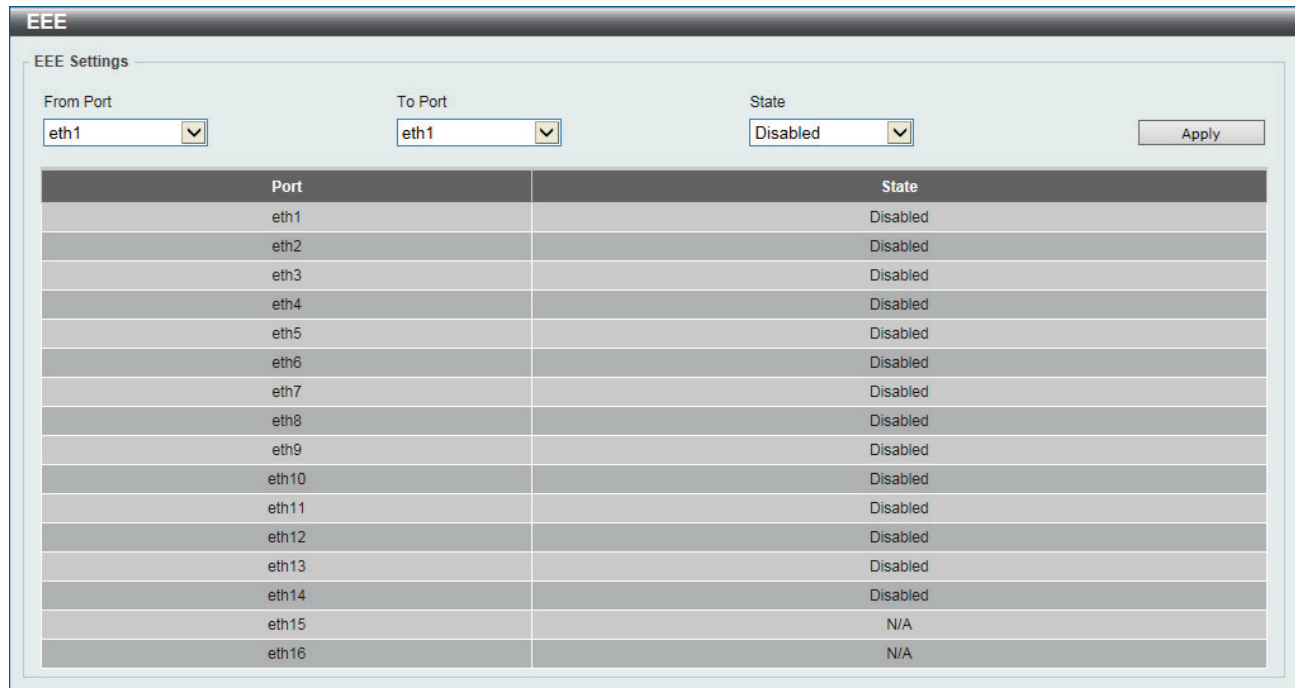
Time Range: Enter the name of the time range to associated with the ports.

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

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

Green > EEE

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.



| Port | State |
|-------|----------|
| eth1 | Disabled |
| eth2 | Disabled |
| eth3 | Disabled |
| eth4 | Disabled |
| eth5 | Disabled |
| eth6 | Disabled |
| eth7 | Disabled |
| eth8 | Disabled |
| eth9 | Disabled |
| eth10 | Disabled |
| eth11 | Disabled |
| eth12 | Disabled |
| eth13 | Disabled |
| eth14 | Disabled |
| eth15 | N/A |
| eth16 | N/A |

Figure 4.161 – Green > EEE

The fields that can be configured are described below:

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

State: Enable or disable the state of this feature here.

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

Appendix A - Technical Specifications

Hardware Specifications

Key Components / Performance

- › Switching Capacity:
 - DXS-1100-10TS: 200 Gbps
 - DXS-1100-16TC: 320 Gbps
- › Max. Forwarding Rate
 - DXS-1100-10TS: 148.801 Mpps
 - DXS-1100-16TC: 238.081 Mpps
- › Forwarding Mode: Store and Forward
- › Packet Buffer memory:
 - DXS-1100-10TS: 2MBytes
 - DXS-1100-16TC: 2MBytes
- › DRAM: 256MBytes
- › Flash Memory: 128MBytes
- › Number of fans:
 - DXS-1100-10TS: 2
 - DXS-1100-16TC: 2
- › Fan start-up speed:
 - DXS-1100-10TS: High speed
 - DXS-1100-16TC: High speed
- › Fan speed adjust to high:
 - DXS-1100-10TS: Rises above 40°C
 - DXS-1100-16TC: Rises above 40°C
- › Fan speed adjust to low:
 - DXS-1100-10TS: Falls below 36°C
 - DXS-1100-16TC: Falls below 36°C

