

D-Link[®]
Building Networks for People

DMS-1100 Series

L2 2.5 GIGABIT ETHERNET SWITCH SERIES

Ver. 1.02



Table of Contents

| | |
|--|-----------|
| Table of Contents | i |
| About This Guide | 1 |
| Terms/Usage | 1 |
| Copyright and Trademarks | 1 |
| 1 Product Introduction | 2 |
| DMS-1100-10TS | 3 |
| Front Panel | 3 |
| Rear Panel | 3 |
| DMS-1100-10TP | 4 |
| Front Panel | 4 |
| Rear Panel | 4 |
| DMS-1100 LED Indicators | 5 |
| 2 Hardware Installation | 7 |
| Safety Cautions | 7 |
| Step 1: Unpacking | 8 |
| Step 2: Switch Installation | 8 |
| Desktop or Shelf Installation | 8 |
| Rack Installation | 9 |
| Step 3 – Plugging in the AC Power Cord with Power Cord Clip | 9 |
| Power Failure | 12 |
| Grounding the Switch | 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 |
| 4 Configuration | 15 |
| Smart Wizard Configuration | 15 |
| IPv4 Information | 15 |
| SNMP Settings | 16 |
| User Accounts Settings | 16 |
| Web-based Management | 17 |
| Tool Bar > Save Menu | 18 |
| Save Configuration | 18 |
| Tool Bar > Tool Menu | 19 |
| Firmware Information | 19 |
| Configuration Information | 19 |
| Firmware Upgrade & Backup > Firmware Upgrade from HTTP | 19 |
| Firmware Upgrade & Backup > Firmware Upgrade from TFTP | 20 |
| Firmware Backup to HTTP & Backup > Firmware Backup to HTTP | 20 |
| Firmware Backup to HTTP & Backup > Firmware Backup to TFTP | 21 |
| Configuration Upgrade & Backup > Configuration Restore from HTTP | 21 |
| Configuration Upgrade & Backup > Configuration Restore from TFTP | 22 |
| Configuration Upgrade & Backup > Configuration Backup to HTTP | 22 |

| | |
|---|----|
| Configuration Upgrade & Backup > Configuration Backup to TFTP | 22 |
| Log Backup > Log Backup to HTTP | 23 |
| Log Backup > Log Backup to TFTP | 23 |
| Ping | 23 |
| Reset | 24 |
| Reboot System | 24 |
| Tool Bar > Smart Wizard..... | 25 |
| Tool Bar > Online Help..... | 25 |
| Function Tree | 27 |
| Device Information..... | 27 |
| System > System Information | 27 |
| System > Port Configuration > Port Settings | 28 |
| System > Port Configuration > Port Status | 29 |
| System > Port Configuration > Error Disable Settings | 29 |
| System > Port Configuration > Jumbo Frame..... | 30 |
| System > PoE > PoE System (DMS-1100-10TP only) | 31 |
| System > PoE > PoE Status (DMS-1100-10TP only) | 32 |
| System > PoE > PoE Configuration (DMS-1100-10TP only) | 32 |
| System > PoE > PoE Measurement (DMS-1100-10TP only) | 33 |
| System > System Log > System Log Settings | 33 |
| System > System Log > System Log Server Settings | 34 |
| System > System Log > System Log | 35 |
| System > Time and SNTP > Clock Settings | 35 |
| System > Time and SNTP > Time Zone Settings | 35 |
| System > Time and SNTP > SNTP Settings..... | 37 |
| Management > User Accounts Settings..... | 38 |
| Management > Password Encryption | 39 |
| Management > SNMP > SNMP Global Settings..... | 39 |
| Management > SNMP > SNMP View Table Settings | 40 |
| Management > SNMP > SNMP Community Table Settings | 41 |
| Management > SNMP > SNMP Group Table Settings | 42 |
| Management > SNMP > SNMP Engine ID Local Settings..... | 43 |
| Management > SNMP > SNMP User Table Settings..... | 43 |
| Management > SNMP > SNMP Host Table Settings..... | 45 |
| Management > Web | 45 |
| Management > Session Timeout | 46 |
| Management > D-Link Discover Protocol Settings..... | 46 |
| L2 Features > FDB > Static FDB > Unicast Static FDB | 47 |
| L2 Features > FDB > Static FDB > Multicast Static FDB..... | 48 |
| L2 Features > FDB > MAC Address Table Settings | 49 |
| L2 Features > FDB > MAC Address Table | 50 |
| L2 Features > 802.1Q VLAN | 50 |
| L2 Features > Asymmetric VLAN..... | 51 |
| L2 Features > VLAN Interface..... | 51 |
| L2 Features > Auto Surveillance VLAN > Auto Surveillance Properties..... | 53 |
| L2 Features > Auto Surveillance VLAN > MAC Settings and Surveillance Device | 54 |
| L2 Features > Voice VLAN > Voice VLAN Global..... | 55 |
| L2 Features > Voice VLAN > Voice VLAN Port | 55 |
| L2 Features > Voice VLAN > Voice VLAN OUI..... | 56 |

| | |
|--|-----|
| L2 Features > Voice VLAN > Voice VLAN Device | 57 |
| L2 Features > Voice VLAN > Voice VLAN LLDP-MED Device..... | 57 |
| L2 Features > STP > STP Global Settings | 57 |
| L2 Features > STP > STP Port Settings | 59 |
| L2 Features > STP > MST Configuration Identification..... | 61 |
| L2 Features > STP > STP Instance | 62 |
| L2 Features > STP > MSTP Port Information | 62 |
| L2 Features > ERPS(G.8032) > ERPS | 63 |
| L2 Features > ERPS(G.8032) > ERPS Profile | 65 |
| L2 Features > Loopback Detection | 66 |
| L2 Features > Link Aggregation | 67 |
| L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings..... | 69 |
| L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Groups Settings | 71 |
| L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Mrouter Settings | 72 |
| L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Statistics Settings | 72 |
| L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Setting..... | 73 |
| 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 > LLDP > LLDP Global Settings | 78 |
| L2 Features > LLDP > LLDP Port Settings | 79 |
| 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 | 84 |
| L2 Features > LLDP > LLDP Statistics Information | 84 |
| L2 Features > LLDP > LLDP Local Port Information..... | 86 |
| L2 Features > LLDP > LLDP Neighbor Port Information..... | 87 |
| L3 Features > IPv4 Interface | 87 |
| L3 Features > IPv4 Default Gateway | 89 |
| L3 Features > IPv6 Interface | 89 |
| L3 Features > IPv6 Default Gateway | 90 |
| QoS > Port Default CoS | 91 |
| QoS > Port Scheduler Method | 91 |
| QoS > Queue Settings | 92 |
| QoS > CoS to Queue Mapping | 93 |
| QoS > Port Rate Limiting..... | 93 |
| Security > Safeguard Engine..... | 94 |
| Security > Trusted Host..... | 94 |
| Security > Traffic Segmentation Settings | 95 |
| Security > Storm Control Settings | 95 |
| Security > DoS Attack Prevention Settings | 97 |
| Security > SSL > SSL Global Setting | 97 |
| Security > SSL > SSL Service Policy | 98 |
| OAM > Cable Diagnostics | 99 |
| Monitoring > Statistics > Port | 99 |
| Monitoring > Statistics > Port Counters..... | 100 |
| Monitoring > Statistics > Counters | 102 |

| | |
|--|------------|
| Monitoring > Mirror Settings | 103 |
| Green > Power Saving | 104 |
| Green > EEE | 104 |
| Appendix A - Technical Specifications | 106 |
| Hardware Specifications | 106 |
| Features | 108 |
| L2 Features | 108 |
| L3 Features | 108 |
| VLAN | 108 |
| QoS (Quality of Service)..... | 108 |
| Security..... | 108 |
| OAM | 108 |
| Management..... | 108 |
| D-Link Green Technology | 108 |
| Appendix B – Rack mount Instructions | 109 |

About This Guide

This guide provides installation and instructions for the D-Link 2.5 Gigabit Ethernet L2 Switch (DMS-1100-10TS and DMS-1100-10TP).



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

This guide is divided into four parts:

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

Terms/Usage

In this guide, the term “Switch” (first letter capitalized) refers to the DMS-1100 Series switch and “switch” (first letter lower case) refers to other Ethernet switches. Some technologies use “switch”, “bridge” and “switching hubs” interchangeably, and all are commonly accepted terms for Ethernet switches.



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



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

Copyright and Trademarks

Information in this document is subjected to change without notice.

© 2017 D-Link Corporation. All rights reserved.

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

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

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

1 Product Introduction

Thank you and congratulations on your purchase of D-Link DMS-1100 Series Switch.

D-Link's latest generation L2 2.5 Gigabit Ethernet switch series blends plug-and-play simplicity with exceptional value and reliability for small and medium-sized business (SMB) networking. All models are housed in a new style rack-mount metal case with easy-to-view front panel diagnostic LEDs, and provide advance features including network security, traffic segmentation, QoS and versatile management.

Flexible Port Configurations: The DMS-1100 Series is D-Link's latest 2.5G switch which provides 8-port 2.5GBASE-T plus 2 SFP+ models. The DMS-1100 Series switches, have the advantage of using intuitive feature-rich software and utilizing a neat and simplified Web GUI allowing users to access and configure the Switch from everywhere via a web browser. 2.5GBASE-T provides the requisite backward compatibility that allows end users to transparently upgrade from 100/1000Mbps to 2.5 Gbps, using Cat 5e, unshielded and shielded twisted-pair cables. 10G SFP+ has the advantage of lower power consumption, longer cable distance, and better latency performance. Direct Attach Cables (DACs) can be used to provide a cost effective way of connecting switches at 10 Gbps that are in close proximity to each other.

D-Link Green Technology: D-Link Green devices aim to provide eco-friendly alternatives without compromising performance. D-Link Green Technology includes a number of innovations to reduce energy consumption on DMS-1100 series switches, such as reducing power when a port does not have a device attached, or adjusting the power usage according to the length of 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, ERPS, 802.3ad LACP, SNTP, LLDP and Loopback Detection to enhance performance and network reliability.

QoS: The switches support bandwidth control and 802.1p priority queues, enabling users to run bandwidth-sensitive applications such as voice and video on the network. These functions allow the switches to work seamlessly with VLANs, 802.1p traffic and IPv6 Traffic Class priority to prioritize traffic on the network.

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

Versatile Management: The new generation of D-Link 2.5 Gigabit Ethernet Switches provide growing businesses with a simple and easy management of their network, using a web-based management interface that allows administrators to remotely control their network down to the port level. Alternatively, the Switch can also be managed, in-band, by using a Telnet connection to any of the LAN ports on the Switch.

Users can also access the switch via Telnet. Some basic tasks can be performed such as changing the Switch IP address, resetting the settings to factory defaults, setting the administrator password and rebooting 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. D-Link Smart Managed Switches provides easy-to-use graphic interface and facilitates the operation efficiency.

DMS-1100-10TS

8-Port 2.5GBASE-T and 2-Port 10G SFP+ Smart Managed Switch.

Front Panel

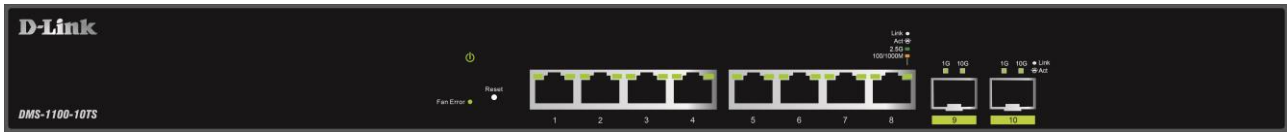



Figure 1.1 – DMS-1100-10TS Front Panel

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

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

Reset: Press the Reset button for 1~5 seconds to reboot the device. Press the Reset button for 6~10 seconds to reset the Switch back to the default settings and led will be solid light with amber for 2 seconds. Or press the Reset button over 11 seconds to enter the loader mode after device reboot and the led will be solid light with green for 2 seconds. If the device cannot reboot the Switch, the device will enter the loader mode automatically.