Port Functions

- › 10GBASE-T ports compliant with the following standards:
 - IEEE 802.3u
 - IEEE 802.3ab
 - IEEE 802.3an
 - IEEE 802.3az Energy Efficient Ethernet
 - Supports Full-Duplex operations
 - IEEE 802.3x Flow Control support for Full-Duplex mode
 - Auto MDI/MDIX
- › 10G SFP+ ports compliant with the following standards:
 - IEEE 802.3z
 - IEEE 802.3ae
 - Supports Full-Duplex operations
- › SFP transceivers supported
 - DEM-302S-LX (1000BASE-LX, Single-mode, 2km)
 - DEM-310GT (1000BASE-LX, Single-mode, 10km)
 - DEM-311GT (1000BASE-SX, Multi-mode, 550m)
 - DEM-312GT2 (1000BASE-SX, Multi-mode, 2km)

- DEM-314GT (1000BASE-LHX, Single-mode, 50km)
- DEM-315GT (1000BASE-ZX, Single-mode, 80km)
- DGS-712 (1000BASE-T Copper SFP, 100m)
- › SFP+ transceivers supported
 - DEM-431XT-DD (10GBASE-SR, 80m: OM1 & OM2 MMF, 300m: OM3 MMF)
 - DEM-431XT (10GBASE-SR (w/o DDM), 80m: OM1 & OM2 MMF, 300m: OM3 MMF)
 - DEM-432XT-DD (10GBASE-LR, 10km)
 - DEM-432XT (10GBASE-LR (w/o DDM), 10km)
 - DEM-433XT-DD (10GBASE-ER, 40km)
 - DEM-433XT (10GBASE-ER (w/o DDM), 40km)
 - DEM-434XT (10GBASE-ZR (w/o DDM), 20km, TX: 1270nm, RX: 1330nm)
 - DEM-436XT-BXU (10GBASE-LR BiDi (w/o DDM), 20km, TX: 1270nm, RX: 1330nm)
 - DEM-436XT-BXD (10GBASE-LR BiDi (w/o DDM), 20km, TX: 1330nm, RX: 1270nm)
- › Direct Attached Cables (DAC) with built-in transceivers
 - DEM-CB100S (10G, SFP+ to SFP+, DAC, 1m)
 - DEM-CB300S (10G, SFP+ to SFP+, DAC, 3m)
 - DEM-CB700S (10G, SFP+ to SFP+, DAC, 7m)

Physical & Environment

- › AC input, 100~240 VAC, 50/60Hz, internal universal power supply
- › Operation Temperature: -5~50°C
- › Storage Temperature -40~70°C
- › Operation Humidity: 0%~95% RH
- › Storage Humidity: 0%~95% RH

Emission (EMI) Certifications

- › CE/FCC/C-Tick/VCCI/BSMI Class A

Safety Certifications

- › UL, CB, CE, BSMI Report

Features

L2 Features

- › Supports up to 16K MAC address
- › Supports 512 static MAC
- › Jumbo frame: Supports up to 9K bytes
- › IGMP snooping v1/v2 (v3 awareness):

- Supports 512 IGMP snooping groups (shared with MLD snooping and static group)
- Supports at least 64 static IGMP groups
- › MLD snooping v1 (v2 awareness):
 - Supports 512 MLD snooping groups (shared with IGMP snooping and static group)
 - Supports at least 64 static MLD groups
- › 802.1D Spanning Tree (STP)
- › 802.1w Rapid Spanning Tree (RSTP)
- › Loopback detection
- › 802.1AX/802.3ad link aggregation:
 - DXS-1100-10TS: Supports maximum of 5 groups per device and 4 ports per group
 - DXS-1100-16TC: Supports maximum of 8 groups per device and 8 ports per group
- › Port mirroring
- › LLDP/LLDP-MED
- › L2 multicast filtering

L3 Features

- › IP configuration

VLAN

- › 802.1Q VLAN standard (VLAN tagging)
- › Up to 128 static VLAN groups
- › Asymmetric VLAN
- › Voice VLAN
- › Auto-surveillance VLAN

QoS (Quality of Service)

- › Priority queue mapping by:
 - 802.1p
 - DSCP
- › Up to 8 queues per port
- › Supports strict / WRR mode in queue handling
- › Bandwidth control

Security

- › Authentication for Web management access
- › User account privilege for Web management access
- › Port security: supports 64 MAC addresses per port
- › DoS attack prevention
- › Traffic segmentation
- › D-Link Safeguard engine
- › Storm control
- › ARP spoofing prevention: supports maximum 128 entries

- › SSL: supports v1/v2/v3 (IPv4/IPv6)

OAM

- › Cable diagnostics
- › Reset button (reset to factory default)

Management

- › Web-based graphical user interface
- › D-Link Network Assistant (DNA)
- › SNMP support
- › DHCP/BOOTP client
- › SNMP trap setting for fan and system events
- › Monitoring: Utilization, Statistics, Device Environment
- › LLDP/LLDP-MED
- › Syslog
- › Password encryption
- › Web-based configuration backup / restore
- › Web-based firmware upgrade / backup / restore
- › Flash file system
- › Dual images / Dual configuration
- › SNTP
- › Reset and reboot

D-Link Green Technology

- › D-Link Power Saving Function Version 3.0
 - By Link Status: Drastically save power when the switch port link is down. For example, no PC connection or the connected PC is powered off.
 - By Cable Length: Detects the length of connected RJ45 cables and adjusts power usage accordingly without affecting performance. Once the RJ45 connection is less than 10 meters, the switch will reduce the power instead of full power, which is only needed for 100 meters cables.
 - By LED Shut-off: LEDs can be turned on/off by port or system through schedule.
 - By Port Shut-off: Each port on the system can be turned on/off by schedule.
 - By System Hibernation: System enters hibernation by schedule. In this mode, switches save most power since main chipsets (both MAC and PHY) are disabled for all ports, and energy required to power the CPU is minimal.
 - By Scheduled Time Range: System enters Power Saving mode by schedule.

Appendix B - System Log Entries

The appendix lists all possible entries and their corresponding meanings that will appear in the System Log of the Switch.

Auto Surveillance VLAN

Log Description:

- › Event Description: When a new surveillance device is detected on an interface.
- › Log Message: New surveillance device detected (<interface-id>, MAC: <mac-address>)
- › Parameters Description:
 - interface-id: Interface name.
 - mac-address: Surveillance device MAC address.

Severity: Informational

Log Description:

- › Event Description: When an interface which is enabled surveillance VLAN joins the surveillance VLAN automatically.
- › Log Message: <interface-id> add into surveillance VLAN <vid>
- › Parameters Description:
 - interface-id: Interface name.
 - vid: VLAN ID

Severity: Informational

Log Description:

- › Event Description: When an interface leaves the surveillance VLAN and at the same time, no surveillance device is detected in the aging interval for that interface, the log message will be sent.
- › Log Message: <interface-id> remove from surveillance VLAN <vid>
- › Parameters Description:
 - interface-id: Interface name.
 - vid: VLAN ID

Severity: Informational

Configuration/Firmware

Log Description:

- › Event Description: Firmware upgraded successfully.
- › Log Message: Firmware upgraded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)
- › Parameters Description:
 - session: The user's session.
 - username: Represent current login user.
 - ipaddr: Represent client IP address.
 - macaddr : Represent client MAC address.
 - serverIP: Server IP address.
 - pathFile: Path and file name on server.

Severity: Informational

Log Description:

- › Event Description: Firmware upgraded unsuccessfully.
- › Log Message: Firmware upgraded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)
- › Parameters Description:
 - session: The user's session.
 - username: Represent current login user.
 - ipaddr: Represent client IP address.
 - macaddr : Represent client MAC address.

- serverIP: Server IP address.
- pathFile: Path and file name on server.

Severity: Warning

Log Description:

- › Event Description: Firmware uploaded successfully.
- › Log Message: Firmware uploaded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)
- › Parameters Description:
 - session: The user's session.
 - username: Represent current login user.
 - ipaddr: Represent client IP address.
 - macaddr : Represent client MAC address.
 - serverIP: Server IP address.
 - pathFile: Path and file name on server.

Severity: Informational

Log Description:

- › Event Description: Firmware uploaded unsuccessfully.
- › Log Message: Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)
- › Parameters Description:
 - session: The user's session.
 - username: Represent current login user.
 - ipaddr: Represent client IP address.
 - macaddr : Represent client MAC address.
 - serverIP: Server IP address.
 - pathFile: Path and file name on server.

Severity: Warning

Log Description:

- › Event Description: Configuration downloaded successfully.
- › Log Message: Configuration downloaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)
- › Parameters Description:
 - session: The user's session.
 - username: Represent current login user.
 - ipaddr: Represent client IP address.
 - macaddr : Represent client MAC address.
 - serverIP: Server IP address.
 - pathFile: Path and file name on server.

Severity: Informational

Log Description:

- › Event Description: Configuration downloaded unsuccessfully.
- › Log Message: Configuration downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)
- › Parameters Description:
 - session: The user's session.
 - username: Represent current login user.
 - ipaddr: Represent client IP address.
 - macaddr : Represent client MAC address.
 - serverIP: Server IP address.
 - pathFile: Path and file name on server.

Severity: Warning

Log Description:

- › Event Description: Configuration uploaded successfully.
- › Log Message: Configuration uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)
- › Parameters Description:
 - session: The user's session.
 - username: Represent current login user.
 - ipaddr: Represent client IP address.
 - macaddr : Represent client MAC address.
 - serverIP: Server IP address.
 - pathFile: Path and file name on server.

Severity: Informational

Log Description:

- › Event Description: Configuration uploaded unsuccessfully.
- › Log Message: Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)
- › Parameters Description:
 - session: The user's session.
 - username: Represent current login user.
 - ipaddr: Represent client IP address.
 - macaddr : Represent client MAC address.
 - serverIP: Server IP address.
 - pathFile: Path and file name on server.

Severity: Warning

Log Description:

- › Event Description: Unknown type files downloaded unsuccessfully.
- › Log Message: Downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)
- › Parameters Description:
 - session: The user's session.
 - username: Represent current login user.
 - ipaddr: Represent client IP address.
 - macaddr : Represent client MAC address.
 - serverIP: Server IP address.
 - pathFile: Path and file name on server.

Severity: Warning

DHCPv6 client

Log Description:

- › Event Description: DHCPv6 client interface administrator state changed.
- › Log Message: DHCPv6 client on interface <ipif-name> changed state to [enabled | disabled].
- › Parameters Description:
 - ipif-name: Name of the DHCPv6 client interface.