Port Link/Act/Speed LED (1-8): The port LEDs indicate a network link through the corresponding port. Blinking indicates the Switch is either sending or receiving data to the port. When the port LED glows amber, it indicates the port is running at 100 Mbps or 1000 Mbps. When the port LED glows green, it is running at 2.5 Gbps.

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



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

Rear Panel



Figure 1.2 – DMS-1100-10TS Rear Panel

Power: Connect the AC power cord to this port.


DMS-1100-10TP

8-port 2.5GBASE-T PoE+ and 2-port 10G SFP+ Smart Managed Switch.

Front Panel



Figure 1.3 – DMS-1100-10TP Front Panel

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

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

Reset: Press the Reset button for 1~5 seconds to reboot the device. Press the Reset button for 6~10 seconds to reset the Switch back to the default settings and led will be solid light with amber for 2 seconds. Or press the Reset button over 11 seconds to enter the loader mode after device reboot and the led will be solid light with green for 2 seconds. If the device cannot reboot the Switch, the device will enter the loader mode automatically.

PoE OK/FAIL: The PoE LED shows the status of the PoE ports, the green light (OK) indicates that PoE work fine and the amber light (Fail) indicate that the PoE is working abnormally.

Port Link/Act/Speed LED (1-8): The port LEDs indicate a network link through the corresponding port. Blinking indicates the Switch is either sending or receiving data to the port. When the port LED glows amber, it indicates the port is running at 100 Mbps or 1000 Mbps. When the port LED glows green, it is running at 2.5 Gbps.

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



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

Rear Panel



Figure 1.4 – DMS-1100-10TP Rear Panel

Power: Connect the AC power cord to this port.

DMS-1100 LED Indicators

The Switch supports LED indicators for Power, Fan Error, PoE OK/Fail and Link/Act for each port. The following shows the LED indicators for the DMS-1100 series Smart Managed Switch along with an explanation of each indicator.



Figure 1.5 –LED Indicators on DMS-1100 series

| Location | LED Indicative | Color | Status | Description |
|---------------------------------------|----------------|-------------|----------------|---|
| Per Device | Power | Green | Solid Light | Power on. |
| | | | Light off | Power off. |
| | Fan Error | Red | Solid light | The fan has runtime failure and is brought offline. |
| LED Per 2.5GBASE-T Port | Link/Act/Speed | Green/Amber | Solid Green | When there is a secure 2.5Gbps connection (or link) at any of the ports. |
| | | | Blinking Green | When there is reception or transmission (i.e. Activity—Act) of data occurring at any of the ports. |
| | | | Solid Amber | When there is a secure 100/1000Mbps Ethernet connection (or link) at any of the ports. |
| | | | Blinking Amber | When there is reception or transmission (i.e. Activity—Act) of data occurring at any of the port. |
| | | | Light off | No link. |
| LED Per SFP+ Port | Link/Act/Speed | Green/Amber | Solid Green | When there is a secure 10Gbps connection (or link) at any of the ports. |
| | | | Blinking Green | When there is reception or transmission (i.e. Activity—Act) of data occurring at any of the ports. |
| | | | Solid Amber | When there is a secure 1000Mbps Ethernet connection (or link) at any of the ports. |
| | | | Blinking Amber | When there is reception or transmission (i.e. Activity—Act) of data occurring at any of the port. |
| | | | Light off | No link. |
| LED Per PoE Port (DMS-1100-10TP only) | PoE Status | Green/Amber | Solid Green | PD device insert and power feeding. |
| | | | Solid Amber | PD device insert but failure occurs. (PSE can't provide power to PD due to PD error or power budget is not enough.) |

| | | | | |
|--|--|--|-----------|----------------------|
| | | | Light off | No PD device insert. |
|--|--|--|-----------|----------------------|

2 *Hardware Installation*

This chapter provides unpacking and installation information for the D-Link DMS-1100 Series Switch.

Safety Cautions

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

- Observe and follow service markings.
 - Do not service any product except as explained in your system documentation.
 - Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose you to electrical shock.
- Only a trained service technician should service components inside these compartments.
- If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your trained service provider:
 - The power cable, extension cable, or plug is damaged.
 - An object has fallen into the product.
 - The product has been exposed to water.
 - The product has been dropped or damaged.
 - The product does not operate correctly when you follow the operating instructions.
- Keep your system away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the system gets wet, contact your trained service provider.
- Do not push any objects into the openings of your system. Doing so can cause fire or electric shock by shorting out interior components.
- Use the product only with approved equipment.
- Allow the product to cool before removing covers or touching internal components.
- Operate the product only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local reseller.
- Also, be sure that attached devices are electrically rated to operate with the power available in your location.
- Use only approved power cable(s). If you have not been provided with a power cable for your system or for any AC powered option intended for your system, purchase a power cable that is approved for use in your country. The power cable must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.
- To help prevent electric shock, plug the system and peripheral power cables into properly grounded electrical outlets.
- These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a 3-wire cable with properly grounded plugs.
- Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.
- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables and power cables carefully; route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.

- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications.
- Always follow your local/national wiring rules.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:
 - Install the power supply before connecting the power cable to the power supply.
 - Unplug the power cable before removing the power supply.
 - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.
- Move products with care; ensure that all casters and/or stabilizers are firmly connected to the system. Avoid sudden stops and uneven surfaces.

Step 1: Unpacking

Open the shipping carton and carefully unpack its contents. Please consult the packing list located in the User Manual to make sure all items are present and undamaged.

- One D-Link DMS-1100 Series switch
- One Multilingual Getting Started Guide
- User Guide CD
- Power Cord and Power Cord Retainer
- Rack-mount kit and Rubber Feet

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

Step 2: Switch Installation

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

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

Desktop or Shelf Installation

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

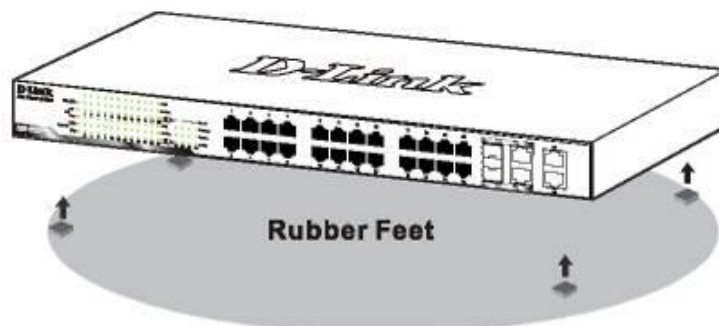


Figure 2.1 – Attach the adhesive rubber pads to the bottom

Rack Installation

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



Figure 2.2 – Attach the mounting brackets to the Switch

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

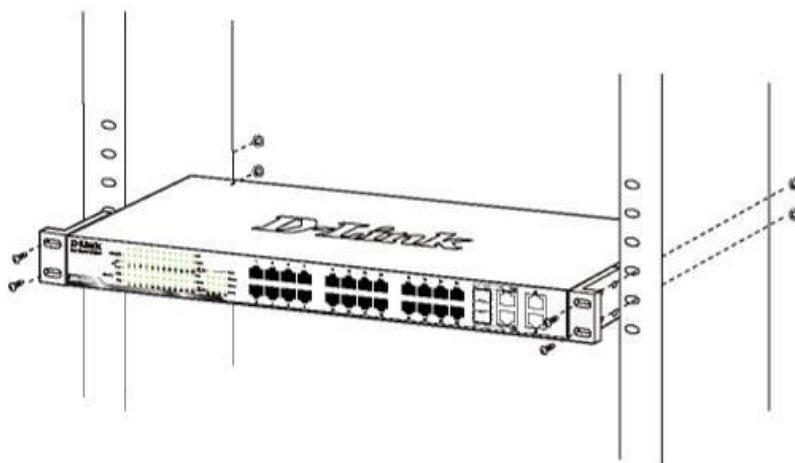


Figure 2.3 – Mount the Switch in the rack or chassis

Step 3 – Plugging in the AC Power Cord with Power Cord Clip

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

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

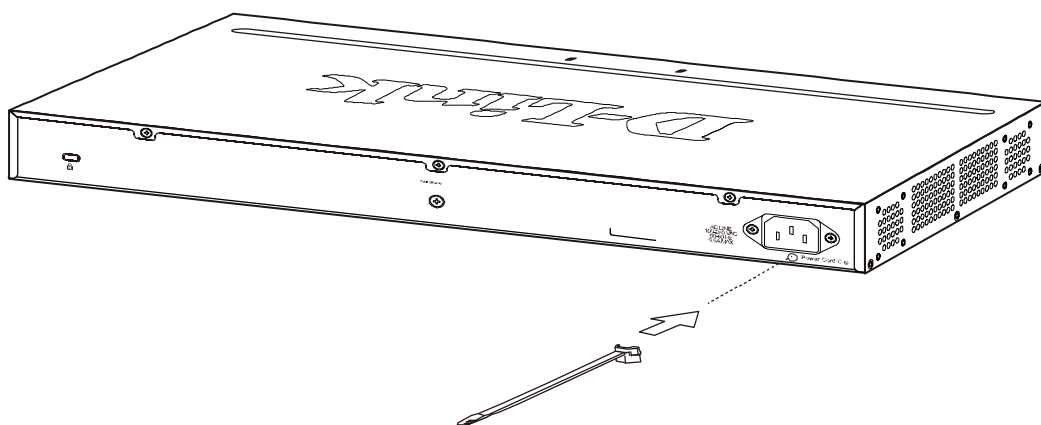


Figure 2.1 – Insert Tie Wrap to the Switch

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

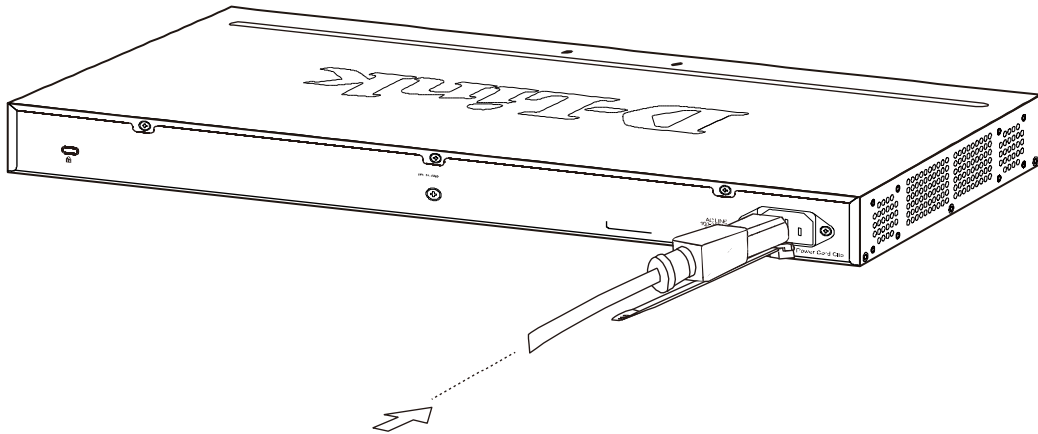


Figure 2.2 – Connect the power cord to the Switch

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

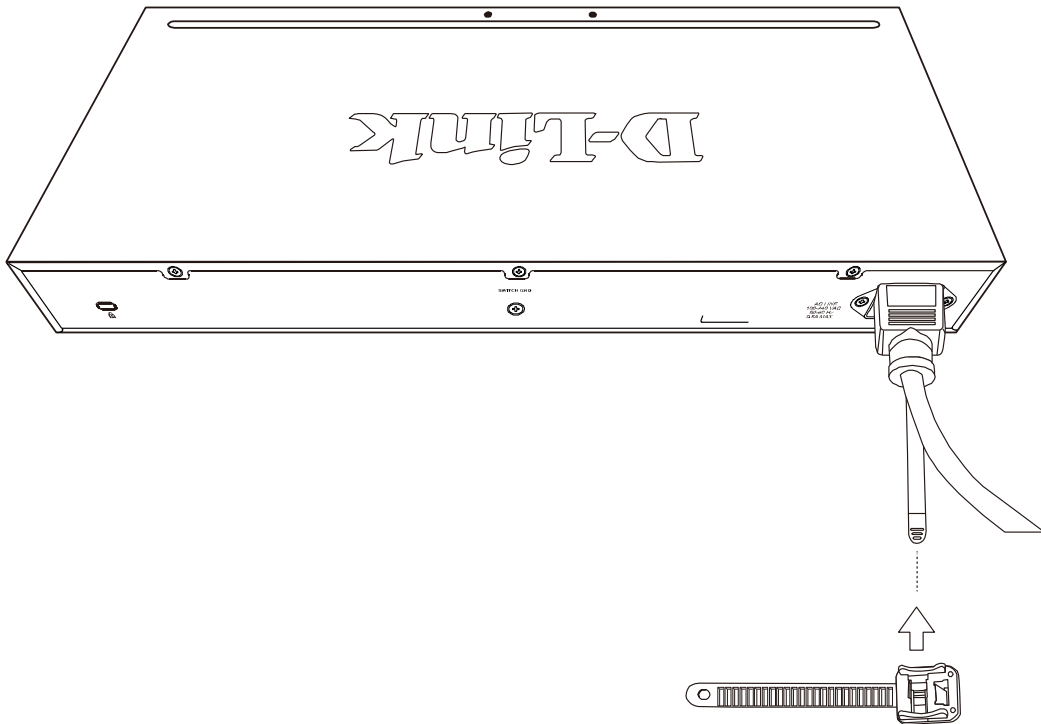


Figure 2.3 – Slide the Retainer through the Tie Wrap

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

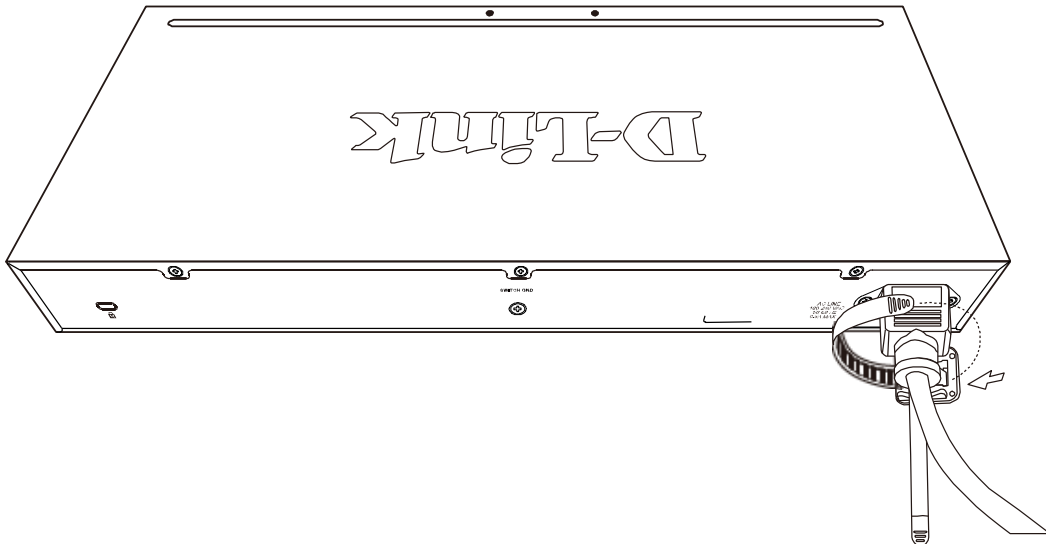


Figure 2.4 – Circle around the power cord

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

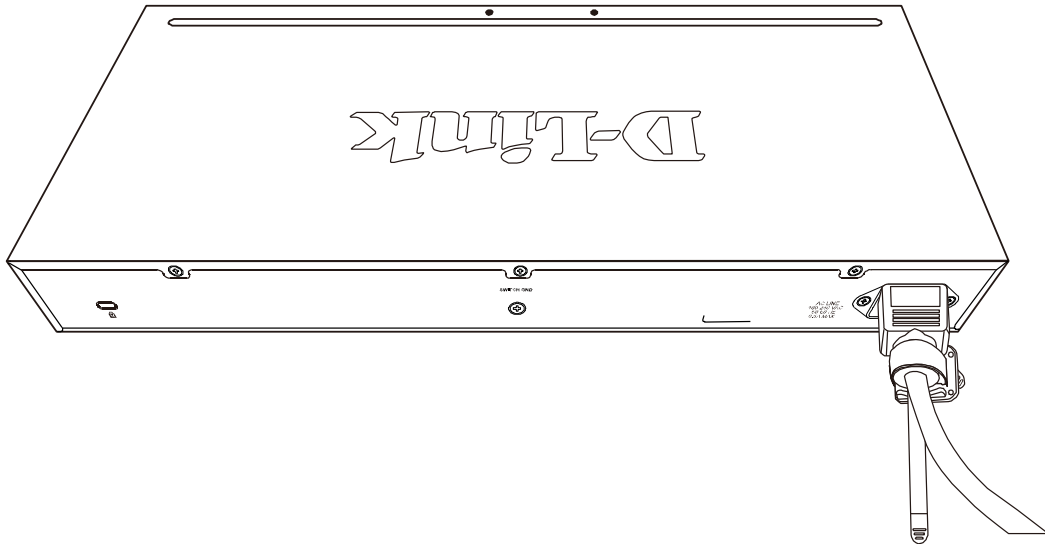


Figure 2.5 – Secure the power cord

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

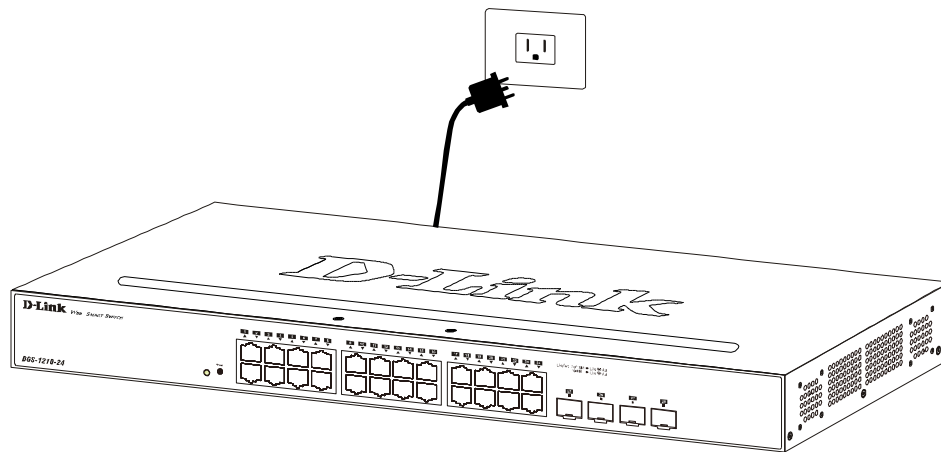


Figure 2.6 – Plugging the switch into an outlet

Power Failure

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

Grounding the Switch

This section describes how to connect the DMS-1100 Series Switch to ground. You must complete this procedure before powering your switch.

Required Tools and Equipment

- Ground screws (included in the accessory kit): One M4 x 6 mm (metric) pan-head screw.
- Ground cable (not included in the accessory kit): The grounding cable should be sized according to local and national installation requirements. Depending on the power supply and system, a 12 to 6 AWG copper conductor is required for U.S installation. Commercially available 6 AWG wire is recommended. The length of the cable depends on the proximity of the switch to proper grounding facilities.
- A screwdriver (not included in the accessory kit)

The following steps let you connect the switch to a protective ground:

Step 1: Verify if the system power is off.

Step 2: Use the ground cable to place the #8 terminal lug ring on top of the ground-screw opening, as seen in the figure below.

Step 3: Insert the ground screw into the ground-screw opening.

Step 4: Using a screwdriver, tighten the ground screw to secure the ground cable to the switch.

Step 5: Attach the terminal lug ring at the other end of the grounding cable to an appropriate grounding stud or bolt on rack where the switch is installed.

Step 6: Verify if the connections at the ground connector on the switch and the rack are securely attached.



Figure 2.10 – Connect a Grounding Cable

3 *Getting Started*

This chapter introduces the management interface of D-Link DMS-1100 Series Switch.

Management Options

The D-Link DMS-1100 Series Switch can be managed through any port 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 subnet as the switch. Each switch can allow up to four users to access the Web-Based Management concurrently.

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

Using Web-based Management

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

Supported Web Browsers

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

- Internet Explorer 7 or later version
- Chrome
- Firefox
- Safari

Connecting to the Switch

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

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

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

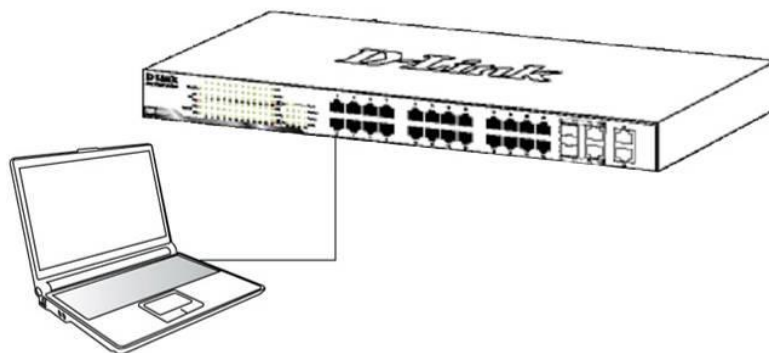


Figure 3.1 – Connected Ethernet cable

Login Web-based Management

In order to login and configure the switch via Web-based GUI, the PC must have an IP address in the same subnet as the switch. For example, if the switch has an IP address of **10.90.90.90**, the PC should have an IP

address of **10.x.y.z** (where x/y is a number between 0 ~ 254 and z is a number between 1 ~ 254), and a subnet mask of **255.0.0.0**. There are two ways to launch the Web-based Management.

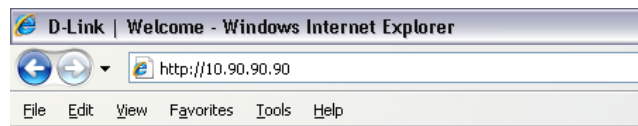


Figure 3.2 –Enter the IP address 10.90.90.90 in the web browser



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 login dialog box appears, enter the password and choose the language of the Web-based Management interface then click **OK**.

The switch supports 10 languages including English, Traditional Chinese, Simplified Chinese, German, Spanish, French, Italian, Portuguese, Japanese and Russian. By default, the language is **English**. Enter the User name and Password with "**admin**" and press Login to enter the main configuration window.