Severity: Informational

Log Description:

- › Event Description: DHCPv6 client obtains an IPv6 address from a DHCPv6 server.
- › Log Message: DHCPv6 client obtains an IPv6 address <ipv6address> on interface <ipif-name>.
- › Parameters Description:
 - ipv6address: IPv6 address obtained from a DHCPv6 server.
 - ipif-name: Name of the DHCPv6 client interface.

Severity: Informational

Log Description:

- › Event Description: The IPv6 address obtained from a DHCPv6 server starts renewing.

- › Log Message: The IPv6 address <ipv6address> on interface <ipif-name> starts renewing.
- › Parameters Description:
 - ipv6address: IPv6 address obtained from a DHCPv6 server.
 - ipif-name: Name of the DHCPv6 client interface.

Severity: Informational

Log Description:

- › Event Description: The IPv6 address obtained from a DHCPv6 server renews success.
- › Log Message: The IPv6 address <ipv6address> on interface <ipif-name> renews success.
- › Parameters Description:
 - ipv6address: IPv6 address obtained from a DHCPv6 server.
 - ipif-name: Name of the DHCPv6 client interface.

Severity: Informational

Log Description:

- › Event Description: The IPv6 address obtained from a DHCPv6 server starts rebinding.
- › Log Message: The IPv6 address <ipv6address> on interface <ipif-name> starts rebinding.
- › Parameters Description:
 - ipv6address: IPv6 address obtained from a DHCPv6 server.
 - ipif-name: Name of the DHCPv6 client interface.

Severity: Informational

Log Description:

- › Event Description: The IPv6 address obtained from a DHCPv6 server rebinds success.
- › Log Message: The IPv6 address <ipv6address> on interface <ipif-name> rebinds success.
- › Parameters Description:
 - ipv6address: IPv6 address obtained from a DHCPv6 server.
 - ipif-name: Name of the DHCPv6 client interface.

Severity: Informational

Log Description:

- › Event Description: The IPv6 address from a DHCPv6 server was deleted.
- › Log Message: The IPv6 address <ipv6address> on interface <ipif-name> was deleted.
- › Parameters Description:
 - ipv6address: IPv6 address obtained from a DHCPv6 server.
 - ipif-name: Name of the DHCPv6 client interface.

Severity: Informational

DOS Prevention

Log Description:

- › Event Description: Detect DOS attack.
- › Log Message: <dos-type> is dropped from (IP: <ip-address> Port <interface-id>).
- › Parameters Description:
 - dos-type: DOS attack type
 - ip-address: IP address.
 - interface-id: Interface name

Severity: Notice

Interface

Log Description:

- › Event Description: When port is down
- › Log Message: Port <port-type><interface-id> link down
- › Parameters Description:
 - port-type: port type

- interface-id: Interface name

Severity: Informational

Log Description:

- › Event Description: When port is up
- › Log Message: Port <port-type><interface-id> link up, <link-speed>
- › Parameters Description:
 - port-type: port type
 - interface-id: Interface name
 - link-speed: port link speed

Severity: Informational

IPv6 Duplicate Address

Log Description:

- › Event Description: When DUT receives Neighbor Solicitation (NS) message with reduplicated address in the DAD duration.
- › Log Message: Duplicate address <ipv6address> via receiving Neighbor Solicitation Messages
- › Parameters Description:
 - ipv6address: IPv6 address in Neighbor Solicitation Messages.

Severity: Warning

Log Description:

- › Event Description: When DUT receives Neighbor Advertisement (NA) message with reduplicated address in the DAD duration.
- › Log Message: Duplicate address <ipv6address> via receiving Neighbor Advertisement Messages
- › Parameters Description:
 - ipv6address: IPv6 address in Neighbor Advertisement Messages.

Severity: Warning

LACP

Log Description:

- › Event Description: Link Aggregation Group link up.
- › Log Message: Link Aggregation Group <group_id> link up.
- › Parameters Description:
 - group_id: The group ID of the link down aggregation group.

Severity: Informational

Log Description:

- › Event Description: Link Aggregation Group link down.
- › Log Message: Link Aggregation Group <group_id> link down.
- › Parameters Description:
 - group_id: The group ID of the link down aggregation group.

Severity: Informational

Log Description:

- › Event Description: Member port attach to Link Aggregation Group.
- › Log Message: <ifname> attach to Link Aggregation Group <group_id>.
- › Parameters Description:
 - ifname: The interface name of the port that attach to aggregation group.
 - group_id: The group ID of the aggregation group that port attach to.

Severity: Informational

Log Description:

- › Event Description: Member port detach from Link Aggregation Group.
- › Log Message: <iface> detach from Link Aggregation Group <group_id>.
- › Parameters Description:
 - iface: The interface name of the port that detach from aggregation group.
 - group_id: The group ID of the aggregation group that port detach from.

Severity: Informational

LBD

Log Description:

- › Event Description: Record the event when an interface detect loop.
- › Log Message: <interface-id> LBD loop occurred.
- › Parameters Description:
 - interface-id: Interface on which loop is detected.