 A screenshot of a login dialog box titled "Connect to 10.90.90.90". It features a key icon and the instruction "Enter your username and password". There are three input fields: "User Name", "Password", and "Language" (set to "English"). At the bottom right, there are "Login" and "Reset" buttons.

Figure 3.3 – Login Dialog Box

Smart Wizard

After a successful login, the Smart Wizard will guide you through essential settings of the D-Link DMS-1100 Series Switch. Please refer to the Smart Wizard Configuration section for details.

Web-based Management

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

4 Configuration

The features and functions of the D-Link DMS-1100 Series Switch can be configured for optimum use through the Web-based Management Utility.

Smart Wizard Configuration

After a successful login, the Smart Wizard will guide you through essential settings of the D-Link DMS-1100 Series Switch. If you do not plan to change anything, click **Exit** to leave the Wizard and enter the Web Interface. You can also skip it by clicking **Ignore the wizard next time** for the next time you logon to the Web-based Management.

IPv4 Information

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

Welcome to Smart Wizard

The wizard will guide you for basic configurations for the IP Information, SNMP, and User Account. If you do not want to change the settings, click on "Exit" to go back to the main page.

Step 1 of 3: The wizard will help to complete settings for System IP address, Netmask, and Gateway.

System IP Information

Static DHCP

IP Address: 10 - 90 - 90 - 90

Netmask: 8 (255.0.0.0) ▼

Gateway: 0 - 0 - 0 - 0

Ignore the wizard next time

Exit Next

Figure 4.1 – IPv4 Information in Smart Wizard



NOTE: The IPv4 Information of Smart Wizard does not support IPv6 address.

SNMP Settings

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

The screenshot shows the 'Welcome to Smart Wizard' interface. It features a blue header with the title 'Welcome to Smart Wizard'. Below the header, there is a wizard icon and a text box explaining the wizard's purpose: 'The wizard will guide you for basic configurations for the IP Information, SNMP, and User Account. If you do not want to change the settings, click on "Exit" to go back to the main page.' Below this, it indicates 'Step 1 of 3: The wizard will help to complete settings for System IP address, Netmask, and Gateway.'

The main configuration area is titled 'System IP Information' and contains the following fields:

- Static
- DHCP
- IP Address: 10 - 90 - 90 - 90
- Netmask: 8 (255.0.0.0)
- Gateway: 0 - 0 - 0 - 0

At the bottom of the configuration area, there is a checkbox labeled 'Ignore the wizard next time' and two buttons: 'Exit' and 'Next'.

Figure 4.2 – SNMP Settings in Smart Wizard

User Accounts Settings

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

Welcome to Smart Wizard

Step 3 of 3: Configure User Account for management.

User Accounts Settings

User Name

Privilege (1-15)

Password Type

Password

Ignore the wizard next time

Exit Back Apply & Save

Figure 4.3 – User Accounts Setting in Smart Wizard

Web-based Management

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

D-Link Building Networks for People

DMS-1100-10TP

Tool Bar

Refresh Interval 10 secs

Save Tools Wizard Online Help English

Logged in as Administrator: admin - 10:00:00 96 Logout

Device Information

| | | | |
|-------------------|---|---------------|---------------------|
| Device Type | DMS-1100-10TP 2.5GbE Smart Managed Switch | MAC Address | 00-50-43-3D-3D-3D |
| System Name | Switch | IP Address | 10.90.90.90 |
| System Location | | Mask | 255.0.0.0 |
| System Contact | | Gateway | 0.0.0.0 |
| Root PROM Version | 1.00.001 | System Time | 14/02/2008 06:41:47 |
| Firmware Version | V1.00.002 | Serial Number | QJQDMS12345600 |
| Hardware Version | A1 | | |

Utilization

Main Configuration Screen

CPU Average (24%) (28%)

Flash Used 80/190KB (34%)

Memory Used 3488/24KB (31%)

Figure 4.4 – Web-based Management

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

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

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

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

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



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

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

Tool Bar > Save Menu

The Save Menu provides Save Configuration and Save Log functions.

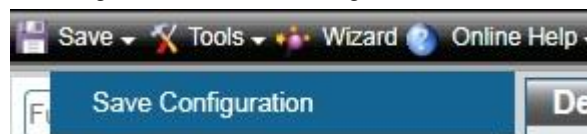


Figure 4.5 – Save Menu

Save Configuration

The Save Configuration page allows user to save the configuration changes to the S witch's non-volatile RAM.

Figure 4.6 – Save Configuration

The fields that can be configured for **Save Configuration** are described below:

| Item | Description |
|-----------------------|---|
| Destination | Select the destination to save the configuration to. |
| Startup-config | Check the box to enable the startup configuration function. |

Table 4.1

Click **Apply** to make the configurations take effect.

Tool Bar > Tool Menu

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



Figure 4.7 – Tool Menu

Firmware Information

The Firmware Information page displays the firmware image information, including the image that has been booted and the image that is selected for the next reboot.

| Firmware Information | | | | |
|----------------------|-----------|----------|---------------------|---------|
| Firmware Information | | | | |
| Image ID | Version | Size (B) | Update Time | |
| 1 | V1.00.002 | 22961424 | 01/01/2009 00:00:00 | Boot Up |
| *2c | V1.00.002 | 22961424 | 01/01/2009 00:00:00 | Boot Up |

c : Current boot up firmware
* : Boot up firmware

Figure 4.8 – Tool Menu > Firmware Information

Configuration Information

The Configuration Information page displays information for the Switch configuration. This includes the configuration that has been loaded and the configuration that is selected for the next reboot.

| Configuration Information | | | |
|---------------------------|---------|-------------|---------|
| Configuration Information | | | |
| Configuration ID | Size(B) | Update Time | |
| * 1 c | 0 | 0 | Boot Up |
| 2 | 0 | 0 | Boot Up |

c : Current boot up configuration
* : Boot up configuration

Figure 4.9 – Tool Menu > Configuration Information

Firmware Upgrade & Backup > Firmware Upgrade from HTTP

The Firmware upgrade from HTTP page allows user to upgrade the firmware of Switch from a firmware file.

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

The fields that can be configured for **Firmware Upgrade** are described below:

| Item | Description |
|------------------------|---|
| Source URL | Click Choose File button to select the source URL to upgrade the configuration from. |
| Destination URL | Displays the destination URL to upgrade to. |

Table 4.2

Click **Upgrade** button to upload firmware to the Switch via **HTTP**.



Note: The new firmware will be set as another image in dual image system. User have to go "system>firmware information" to select new image as boot up firmware and reboot the system. Then new firmware will be activated.

Firmware Upgrade & Backup > Firmware Upgrade from TFTP

This Firmware Upgrade from TFTP page allows user to upgrade firmware using TFTP.

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

The fields that can be configured for **Firmware Upgrade from TFTP** are described below:

| Item | Description |
|------------------------|---|
| TFTP Server IP | Select IPv4 or IPv6 and enter the address to be configured. |
| Source URL | Enter the source URL address. |
| Destination URL | Displays the destination URL address. |

Table 4.3

Click the **Upgrade** button to upgrade the firmware from specified TFTP address.



Note: The new firmware will be set as another image in dual image system. **User** have to go "system>firmware information" to select new image as boot up firmware and reboot the system. Then new firmware will be activated.

Firmware Backup to HTTP & Backup > Firmware Backup to HTTP

The Firmware Backup to HTTP page allows user to save a backup of the firmware, select the source URL and then click **Backup**.

The screenshot shows a web interface titled 'Firmware Backup to HTTP'. Below the title, there is a sub-header 'Firmware Backup to HTTP'. Underneath, there is a 'Source URL' label followed by a dropdown menu currently showing 'Image1'. To the right of the dropdown is a 'Backup' button.

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

The fields that can be configured for **Firmware Backup to HTTP** are described below:

| Item | Description |
|-------------------|--|
| Source URL | Select the source URL to be backup to. |

Table 4.4

Click **Backup** button to backup the specified firmware.

Firmware Backup to HTTP & Backup > Firmware Backup to TFTP

The Firmware Backup to TFTP allows user to save a backup of the firmware using TFTP, enter the TFTP server IP address, the source URL, and the destination URL. Click **Backup**.

The screenshot shows a web interface titled 'Firmware Backup to TFTP'. Below the title, there is a sub-header 'Firmware Backup to TFTP'. Underneath, there are three main fields: 'TFTP Server IP' with a text input and radio buttons for 'IPv4' (selected) and 'IPv6'; 'Source' with a dropdown menu showing 'Image1'; and 'Destination URL' with a text input showing '64 chars'. A 'Backup' button is located at the bottom right.

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

The fields that can be configured for **Firmware Backup to TFTP** are described below:

| Item | Description |
|------------------------|---|
| TFTP Server IP | Select IPv4 or IPv6 and enter the address to be configured. |
| Source | Enter the source URL address. |
| Destination URL | Displays the destination URL address. |

Table 4.5

Click the **Upgrade** button to upgrade the firmware to specified TFTP address.

Configuration Upgrade & Backup > Configuration Restore from HTTP

The Configuration Restore from HTTP page allows user to restore the Switch from a saved configuration file.

The screenshot shows a web interface titled 'Configuration Restore from HTTP'. Below the title, there is a sub-header 'Configuration Restore from HTTP'. Underneath, there are two main fields: 'Source URL' with a 'Choose File' button and 'No file chosen' text; and 'Destination' with a dropdown menu showing 'Config 1' and a checked checkbox for 'startup-config'. A 'Restore' button is located at the bottom right.

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

The fields that can be configured for **Configuration Restore** are described below:

| Item | Description |
|-------------------|---|
| Source URL | Click Choose File button to select the source URL to restore the configuration from. |

| | |
|------------------------|---|
| Destination URL | Displays the destination URL to upgrade to. |
| Startup-config | Check the box to enable the startup configuration function. |

Table 4.6

Click **Restore** button to upload configuration to the Switch via **HTTP**.

Configuration Upgrade & Backup > Configuration Restore from TFTP

The Configuration Restore from TFTP page allows user to load the Switch's configuration from a saved configuration file using TFTP.

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

The fields that can be configured for **Configuration Restore from TFTP** are described below:

| Item | Description |
|------------------------|---|
| TFTP Server IP | Select IPv4 or IPv6 and enter the address to be configured. |
| Destination URL | Displays the destination URL address. |
| Startup-config | Check the box to enable the startup configuration function. |
| Source URL | Enter the source URL address. |

Table 4.7

Click the **Restore** button to upgrade the configuration from specified TFTP address.

Configuration Upgrade & Backup > Configuration Backup to HTTP

The Configuration Backup to HTTP page allows user to save the current configuration to a file.

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

Configuration Upgrade & Backup > Configuration Backup to TFTP

The Configuration Backup to TFTP page allows user to save the current configuration to a file using TFTP.

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

The fields that can be configured for **Configuration Backup from TFTP** are described below:

| Item | Description |
|------------------------|---|
| TFTP Server IP | Select IPv4 or IPv6 and enter the address to be configured. |
| Source | Enter the source URL address. |
| Startup-config | Check the box to enable the startup configuration function. |
| Destination URL | Displays the destination URL address. |

Table 4.8

Click the **Backup** button to save the configuration from specified TFTP address.

Log Backup > Log Backup to HTTP

The Log Backup to HTTP page allows user to save the log to a file.

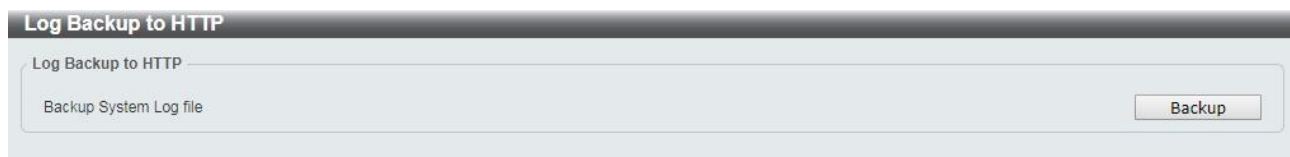


Figure 4.18 – Tool Menu > Log Backup > Log Backup to HTTP

Log Backup > Log Backup to TFTP

The Log Backup to TFTP page allows user to save the log to a file using TFTP.



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

The fields that can be configured for **Log Backup** are described below:

| Item | Description |
|------------------------|---|
| TFTP Server IP | Select IPv4 or IPv6 and enter the address to be configured. |
| Destination URL | Enter the destination URL for the backup. |

Table 4.9

Click the **Backup** button to save the log to specified TFTP address.

Ping

The Ping page allows user to ping a computer or device. The result will be displayed in the **Result** box.

Ping

IPv4 Ping

Target IPv4 Address

Ping Times (1-255) Infinite

Timeout (1-99) sec

Apply

IPv6 Ping

Target IPv6 Address

Ping Times (1-255) Infinite

Timeout (1-99) sec

Apply

Figure 4.20 – Ping

The fields that can be configured for **Ping** are described below:

| Item | Description |
|----------------------------|--|
| IPv4 Ping | |
| Target Ipv4 Address | Enter the IPv4 address to be pinged. |
| Ping Times (1-255) | Specify the ping time. The range is from 1 to 255. |
| Timeout (1-99) | Specify the timeout period while waiting for a response from the remote device. The range is from 1 to 99 seconds. |
| IPv6 Ping | |
| Target Ipv6 Address | Enter the IPv6 address to be pinged. |
| Ping Times (1-255) | Specify the ping time. The range is from 1 to 255. |
| Timeout (1-99) | Specify the timeout period while waiting for a response from the remote device. The range is from 1 to 99 seconds. |

Table 4.10

Click **Apply** to make the configurations take effect.

Reset

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

Reset

Reset

The Switch will be reset to its factory defaults except IP address, and then will save, reboot.

The Switch will be reset to its factory defaults including IP address.

Apply

Figure 4.21 – Tool Menu > Reset

Reboot System

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

Reboot System

Reboot System

Do you want to save the settings? Yes No

Destination startup-config

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

Reboot

Figure 4.22 – Tool Menu > Reboot System

The fields that can be configured for **Reboot System** are described below:

| Item | Description |
|-----------------------|--|
| Destination | Select the configuration destination to be saved. |
| Startup-config | When checking the box, only the current startup configuration file will be backed up which may be stored in the "Config 1" location. |

Table 4.11

Click **Reboot** to reboot the system with specified configuration.

Tool Bar > Smart Wizard

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

Tool Bar > Online Help

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



Figure 4.23 – Online Help



Figure 4.24 – User Guide Micro Site

Function Tree

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

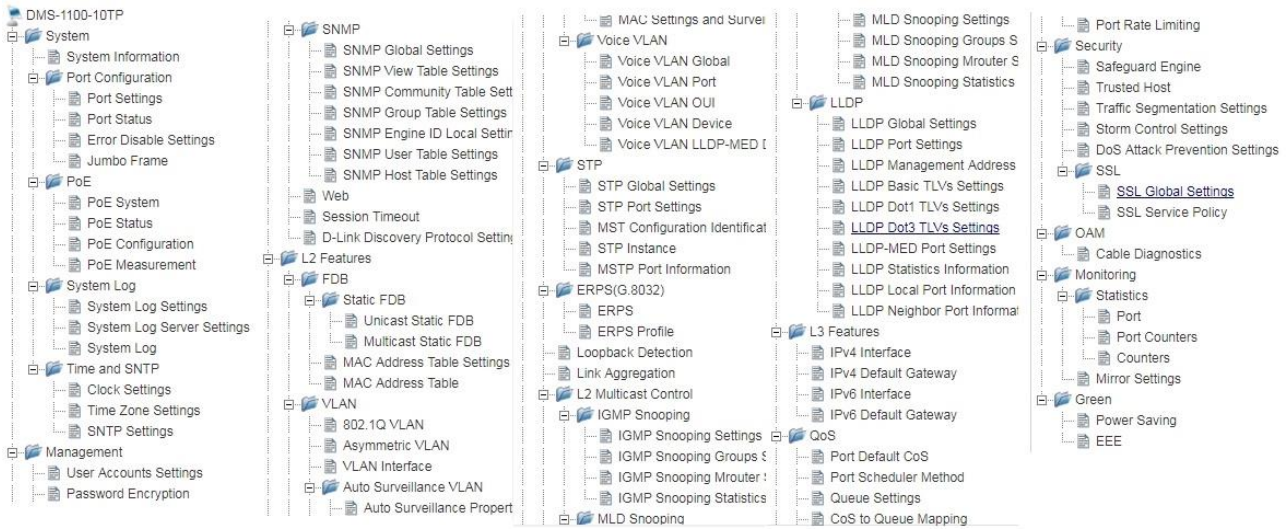


Figure 4.25 –Function Tree

Device Information

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

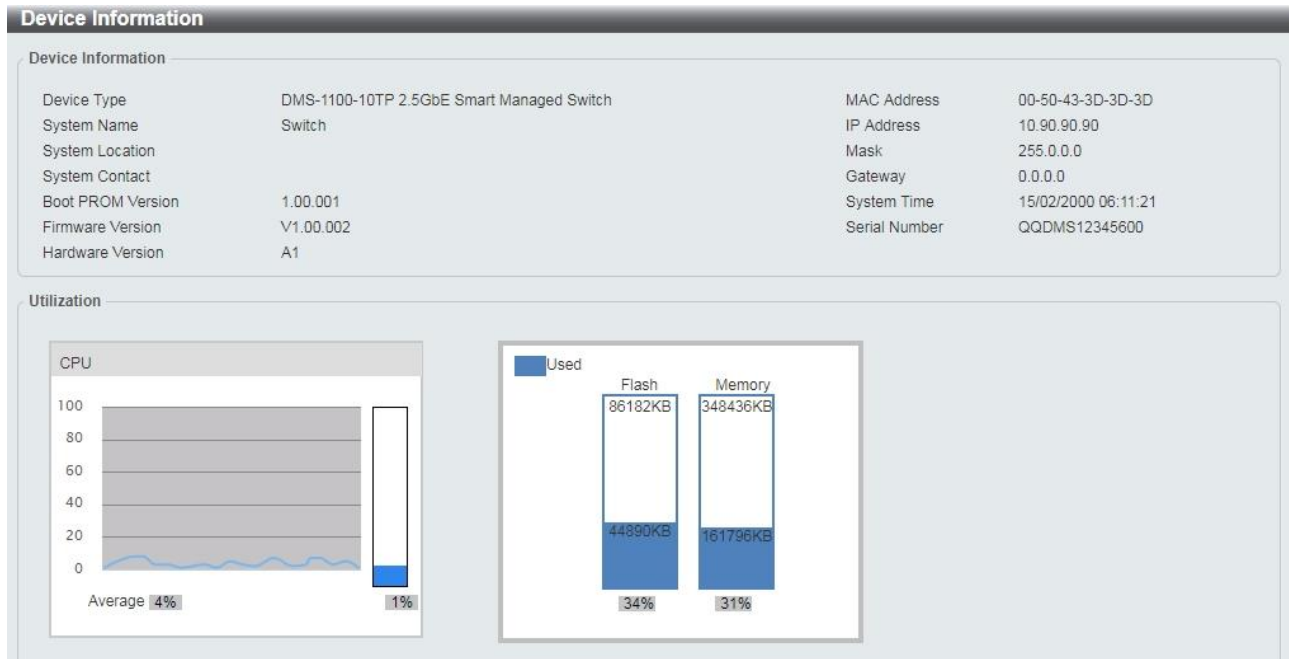


Figure 4.26 – Device Information

System > System Information

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

Figure 4.27 – System > System Information

The fields that can be configured for **System Information** are described below:

| Item | Description |
|------------------------|--|
| System name | Enter the system name to be specified. |
| System Location | Enter the system location to be specified. |
| System Contact | Enter the system contact to be specified. |

Table 4.12

Click **Apply** to make the configurations take effect.

System > Port Configuration > Port Settings

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

| Port | Link Status | State | Flow Control | | Duplex | Speed | Description |
|--------------|-------------|---------|--------------|---------|-------------|------------|-------------|
| | | | Send | Receive | | | |
| eth1/0/1 | Down | Enabled | On | On | Auto-duplex | Auto-speed | |
| eth1/0/2 | Down | Enabled | On | On | Auto-duplex | Auto-speed | |
| eth1/0/3 | Up | Enabled | On | On | Auto-duplex | Auto-speed | |
| eth1/0/4 | Down | Enabled | On | On | Auto-duplex | Auto-speed | |
| eth1/0/5 | Down | Enabled | On | On | Auto-duplex | Auto-speed | |
| eth1/0/6 | Down | Enabled | On | On | Auto-duplex | Auto-speed | |
| eth1/0/7 | Down | Enabled | On | On | Auto-duplex | Auto-speed | |
| eth1/0/8 | Down | Enabled | On | On | Auto-duplex | Auto-speed | |
| eth1/0/9(F) | Down | Enabled | Off | Off | Auto-duplex | Auto-speed | |
| eth1/0/10(F) | Down | Enabled | Off | Off | Auto-duplex | Auto-speed | |

Figure 4.28 – System > Port Configuration > Port Settings

The fields that can be configured for **Port Settings** are described below:

| Item | Description |
|----------------------------|--|
| From Port / To Port | Select the appropriate port range to be configured. |
| Media | Select the media type for specified port. The media type is Copper for port 1 ~ port 8 and Fiber for port 9 ~ port 10. |
| State | Enable or disable the physical port. |
| Flow Control | Select On or Off . Ports configured for full-duplex use 802.3x flow control, half-duplex ports use back-pressure flow control, and Auto ports use an automatic selection of the two. |
| Duplex | Select the duplex mode used. Options to choose from are Auto and |

| | |
|------------------------------|--|
| | Full. |
| Speed | Select the speed for the ports. The speed values are Auto , 10M , 100M , 1000M , 2.5G and 10G . Any other configuration will result in a link down status for both ports. |
| Capability Advertised | When the Speed is set to Auto , these capabilities are advertised during auto-negotiation. When specify the port 1 ~ port 8, these capabilities advertised with 10G cannot be selected. When specify the port 9 ~ port 10, the capability advertised can be selected with 1000M and 10G . |
| Description | Enter a 64 characters description for the corresponding port. |

Table 4.13

Click **Apply** to make the configurations take effect.