Severity: Critical

Log Description:

- › Event Description: Record the event when an interface loop recovered.
- › Log Message: <interface-id> LBD loop recovered.
- › Parameters Description:
 - interface-id: Interface on which loop is detected.

Severity: Critical

LLDP(-MED)

Log Description:

- › Event Description: LLDP-MED topology change detected
- › Log Message: LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>)
- › Parameters Description:
 - portNum: The port number.
 - chassisType: chassis ID subtype.
 - Value list:
 - 1. chassisComponent(1)
 - 2. interfaceAlias(2)
 - 3. portComponent(3)
 - 4. macAddress(4)
 - 5. networkAddress(5)
 - 6. interfaceName(6)
 - 7. local(7)
 - chassisID: chassis ID.
 - portType: port ID subtype.
 - Value list:
 - 1. interfaceAlias(1)
 - 2. portComponent(2)
 - 3. macAddress(3)
 - 4. networkAddress(4)
 - 5. interfaceName(5)
 - 6. agentCircuitId(6)
 - 7. local(7)
 - portID: port ID.
 - deviceClass: LLDP-MED device type.

Severity: Notice

Log Description:

- › Event Description: Conflict LLDP-MED device type detected
- › Log Message: Conflict LLDP-MED device type detected (on port <portNum>, chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>)

- › Parameters Description:
 - portNum: The port number.
 - chassisType: chassis ID subtype.
Value list:
 1. chassisComponent(1)
 2. interfaceAlias(2)
 3. portComponent(3)
 4. macAddress(4)
 5. networkAddress(5)
 6. interfaceName(6)
 7. local(7)
 - chassisID: chassis ID.
 - portType: port ID subtype.
Value list:
 1. interfaceAlias(1)
 2. portComponent(2)
 3. macAddress(3)
 4. networkAddress(4)
 5. interfaceName(5)
 6. agentCircuitId(6)
 7. local(7))
 - portID: port ID.
 - deviceClass: LLDP-MED device type.

Severity: Notice

Log Description:

- › Event Description: Incompatible LLDP-MED TLV set detected
- › Log Message: Incompatible LLDP-MED TLV set detected (on port <portNum>, chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>)
- › Parameters Description:
 - portNum: The port number.
 - chassisType: chassis ID subtype.
Value list:
 1. chassisComponent(1)
 2. interfaceAlias(2)
 3. portComponent(3)
 4. macAddress(4)
 5. networkAddress(5)
 6. interfaceName(6)
 7. local(7)
 - chassisID: chassis ID.
 - portType: port ID subtype.
Value list:
 1. interfaceAlias(1)
 2. portComponent(2)
 3. macAddress(3)
 4. networkAddress(4)
 5. interfaceName(5)
 6. agentCircuitId(6)
 7. local(7))
 - portID: port ID.
 - deviceClass: LLDP-MED device type.

Severity: Notice

Peripheral

Log Description:

- › Event Description: Fan Recovered.
- › Log Message: <fan-descr> back to normal.
- › Parameters Description:

- fan-descr: The FAN ID and position.

Severity: Critical

Log Description:

- › Event Description: Fan Fail.
- › Log Message: <fan-descr> failed.
- › Parameters Description:
 - fan-descr: The FAN ID and position.

Severity: Critical

Log Description:

- › Event Description: Temperature sensor enters alarm state.
- › Log Message: <thermal-sensor-descr> detects abnormal temperature <degree>
- › Parameters Description:
 - thermal-sensor-descr: The sensor ID and position.
 - degree: The current temperature.

Severity: Critical

Log Description:

- › Event Description: Temperature recovers to normal.
- › Log Message: <thermal-sensor-descr> temperature back to normal.
- › Parameters Description:
 - thermal-sensor-descr: The sensor ID and position.

Severity: Critical

Port Security

Log Description:

- › Event Description: Address full on a port.
- › Log Message: MAC address <macaddr> causes port security violation on <interface-id>.
- › Parameters Description:
 - macaddr: The violation MAC address.
 - interface-id: The interface name.

Severity: Warning

Log Description:

- › Event Description: Address full on system
- › Log Message: Limit on system entry number has been exceeded.

Severity: Warning

Safeguard

Log Description:

- › Event Description: The host enters the mode of exhausted.
- › Log Message: Safeguard Engine enters EXHAUSTED mode.

Severity: Warning

Log Description:

- › Event Description: The host enters the mode of normal.
- › Log Message: Safeguard Engine enters NORMAL mode.

Severity: Informational

SNMP

Log Description:

- › Event Description: SNMP request received with invalid community string
- › Log Message: SNMP request received from <ipaddr> with invalid community string.
- › Parameters Description:
 - ipaddr: The IP address.

Severity: Informational

Storm Control

Log Description:

- › Event Description: Storm occurrence.
- › Log Message: <Broadcast | Multicast | Unicast> storm is occurring on <interface-id>.
- › Parameters Description:
 - Broadcast: Storm is resulted by broadcast packets(DA = FF:FF:FF:FF:FF:FF).
 - Multicast: Storm is resulted by multicast packets, including unknown L2 multicast, known L2 multicast, unknown IP multicast and known IP multicast.
 - Unicast: Storm is resulted by unicast packets, including both known and unknown unicast packets.
 - interface-id: The interface ID on which a storm is occurring.

Severity: Warning

Log Description:

- › Event Description: Storm cleared.
- › Log Message: <Broadcast | Multicast | Unicast> storm is cleared on <interface-id>.
- › Parameters Description:
 - Broadcast: Broadcast storm is cleared.
 - Multicast: Multicast storm is cleared.
 - Unicast: Unicast storm (including both known and unknown unicast packets) is cleared.
 - interface-id: The interface ID on which a storm is cleared.

Severity: Informational

Log Description:

- › Event Description: Port shut down due to a packet storm.
- › Log Message: <interface-id> is currently shut down due to the <Broadcast | Multicast | Unicast> storm.
- › Parameters Description:
 - interface-id: The interface ID on which is error-disabled by storm.
 - Broadcast: The interface is disabled by broadcast storm.
 - Multicast: The interface is disabled by multicast storm.
 - Unicast: The interface is disabled by unicast storm (including both known and unknown unicast packets).

Severity: Warning

STP Debug Enhancement

Log Description:

- › Event Description: Used to record the event that Spanning Tree Protocol is enabled.
- › Log Message: Spanning Tree Protocol is enabled

Severity: Informational

Log Description:

- › Event Description: Used to record the event that Spanning Tree Protocol is disabled.
- › Log Message: Spanning Tree Protocol is disabled.

Severity: Informational

Log Description:

- › Event Description: Used to record STP topology change event.
- › Log Message: Topology changed (Interface:<interface_id>, MAC:<macaddr>)
- › Parameters Description:
 - interface_id: The port number which detect or receive topochange information.
 - macaddr: The system of bridge mac address.

Severity: Notice**Log Description:**

- › Event Description: Used to record STP new root bridge selected.
- › Log Message: STP New Root bridge selected (MAC: <macaddr> Priority :<priority>)
- › Parameters Description:
 - macaddr: The system of bridge mac address.
 - priority: The bridge priority value must be divisible by 4096

Severity: Informational**Log Description:**

- › Event Description: Used to record STP new root port selected.
- › Log Message: New root port selected (Interface:<interface_id>)
- › Parameters Description:
 - interface_id: The port number which detect or receive topochange information.

Severity: Notice**Log Description:**

- › Event Description: Used to record STP port state change event.
- › Log Message: Spanning Tree port status change (Interface:<interface_id>) <old_status> -> <new_status>
- › Parameters Description:
 - interface_id: The port number which detect or receive topochange information.
 - old_status: The port of STP state. The value may be Disable, Discarding, Learning, Forwarding.
 - new_status: The port of STP state. The value may be Disable, Discarding, Learning, Forwarding.

Severity: Notice**Log Description:**

- › Event Description: Used to record STP port role change event.
- › Log Message: Spanning Tree port role change (Interface:<interface_id>) <old_role> -> <new_role>
- › Parameters Description:
 - interface_id: The port number which detect or receive topochange information.
 - old_role: The port role of STP. The value may be Disable, Alternate, Backup, Root, Designated.
 - new_role: The port role of STP. The value may be Disable, Alternate, Backup, Root, Designated.

Severity: Informational**Log Description:**

- › Event Description: Use to record action to change the STP version.
- › Log Message: Spanning Tree version change (new version : <new_version>)
- › Parameters Description:
 - new_version: Running under which version of STP.

Severity: Informational

System**Log Description:**

- › Event Description: System started up.

- › Log Message: System started up

Severity: Critical

Log Description:

- › Event Description: System warm start
- › Log Message: System warm start

Severity: Critical

Log Description:

- › Event Description: System cold start.
- › Log Message: System cold start

Severity: Critical

Log Description:

- › Event Description: Configuration saved to flash.
- › Log Message: Configuration saved to flash (Username: <username>, IP: <ipaddr>)
- › Parameters Description:
 - username: Represent current login user.
 - ipaddr: Represent client IP address.

Severity: Informational

Log Description:

- › Event Description: Log message successfully uploaded
- › Log Message: Log message uploaded by WEB successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <serverIP>, File Name: <pathFile>)
- › Parameters Description:
 - username: Represent current login user.
 - ipaddr: Represent client IP address.
 - macaddr : Represent client MAC address.
 - serverIP: Server IP address.
 - pathFile: Path and file name on server.

Severity: Informational

Log Description:

- › Event Description: Log message upload was unsuccessful.
- › Log Message: Log message upload by WEB unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <serverIP>, File Name: <pathFile>)
- › Parameters Description:
 - username: Represent current login user.
 - ipaddr: Represent client IP address.
 - macaddr : Represent client MAC address.
 - serverIP: Server IP address.
 - pathFile: Path and file name on server.