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

System > Port Configuration > Port Status

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

| Port Status | | | | | | | |
|--------------|---------------|-------------------|------|-----------------------|---------|-----------|------------|
| Port Status | | | | | | | |
| Port | Status | MAC Address | VLAN | Flow Control Operator | | Duplex | Speed |
| | | | | Send | Receive | | |
| eth1/0/1 | Not-Connected | 00-50-43-3D-3D-3E | 1 | Off | Off | Auto | Auto |
| eth1/0/2 | Not-Connected | 00-50-43-3D-3D-3F | 1 | Off | Off | Auto | Auto |
| eth1/0/3 | Connected | 00-50-43-3D-3D-40 | 1 | Off | Off | Auto-Full | Auto-1000M |
| eth1/0/4 | Not-Connected | 00-50-43-3D-3D-41 | 1 | Off | Off | Auto | Auto |
| eth1/0/5 | Not-Connected | 00-50-43-3D-3D-42 | 1 | Off | Off | Auto | Auto |
| eth1/0/6 | Not-Connected | 00-50-43-3D-3D-43 | 1 | Off | Off | Auto | Auto |
| eth1/0/7 | Not-Connected | 00-50-43-3D-3D-44 | 1 | Off | Off | Auto | Auto |
| eth1/0/8 | Not-Connected | 00-50-43-3D-3D-45 | 1 | Off | Off | Auto | Auto |
| eth1/0/9(F) | Not-Connected | 00-50-43-3D-3D-46 | 1 | Off | Off | Auto | Auto |
| eth1/0/10(F) | Not-Connected | 00-50-43-3D-3D-47 | 1 | Off | Off | Auto | Auto |

Figure 4.29 – System > Port Configuration > Port Status

System > Port Configuration > Error Disable Settings

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

| Error Disable Settings | | | |
|---|---------------------------------------|---------------------------------------|---------------------------------------|
| Error Disable Trap Settings | | | |
| Asserted | <input type="text" value="Disabled"/> | <input type="text" value="Disabled"/> | <input type="text" value="0"/> |
| Cleared | <input type="text" value="Disabled"/> | <input type="text" value="0"/> | <input type="text" value="0"/> |
| Notification Rate (0-1000) | <input type="text" value="0"/> | <input type="text" value="0"/> | <input type="text" value="0"/> |
| <input type="button" value="Apply"/> | | | |
| Error Disable Recovery Settings | | | |
| ErrDisable Cause | <input type="text" value="All"/> | State | <input type="text" value="Disabled"/> |
| | | Interval (5-86400) | <input type="text" value=""/> |
| <input type="button" value="Apply"/> | | | |
| ErrDisable Cause | State | Interval (sec) | |
| Storm Control | Disabled | 300 | |
| Loopback Detect | Disabled | 300 | |
| Interfaces that will be recovered at the next timeout : | | | |
| Interface | VLAN | ErrDisable Cause | Time left (sec) |
| << Table is empty >> | | | |

Figure 4.30 – System > Port Configuration > Error Disable Settings

The fields that can be configured for **Error Disable Settings** are described below:

| Item | Description |
|--|--|
| Error Disable Trap Settings | |
| Asserted | Select to enable or disable the notifications when entering into the error disabled state. |
| Cleared | Select to enable or disable the notifications when exiting from the error disabled state. |
| Notification Rate (0-1000) | Enter the number of traps per minute. The packets that exceed the rate will be dropped. The value is between 0 and 1000. |
| Error Disable Recovery Settings | |
| ErrDisable Cause | Specify the error disable causes. Options to choose from are Storm and Loopback Detect . |
| State | Select to enable or disable the auto-recovery for an error port caused by the specified cause. |
| Interval (5-586400) | Enter the time interval. The values are between 5 and 586400 seconds. And default value is 300. |

Table 4.14

Click **Apply** to make the configurations take effect.

System > Port Configuration > Jumbo Frame

The Jumbo Frame page allows user to view and configure the Jumbo Frame settings.

| Port | Maximum Receive Frame Size (bytes) |
|-----------|------------------------------------|
| eth1/0/1 | 1536 |
| eth1/0/2 | 1536 |
| eth1/0/3 | 1536 |
| eth1/0/4 | 1536 |
| eth1/0/5 | 1536 |
| eth1/0/6 | 1536 |
| eth1/0/7 | 1536 |
| eth1/0/8 | 1536 |
| eth1/0/9 | 1536 |
| eth1/0/10 | 1536 |

Figure 4.31 –System > Port Configuration > Jumbo Frame

The fields that can be configured for **Jumbo Frame** are described below:

| Item | Description |
|---|--|
| From Port / To Port | Specify the port to be configured. |
| Maximum Receive Frame Size (1518-9216) | Specify the maximum receive frame size. The range is between 1518 and 9216. The default value is 1536. |

Table 4.15

Click **Apply** to make the configurations take effect.

System > PoE > PoE System (DMS-1100-10TP only)

DMS-1100-10TP supports Power over Ethernet (PoE) as defined by the IEEE specification. It supplies power to PD device up to 30W for port 1~8, meeting IEEE802.3af standards and pre-802.3at standards.

DMS-1100-10TP works with all D-Link 802.3af or 802.3at capable devices. The Switch is highly compatible with all IEEE 802.3at/af compliant equipment, and transform the PoE to provide power to D-Link wireless APs, IP Cams, IP phones. And also works with DPE-301GS PoE splitter providing 30W power to legacy PD devices.

IEEE 802.3af defined that the PSE provides power according to the following classification:

| Class | Usage | Minimum Power Levels Output at the PSE | Maximum Power Levels at the Powered Device |
|-------|----------|--|--|
| 0 | Default | 15.4W | 0.44 to 12.95W |
| 1 | Optional | 4.0W | 0.44 to 3.84W |
| 2 | Optional | 7.0W | 3.84 to 6.49W |
| 3 | Optional | 15.4W | 6.49 to 12.95W |
| 4 | Optional | Treat as Class 0 | Reserved for future use |

IEEE 802.3at defined that the PSE provides power according to the following classification:

| Class | Usage | Powered Device Classification | Guaranteed output power by PSE Output | Maximum Power Levels at the Powered Device |
|-------|----------|-------------------------------|---------------------------------------|--|
| 0 | Default | Default, Type 1 | 15.4W | 0.44 to 12.95W |
| 1 | Optional | Type 1 | 4.0W | 0.44 to 3.84W |
| 2 | Optional | Type 1 | 7.0W | 3.84 to 6.49W |
| 3 | Optional | Type 1 | 15.4W | 6.49 to 12.95W |
| 4 | Optional | Type 2 | 30W | 12.95 to 25.5W |

IEEE 802.3at defined that the PSE provides power according to the following classification: The PoE System page is used to configure the PoE system for PoE modules.

Figure 4.32 –System > PoE > PoE System

The fields that can be configured for **PoE System** are described below:

| Item | Description |
|-------------------------|--|
| Power Budget (W) | Displays the power budget of Watts on the device |

| | |
|-----------------------|--|
| Delivered (W) | Displays how much power of Watts had been delivered. |
| Legacy Support | Specify to enable or disable detecting legacy PDs signal. The default is disabled. |

Table 4.16

Click **Apply** to make the configurations take effect.



Note: This product is to be connected only to PoE networks without routing to the outside plant.

System > PoE > PoE Status (DMS-1100-10TP only)

The PoE Status page displays the PoE status of each port.

| PoE Status | | | | | |
|------------|----------|-------|---------|----------|--|
| PoE Status | | | | | |
| Port | State | Class | Max (W) | Used (W) | |
| eth1/0/1 | Disabled | N/A | 0.0 | 0.0 | |
| eth1/0/2 | Disabled | N/A | 0.0 | 0.0 | |
| eth1/0/3 | Disabled | N/A | 0.0 | 0.0 | |
| eth1/0/4 | Disabled | N/A | 0.0 | 0.0 | |
| eth1/0/5 | Disabled | N/A | 0.0 | 0.0 | |
| eth1/0/6 | Disabled | N/A | 0.0 | 0.0 | |
| eth1/0/7 | Disabled | N/A | 0.0 | 0.0 | |
| eth1/0/8 | Disabled | N/A | 0.0 | 0.0 | |

Figure 4.33 –System > PoE > PoE Status



Note: For the PoE Port Settings table, if the classification was shown as “Legacy PD”, it will be classified to non-AF PD or Legacy PD.

System > PoE > PoE Configuration (DMS-1100-10TP only)

The PoE Configuration page is used to configure the PoE port.

| PoE Configuration | | | | | |
|-------------------|----------|----------|------|--------------------------|--|
| PoE Configuration | | | | | |
| From Port | To Port | Priority | Mode | Max Wattage(1000-30000) | |
| eth1/0/1 | eth1/0/1 | Low | Auto | <input type="checkbox"/> | |
| Apply | | | | | |
| Port | Admin | Priority | | | |
| eth1/0/1 | Auto | Low | | | |
| eth1/0/2 | Auto | Low | | | |
| eth1/0/3 | Auto | Low | | | |
| eth1/0/4 | Auto | Low | | | |
| eth1/0/5 | Auto | Low | | | |
| eth1/0/6 | Auto | Low | | | |
| eth1/0/7 | Auto | Low | | | |
| eth1/0/8 | Auto | Low | | | |

Figure 4.34 –System > PoE > PoE Configuration

The fields that can be configured for **PoE Configuration** are described below:

| Item | Description |
|----------------------------|---|
| From Port / To Port | Select the appropriate port range used for the configuration. |

| | |
|---------------------------------|--|
| Pirority | Select the priority for provisioning power to the port. Options to choose from are Critical, High and Low. |
| Mode | Select the power management mode for the PoE ports. Options to choose from are Auto, Class 1, Class 2, Class 3, and Class 4. |
| Max Wattage (1000-30000) | When selecting Auto in the Mode drop-down list, this option appears. Tick the check box and enter the maximum wattage of power that can be provisioned to the auto-detected PD. If the value is not entered, the class of the PD automatically determines the maximum wattage which can be provisioned. The valid range for maximum wattage is between 1000 mW and 30000 mW. |

Table 4.17

Click **Apply** to make the configurations take effect.



Note: For DMS-1100-10TP, the port 1 ~ port 8 are compliance with 802.3at. The total PoE budget is 240 Watts.

System > PoE > PoE Measurement (DMS-1100-10TP only)

The PoE measurement page displays the measurement information of PoE ports.

| PoE Measurement | | | |
|-----------------|-------------|--------------|-----------|
| PoE Measurement | | | |
| Port | Voltage (V) | Current (mA) | Power (W) |
| eth1/0/1 | 0.0 | 0 | 0.0 |
| eth1/0/2 | 0.0 | 0 | 0.0 |
| eth1/0/3 | 0.0 | 0 | 0.0 |
| eth1/0/4 | 0.0 | 0 | 0.0 |
| eth1/0/5 | 0.0 | 0 | 0.0 |
| eth1/0/6 | 0.0 | 0 | 0.0 |
| eth1/0/7 | 0.0 | 0 | 0.0 |
| eth1/0/8 | 0.0 | 0 | 0.0 |

Figure 4.35 –System > PoE > PoE Measurement

System > System Log > System Log Settings

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

| System Log Settings | | | |
|--------------------------------------|-------------|--------------|-----------------------------------|
| Global State | | | |
| Source Interface State | Enabled | | |
| Type | VLAN | VID (1-4094) | 1 |
| <input type="button" value="Apply"/> | | | |
| Buffer Log Settings | | | |
| Buffer Log State | Enabled | | |
| Severity | 4(Warnings) | | |
| Write Delay (0-65535) | 300 | sec | <input type="checkbox"/> Infinite |
| <input type="button" value="Apply"/> | | | |

Figure 4.36 – System > System Log > System Log Settings

The fields that can be configured for **System Log Settings** are described below:

| Item | Description |
|------------------------|-------------|
| Global Settings | |

| | |
|-------------------------------|--|
| Source Interface State | Select to enable or disable the source interface's global state. |
| Type | Select the type of interface that will be used. The default option is VLAN . |
| VID (1-4094) | Specifies the VLAN ID. The possible range is 1 – 4094. |
| Buffer Log Settings | |
| Buffer Log State | Select to enable or disable the buffer log state. |
| Severity | Select the severity value of the type of information that will be logged. The values are 0 (Emergencies), 1 (Alerts) , 2 (Critical) , 3 (Errors) , 4 (Warnings) , 5 (Notifications) , 6 (Informational) , and 7 (Debugging) . |
| Write Delay (0-65535) | Enter the interval for periodic writing of the logging buffer to flash. The value is between 0 and 65535 seconds. And default is 300 seconds. Tick the Infinite option, to disable the write delay feature. |

Table 4.18

Click **Apply** to make the configurations take effect.

System > System Log > System Log Server Settings

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

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

The fields that can be configured for **System Log Server Settings** are described below:

| Item | Description |
|-------------------------------------|--|
| IPv4 Address | Select and enter the IPv4 address. |
| UDP Port (514 or 1024-65535) | Enter the system log server's UDP port number. This value must be 514 or between 1024 and 65535. The default value is 514. |
| Severity | Select the severity value of the type of information that will be logged. Options to choose from are 0 (Emergencies) , 1 (Alerts) , 2 (Critical) , 3 (Errors) , 4 (Warnings) , 5 (Notifications) , 6 (Informational) , and 7 (Debugging) . |
| Facility | Select the facility value. The values must be between 0 and 23. |

Table 4.19

Click **Apply** to make the configurations take effect and click the **Delete** button to remove the entry.

System > System Log > System Log

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

System Log

System Log

Clear Log

Total Entries : 13

| Index | Time | Level | Log Description |
|-------|---------------------|-------------|---|
| 13 | 03/03/2000 02:45:30 | Warnings(4) | Login failed through Web(IP: 10.90.90.98) |
| 12 | 03/03/2000 02:44:09 | Critical(2) | System started up |
| 11 | 20/03/2014 15:44:29 | Critical(2) | Side Fan failed. |
| 10 | 15/02/2000 06:03:40 | Critical(2) | System started up |
| 9 | 20/03/2014 15:44:29 | Critical(2) | Side Fan failed. |
| 8 | 14/02/2000 06:35:20 | Critical(2) | System started up |
| 7 | 20/03/2014 15:44:29 | Critical(2) | Side Fan failed. |
| 6 | 08/02/2000 06:47:29 | Warnings(4) | Login failed through Web(IP: 10.90.90.96) |
| 5 | 08/02/2000 06:45:24 | Critical(2) | System started up |
| 4 | 20/03/2014 15:44:29 | Critical(2) | Side Fan failed. |

1/2 < < 1 2 > > Go

Figure 4.38 – System > System Log > System Log

System > Time and SNTP > Clock Settings

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

Clock Settings

Clock Settings

Time (HH:MM:SS)

Date (DD/MM/YYYY)

Apply

Figure 4.39 – System > Time and SNTP > Clock Settings

The fields that can be configured for **Clock Settings** are described below:

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

Table 4.20

Click **Apply** to make the configurations take effect.

System > Time and SNTP > Time Zone Settings

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

| TimeZone Settings | |
|--------------------------|----------|
| Summer Time State | Disabled |
| Time Zone | + 00 00 |
| Recurring Setting | |
| From: Week of the Month | Last |
| From: Day of the Week | Sun |
| From: Month | Jan |
| From: Time (HH:MM) | 00 00 |
| To: Week of the Month | Last |
| To: Day of the Week | Sun |
| To: Month | Jan |
| To: Time (HH:MM) | 00 00 |
| Offset | 60 |
| Date Settings | |
| From: Date of the Month | 01 |
| From: Month | Jan |
| From: Year | |
| From: Time (HH:MM) | 00 00 |
| To: Date of the Month | 01 |
| To: Month | Jan |
| To: Year | |
| To: Time (HH:MM) | 00 00 |
| Offset | 60 |
| Apply | |

Figure 4.40 – System > Time and SNTP > Time Zone Settings

The fields that can be configured for **Time Zone Settings** are described below:

| Item | Description |
|--------------------------------|--|
| Time Zone Settings | |
| Summer Time State | Select Summer Time State setting. Options to choose from are Disabled , Recurring Setting , and Date Setting . |
| Time Zone | Select the local time zone's offset from Coordinated Universal Time (UTC). |
| Recurring Settings | |
| From: Week of the Month | Select week of the month that daylight saving time will start. |
| From: Day of the Week | Select day of the week that daylight saving time will start. |
| From: Month | Select the month that daylight time will start. |
| From: Time in HH MM | Select the time of the day that daylight saving time will start. |
| To: Week of the Month | Select week of the month that daylight saving time will end. |
| To: Day of the Week | Specify day of the week that daylight saving time will end. |
| To: Month | Select the month that daylight saving time will end. |
| To: Time In HH MM | Select the time of the day that daylight saving time will end. |
| Offset | Enter the number of minutes to add during daylight saving time. The default value is 60. The range of this offset is 30, 60, 90 and 120. |
| Date Settings | |

| | |
|--------------------------------|---|
| From: Date of the Month | Select date of the month that daylight saving time will start. |
| From: Month | Select the month that daylight saving time will start. |
| From: Year | Select the year that the daylight saving time will start. |
| From: Time In HH MM | Select the time of the day that daylight saving time will start. |
| To: Date of the Month | Select the date of the month that daylight saving time will end. |
| To: Month | Select the month that daylight saving time will end. |
| To: Year | Select the year that the daylight saving time will end. |
| To: Time In HH MM | Select the time of the day that daylight time will end. |
| Offset | Select the number of minutes to add during daylight saving time. The default value is 60. The range of this offset is 30, 60, 90 and 120. |

Table 4.21

Click **Apply** to make the configurations take effect.

System > Time and SNTP > SNTP Settings

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

Figure 4.41 – System > Time and SNTP > SNTP Settings

The fields that can be configured for **SNTP Settings** are described below:

| Item | Description |
|---------------------------------|--|
| SNTP Global Settings | |
| SNTP State | Select to enable or disable the SNTP state. |
| Poll Interval (30-99999) | Enter the poll interval. The value is from 30 to 99999 seconds. The default interval is 720 seconds. |
| SNTP Server Settings | |
| IPv4 Address | Enter the IPv4 address of the SNTP server which provides the clock synchronization. |

Table 4.22

Click **Apply** to make the configurations take effect.

Management > User Accounts Settings

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

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

- **Basic User** – Privilege Level 1. This user account level has the lowest priority of the user accounts. The purpose of this type of user account level is for basic system checking.
- **Operator** – Privilege Level 12. This user account level is used to grant system configuration information for users who need to change or monitor system configuration, except for security related information such as user accounts and SNMP account settings.
- **Administrator** – Privilege Level 15. This administrator user account level can monitor all system information and change any of the system configuration settings expressed in this guide.

The screenshot shows the 'User Accounts Settings' page. It has two tabs: 'User Management Settings' (selected) and 'Session Table'. Under 'User Management Settings', there are input fields for 'User Name' (with a '32 chars' limit), 'Privilege (1-15)', 'Password Type' (set to 'None'), and 'Password'. An 'Apply' button is on the right. Below the fields, it says 'Total Entries : 1'. A table lists the existing user:

| User Name | Privilege | Password | |
|-----------|-----------|----------|--------|
| admin | 15 | ***** | Delete |

Figure 4.42 – Management > User Accounts Settings

The fields that can be configured for **User Accounts Settings** are described below:

| Item | Description |
|-------------------------|--|
| User Name | Enter the name of the user name. The name can be up to 32 characters long. |
| Privilege (1-15) | Select the privilege level for this account. The value is between 1 and 15. |
| Password Type | Select a password type for this user account. The options are None , Plain Text , and Encrypted . |
| Password | If you selected either Plain Text or Encrypted for the password type, please enter a password for this user account. |

Table 4.23

Click **Apply** to make the configurations take effect.

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

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

The screenshot shows the 'User Accounts Settings' page with the 'Session Table' tab selected. It displays 'Total Entries : 1' and a table of active sessions:

| Type | User Name | Privilege | Login Time | IP Address |
|------|-----------|-----------|------------|-------------|
| HTTP | admin | 15 | 12:24 | 10.90.90.96 |

Figure 4.43 – Management > User Accounts Settings – Session Table

Management > Password Encryption

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

Figure 4.44 – Management > Password Encryption

The fields that can be configured for **Password Encryption** are described below:

| Item | Description |
|----------------------------------|--|
| Password Encryption State | Specify to enable or disable the password encryption. |
| Password Type | Specify the password encryption type to Encrypted-SHA1 or Encrypted-MD5. |

Table 4.24

Click **Apply** to make the configurations take effect.

Management > SNMP > SNMP Global Settings

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

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

The default SNMP global state is disabled. Select **Enable** and then select **Trap Settings**. Click **Apply** to enable the SNMP function.

Figure 4.45 – Management > SNMP > SNMP Global Settings

The fields that can be configured for **SNMP Global Settings** are described below:

| Item | Description |
|------|-------------|
|------|-------------|

| SNMP Global Settings | |
|--|--|
| SNMP Global State | Specify to enable or disable the SNMP feature. The default setting is <i>Disabled</i> . |
| SNMP Response Broadcast Request | Select to enable or disable the server to response to broadcast SNMP GetRequest packets. |
| SNMP UDP Port (0-65535) | Enter the SNMP UDP port number. The value is between 0 and 65535. |
| Trap Source Interface | Specify the interface whose IP address will be used as the source address for sending the SNMP trap packet. |
| Trap Settings | |
| Trap Global State | Enable or disable SNMP trap notifications from client devices. Disabling this option means no trap signals will be sent. When enabling this option, you may choose the type of SNMP traps to enable. |
| SNMP Authentication Trap | Tick this option to control the sending of SNMP authentication failure notifications. An authentication Failure trap 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 | Check this feature to enable Link Up traps. Whenever a device changes status from 'link down' to 'link up', it will send a Link Up trap to the management station. |
| Port Link Down | Check this feature to enable Link Down traps. Whenever a device changes status from 'link up' to 'link down', it will send a Link Down trap to the management station. |
| STP Port Status Change | Check this feature to enable STP Port Status Change traps. Whenever a device changes status from STP Port Status, it will send a STP Port Status Change trap to the management station. |
| LBV Detection | Check this feature to enable LBV Detection traps. Whenever a device does detect LBV, it will send a LBV Detection trap to the management station. |
| Firmware Upgrade | Check this feature to enable Firmware Upgrade traps. Whenever a device does do firmware upgrade, it will send a Firmware Upgrade trap to the management station. |

Table 4.25

Click **Apply** to make the configurations take effect.

Management > SNMP > SNMP View Table Settings

The SNMP View page allows user to define SNMP Views, which can be used to manage the MIB objects that are accessible to a remote SNMP manager.

SNMP View Table Settings

SNMP View Settings

View Name *

Subtree OID *

View Type

* Mandatory Field Add

Total Entries : 8

| View Name | Subtree OID | View Type | |
|---------------|--------------------|-----------|--------|
| restricted | 1.3.6.1.2.1.1 | Included | Delete |
| restricted | 1.3.6.1.2.1.11 | Included | Delete |
| restricted | 1.3.6.1.6.3.10.2.1 | Included | Delete |
| restricted | 1.3.6.1.6.3.11.2.1 | Included | Delete |
| restricted | 1.3.6.1.6.3.15.1.1 | Included | Delete |
| CommunityView | 1 | Included | Delete |
| CommunityView | 1.3.6.1.6.3 | Excluded | Delete |
| CommunityView | 1.3.6.1.6.3.1 | Included | Delete |

1/1 Go

Figure 4.46 – Management > SNMP > SNMP View Table Settings

The fields that can be configured for **SNMP View Table Settings** are described below:

| Item | Description |
|--------------------|--|
| View Name | Create a name of the view, up to 32 characters. |
| Subtree OID | The Object Identifier (OID) Subtree for the view. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager. |
| View Type | Select the OIDs that can accessed by a SNMP manager. |

Table 4.26

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

Management > SNMP > SNMP Community Table Settings

The SNMP Community page allows user to set the SNMP community string of the Switch. SNMP managers using the same community string are permitted access to the Switch's SNMP agent.