Severity: Warning

Voice VLAN

Log Description:

- › Event Description: When a new voice device is detected on an interface.
- › Log Message: New voice device detected (<interface-id>, MAC: <mac-address>)
- › Parameters Description:
 - interface-id: Interface name.
 - mac-address: Voice device MAC address

Severity: Informational

Log Description:

- › Event Description: When an interface which is in auto voice VLAN mode joins the voice VLAN.
- › Log Message: <interface-id> add into voice VLAN <vid>
- › Parameters Description:
 - interface-id: Interface name.
 - vid: VLAN ID

Severity: Informational**Log Description:**

- › Event Description: When an interface leaves the voice VLAN and at the same time, no voice device is detected in the aging interval for that interface, the log message will be sent.
- › Log Message: <interface-id> remove from voice VLAN <vid>
- › Parameters Description:
 - interface-id: Interface name.
 - vid: VLAN ID

Severity: Informational

Web

Log Description:

- › Event Description: Successful login through Web.
- › Log Message: Successful login through Web (Username: <username>, IP: <ipaddr>).
- › Parameters Description:
 - username: The use name that used to login HTTP server.
 - ipaddr: The IP address of HTTP client.

Severity: Informational**Log Description:**

- › Event Description: Login failed through Web.
- › Log Message: Login failed through Web (Username: <username>, IP: <ipaddr>).
- › Parameters Description:
 - username: The use name that used to login HTTP server.
 - ipaddr: The IP address of HTTP client.

Severity: Warning**Log Description:**

- › Event Description: Web session timed out.
- › Log Message: Web session timed out (Username: <username>, IP: <ipaddr>).
- › Parameters Description:
 - username: The use name that used to login HTTP server.
 - ipaddr: The IP address of HTTP client.

Severity: Informational**Log Description:**

- › Event Description: Logout through Web.
- › Log Message: Logout through Web (Username: <username>, IP: <ipaddr>).
- › Parameters Description:
 - username: The use name that used to login HTTP server.
 - ipaddr: The IP address of HTTP client. Informational

Severity: Informational**Log Description:**

- › Event Description: Successful login through Web (SSL)
- › Log Message: Successful login through Informational Web (SSL) (Username: <username>, IP: <ipaddr>).

- Parameters Description:
 - username: The use name that used to login HTTPS server.
 - ipaddr: The IP address of HTTPS client.

Severity: Informational

Log Description:

- Event Description: Login failed through Web (SSL).
- Log Message: Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>).
- Parameters Description:
 - username: The use name that used to login HTTPS server.
 - ipaddr: The IP address of HTTPS client.

Severity: Warning

Log Description:

- Event Description: Web (SSL) session timed out.
- Log Message: Web (SSL) session timed out (Username: <username>, IP: <ipaddr>).
- Parameters Description:
 - username: The use name that used to login HTTPS server.
 - ipaddr: The IP address of HTTPS client.

Severity: Informational

Log Description:

- Event Description: Logout through Web (SSL).
- Log Message: Logout through Web (SSL) (Username: <username>, IP: <ipaddr>).
- Parameters Description:
 - username: The use name that used to login HTTPS server.
 - ipaddr: The IP address of HTTPS client.

Severity: Informational

Appendix C - Trap Entries

The appendix lists all possible trap log entries and their corresponding meanings that will appear in the Switch.

Authentication Fail

Trap Name: authenticationFailure

Description: An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.

OID: 1.3.6.1.6.3.1.1.5.5

DOS Prevention

Trap Name: dDosPreveAttackDetectedPacket

Description: The trap is sent when detect DOS attack.

Binding objects:

- (1) dDoSPrevCtrlAttackType
- (2) dDosPrevNotifInfoDropIpAddr
- (3) dDosPrevNotifInfoDropPortNumber

OID: 1.3.6.1.4.1.171.14.59.0.2

ErrDisable

Trap Name: dErrDisNotifyPortDisabledAssert

Description: The trap is sent when a port enters into error disabled state.

Binding objects:

- (1) dErrDisNotifyInfoPortIfIndex
- (2) dErrDisNotifyInfoReasonID

OID: 1.3.6.1.4.1.171.14.45.0.1

Trap Name: dErrDisNotifyPortDisabledClear

Description: The trap is sent when a port loop restarts after the interval time.

Binding objects:

- (1) dErrDisNotifyInfoPortIfIndex
- (2) dErrDisNotifyInfoReasonID

OID: 1.3.6.1.4.1.171.14.45.0.2

General Management

Trap Name: dGenMgmtLoginFail

Description: This trap is sent when the user login failed to the switch.

Binding objects:

- (1) dGenMgmtNotifyInfoLoginType
- (2) dGenMgmtNotifyInfoUserName

OID: 1.3.6.1.4.1.171.14.165.0.1

LBD

Trap Name: dLbdLoopOccurred

Description: This trap is sent when an interface loop occurs.

Binding objects:

(1) dLbdNotifyInfolIndex

OID: 1.3.6.1.4.1.171.14.46.0.1

Trap Name: dLbdLoopRestart

Description: This trap is sent when an interface loop restarts after the interval time.

Binding objects:

(1) dLbdNotifyInfolIndex

OID: 1.3.6.1.4.1.171.14.46.0.2

LLDP

Trap Name: lldpRemTablesChange

Description: An lldpRemTablesChange notification is sent when the value of lldpStatsRemTableLastChangeTime changes. It can be utilized by an NMS to trigger LLDP remote systems table maintenance polls.

Binding objects:

(1) lldpStatsRemTablesInserts

(2) lldpStatsRemTablesDeletes

(3) lldpStatsRemTablesDrops

(4) lldpStatsRemTablesAgeouts

OID: 1.0.8802.1.1.2.0.0.1

Trap Name: lldpXMedTopologyChangeDetected

Description: A notification generated by the local device sensing a change in the topology that indicates that a new remote device attached to a local port, or a remote device disconnected or moved from one port to another.

Binding objects:

(1) lldpRemChassisIdSubtype

(2) lldpRemChassisId

(3) lldpXMedRemDeviceClass

OID: 1.0.8802.1.1.2.1.5.4795.0.1

MAC-notification

Trap Name: dL2FdbMacNotification

Description: This trap indicates the MAC addresses variation in the address table.

Binding objects:

(1) dL2FdbMacChangeNotifyInfo

OID: 1.3.6.1.4.1.171.14.3.0.1

Peripheral

Trap Name: dEntityExtFanStatusChg

Description: Fan status change notification.

Binding objects:

(1) dEntityExtEnvFanUnitId

(2) dEntityExtEnvFanIndex

(3) dEntityExtEnvFanStatus

OID: 1.3.6.1.4.1.171.14.5.0.1

Port

Trap Name: linkUp**Description:** A notification is generated when port linkup.

Binding objects:

- (1) ifIndex
- (2) if AdminStatus
- (3) ifOperStatus

OID: 1.3.6.1.6.3.1.1.5.4**Trap Name:** linkDown**Description:** A notification is generated when port linkdown.

Binding objects:

- (1) ifIndex
- (2) if AdminStatus
- (3) ifOperStatus

OID: 1.3.6.1.6.3.1.1.5.3**Port Security**

Trap Name: dPortSecMacAddrViolation**Description:** When the port security trap is enabled, new MAC addresses that violate the pre-defined port security configuration will trigger trap messages to be sent out.

Binding objects:

- (1) ifIndex
- (2) dPortSecIfCurrentStatus
- (3) dPortSecIfViolationMacAddress

OID: 1.3.6.1.4.1.171.14.8.0.1**RMON**

Trap Name: risingAlarm**Description:** The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps.

Binding objects:

- (1) alarmIndex
- (2) alarmVariable
- (3) alarmSampleType
- (4) alarmValue
- (5) alarmRisingThreshold

OID: 1.3.6.1.2.1.16.0.1**Trap Name:** fallingAlarm**Description:** The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.

Binding objects:

- (1) alarmIndex
- (2) alarmVariable
- (3) alarmSampleType
- (4) alarmValue
- (5) alarmFallingThreshold

OID: 1.3.6.1.2.1.16.0.2

Safeguard

Trap Name: dSafeguardChgToExhausted

Description: This trap indicates System change operation mode from normal to exhaust.

Binding objects:

(1) dSafeguardEngineCurrentMode

OID: 1.3.6.1.4.1.171.14.19.1.1.0.1

Trap Name: dSafeguardChgToNormal

Description: This trap indicates system change operation mode from exhausted to normal.

Binding objects:

(1) dSafeguardEngineCurrentMode

OID: 1.3.6.1.4.1.171.14.19.1.1.0.2

Start

Trap Name: coldStart

Description: A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.

OID: 1.3.6.1.6.3.1.1.5.1

Trap Name: warmStart

Description: A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.

OID: 1.3.6.1.6.3.1.1.5.2

Storm Control

Trap Name: dStormCtrlOccurred

Description: This trap is sent when dStormCtrlNotifyEnable is 'stormOccurred' or 'both' and a storm is detected.

Binding objects:

(1) ifIndex

(2) dStormCtrlNotifyTrafficType

OID: 1.3.6.1.4.1.171.14.25.0.1

Trap Name: dStormCtrlStormCleared

Description: This trap is sent when dStormCtrlNotifyEnable is 'stormCleared' or 'both' and a storm is cleared.

Binding objects:

(1) ifIndex

(2) dStormCtrlNotifyTrafficType

OID: 1.3.6.1.4.1.171.14.25.0.2

STP

Trap Name: newRoot

Description: The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional.

OID: 1.3.6.1.2.1.17.0.1

Trap Name: topologyChange

Description: A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.

OID: 1.3.6.1.2.1.17.0.2

System File

Trap Name: dsfUploadImage

Description: The notification is sent when the user uploads image file successfully.

OID: 1.3.6.1.4.1.171.14.14.0.1

Trap Name: dsfDownloadImage

Description: The notification is sent when the user downloads image file successfully.

OID: 1.3.6.1.4.1.171.14.14.0.2

Trap Name: dsfUploadCfg

Description: The notification is sent when the user uploads configuration file successfully.

OID: 1.3.6.1.4.1.171.14.14.0.3

Trap Name: dsfDownloadCfg

Description: The notification is sent when the user downloads configuration file successfully.

OID: 1.3.6.1.4.1.171.14.14.0.4

Trap Name: dsfSaveCfg

Description: The notification is sent when the user saves configuration file successfully.

OID: 1.3.6.1.4.1.171.14.14.0.5

D-Link[®]
Building Networks for People