SNMP Community Table Settings

SNMP Community Table Settings

Key Type

Community Name

View Name

Access Right

Add

Total Entries : 2

| Community Name | View Name | Access Right | |
|----------------|---------------|--------------|--------|
| private | CommunityView | Read Write | Delete |
| public | CommunityView | Read Only | Delete |

1/1 Go

Figure 4.47 – Management > SNMP > SNMP Community Table Settings

The fields that can be configured for **SNMP Community Table Settings** are described below:

| Item | Description |
|------|-------------|
|------|-------------|

| | |
|-----------------------|--|
| Key Type | Select the key type for the SNMP community. Select either Plain Text or Encrypted . |
| Community Name | Select an alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent. |
| View Name | Enter an alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed access to on the Switch. The view name must exist in the SNMP View Table. |
| Access Right | Select the user's access rights from the drop-down menu: <ul style="list-style-type: none"> ◆ Read Only - SNMP community members can read the contents of the MIBs on the Switch. ◆ Read Write - SNMP community members can read and write the contents of the MIBs on the Switch. |

Table 4.27

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

Management > SNMP > SNMP Group Table Settings

The SNMP Group page allows user to manage SNMP Groups. Access to SNMP OIDs and security policies can be controlled on a per group basis.

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

Total Entries : 5

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

1/1 < << 1 >> > Go

Figure 4.48 – Management > SNMP > SNMP Group Table Settings

The fields that can be configured for **SNMP Group Table Settings** are described below:

| Item | Description |
|----------------------------------|---|
| Group Name | Enter a SNMP group name of up to 32 characters. |
| User-based Security Model | Select the SNMP security model. <ul style="list-style-type: none"> ◆ SNMPv1 - SNMPv1 does not support any security features. ◆ SNMPv2c - SNMPv2 supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. |

| | |
|-------------------------|---|
| | <ul style="list-style-type: none"> ◆ SNMPv3 - SNMPv3 provides secure access to devices through a combination of authentication and encryption. |
| Security Level | <p>This function is only available when you select SNMPv3 security level.</p> <ul style="list-style-type: none"> ◆ NoAuthNoPriv – No authorization and no encryption for packets sent between the Switch and SNMP manager. ◆ AuthNoPriv – Authorization is required, but no encryption for packets sent between the Switch and SNMP manager. ◆ AuthPriv – Both authorization and encryption are required for packets sent between the Switch and SNMP manger. |
| Read View Name | Enter a SNMP group name for users that are allowed SNMP read privileges to the Switch's SNMP agent. |
| Write View Name | Enter a SNMP group name for users that are allowed SNMP write privileges to the Switch's SNMP agent. |
| Notify View Name | Enter a SNMP group name for users that can receive SNMP trap messages generated by the Switch's SNMP agent. |

Table 4.28

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

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

Management > SNMP > SNMP Engine ID Local Settings

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

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

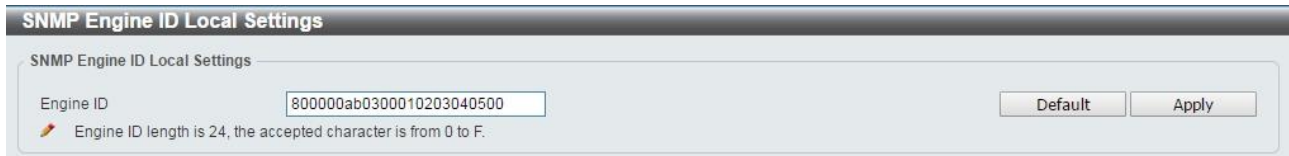


Figure 4.49 – Management > SNMP > SNMP Engine ID Local Settings

Management > SNMP > SNMP User Table Settings

The SNMP User Table Settings page allows user to manage the SNMP users that can access the Switch. It allows user to set the Group, SNMP version, and authentication and encryption type for a user.

Figure 4.50 – Management > SNMP > SNMP User Table Settings

The fields that can be configured for **SNMP User Table Settings** are described below:

| Item | Description |
|----------------------------------|---|
| User Name | Enter a SNMP user name of up to 32 characters. |
| Group Name | Enter the SNMP group of the SNMP user. |
| SNMP Version | Select the SNMP version of the user. The options to choose are v1 , v2c and v3 . |
| SNMP V3 Encryption | When selecting v3 in the SNMP Version drop-down list, this option is available. Options to choose from are None , Password , and Key . |
| Auth-Protocol by Password | Select either MD5 or SHA to be the authentication protocol. Enter a password for SNMPv3 encryption in the right column. <ul style="list-style-type: none"> ◆ MD5 – Select to use the HMAC-MD5-96 authentication level. This field will require the user to enter a password. ◆ SHA - Select that the HMAC-SHA authentication protocol will be used. This field will require the user to enter a password. |
| Priv-Protocol by Password | Select either None or DES56 and then enter a password for SNMPv3 encryption in the right column. <ul style="list-style-type: none"> ◆ None – Select to not use any authorization. ◆ DES56 – Select to use DES 56-bit encryption, based on the CBC-DES (DES-56) standard. This field will require you to enter a password. |
| Auth-Protocol by Key | Select either MD5 or SHA to be the authentication protocol. Enter a key for SNMPv3 encryption in the right column. <ul style="list-style-type: none"> ◆ MD5 – Select to use the HMAC-MD5-96 authentication level. This field will require the user to enter a key. ◆ SHA – Select to use the HMAC-SHA authentication protocol. This field will require you to enter a key. |
| Priv-Protocol by Key | Select either None or DES56 and then enter a password for SNMPv3 encryption in the right column. <ul style="list-style-type: none"> ◆ None – Select to not use any authorization. ◆ DES56 – Select to use DES 56-bit encryption, based on the CBC-DES (DES-56) standard. This field will require the user to enter a key. |

Table 4.29

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

Management > SNMP > SNMP Host Table Settings

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

Figure 4.51 – Management > SNMP > SNMP Host Table Settings

The fields that can be configured for **SNMP Host Table Settings** are described below:

| Item | Description |
|--|---|
| Host IPv4/IPv6 Address | Select IPv4 or IPv6 and specify the IP address of SNMP management host. |
| User-based Security Model | Specify the SNMP version to be used to the management host. The options are SNMPv1 , SNMPv2C and SNMPv3 . |
| Security Level | When selecting SNMPv3 in the User-based Security Model drop-down list, this option is available. <ul style="list-style-type: none"> ◆ NoAuthNoPriv – Select to have no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. ◆ AuthNoPriv – Select to require authorization, but with no encryption of packets sent between the Switch and a remote SNMP manager. ◆ AuthPriv – Select to require authorization, and packets sent between the Switch and a remote SNMP manger will be encrypted. |
| UDP Port (0-65535) | Enter the UDP port number. The default trap UDP port number is 162. The range of UDP port numbers is from 0 to 65535 . |
| Community String / SNMPv3 User Name | Enter the community string to be sent with the notification packet. |

Table 4.30

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

Management > Web

The Web page allows user to configure Web settings on the Switch.

Figure 4.52 – Management > Telnet/Web

The fields that can be configured for **Web** are described below:

| Item | Description |
|-----------------------|--|
| Port (1-65535) | Enter the TCP port number used for Telnet management of the Switch. The standard TCP port for the HTTP protocol is 80. |

Table 4.31

Click **Apply** to make the configurations take effect.

Management > Session Timeout

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

Figure 4.53 – Management > Session Timeout

The fields that can be configured for **Session Timeout** are described below:

| Item | Description |
|---------------------------------------|---|
| Web Session Timeout (60-36000) | Enter the time in seconds of the web session timeout. The range of timeout is between 60 and 36000 seconds. Tick the Default check box to use default value. The default is 180. |

Table 4.32

Click **Apply** to make the configurations take effect.

Management > D-Link Discover Protocol Settings

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

Figure 4.54 – Management > D-Link Discover Protocol Settings

The fields that can be configured for **D-Link Discover Protocol Settings** are described below:

| Item | Description |
|--|---|
| DDP Global Settings | |
| D-Link Discovery Protocol State | Select the enable or disable the D-Link Discovery Protocol state. |
| Report Timer | Specify the interval in seconds between two consecutive DDP report messages. Options to choose from are 30 , 60 , 90 , 120 , and Never . |
| DDP Port Settings | |
| From Port / To Port | Enter the appropriate port range used for the configuration. |
| State | Select to enable or disable the DDP port state. |

Table 4.33

Click **Apply** to make the configurations take effect.

L2 Features > FDB > Static FDB > Unicast Static FDB

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

Figure 4.55 – L2 Features > FDB > Static FDB > Unicast Static FDB

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

and port number.

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

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

The fields that can be configured for **Unicast Static FDB** are described below:

| Item | Description |
|---------------------|---|
| Port / Drop | Allows the selection of the port number on which the MAC address entered resides. This option could also drop the MAC address from the unicast static FDB. When selecting Port , select the switch unit and port number. |
| VID (1-4094) | Enter the VLAN ID on which the associated unicast MAC address resides. |
| MAC Address | Enter the MAC address to which packets will be statically forwarded or dropped. This must be a unicast MAC address. |

Table 4.34

Click **Apply** to make the configurations take effect.

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

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

L2 Features > FDB > Static FDB > Multicast Static FDB

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

Figure 4.56 – L2 Features > FDB > Static FDB > Multicast Static FDB

The fields that can be configured for **Multicast Static FDB** are described below:

| Item | Description |
|----------------------------|--|
| From Port / To Port | Enter the appropriate port range used for the configuration. |
| VID (1-4094) | Enter the VLAN ID of the VLAN the corresponding MAC address belongs to. |
| MAC Address | Enter the static destination MAC address of the multicast packets. This must be a multicast MAC address. The format of the destination MAC address is 01-XX-XX-XX-XX-XX. |

Table 4.35

Click **Apply** to make the configurations take effect.

Click the **Delete All** button to remove all the entries.

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

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

L2 Features > FDB > MAC Address Table Settings

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

Figure 4.57 – L2 Features > FDB > MAC Address Table Settings – Global Setting

The fields that can be configured for **MAC Address Table Settings** are described below:

| Item | Description |
|------------------------------|--|
| Aging Time | Enter the MAC address table's aging time value. This value must be between 10 and 410 seconds. Entering 0 will disable MAC address aging. By default, this value is 300 seconds. |
| Aging Destination Hit | Select to enable or disable the aging destination hit function. |

Table 4.36

Click **Apply** to make the configurations take effect.

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

Figure 4.58 – L2 Features > FDB > MAC Address Table Settings – MAC Address Learning

The fields that can be configured for **MAC Address Table Settings** are described below:

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

specified ports.

Table 4.37

Click **Apply** to make the configurations take effect.

L2 Features > FDB > MAC Address Table

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

Figure 4.59 – L2 Features > FDB > MAC Address Table

The fields that can be configured for **MAC Address Table** are described below:

| Item | Description |
|---------------------|---|
| Port | Select the port that will be used for this configuration. |
| VID (1-4094) | Enter the VLAN ID that will be used for this configuration. |
| MAC Address | Enter the MAC address that will be used for this configuration. |

Table 4.38

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

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

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

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

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

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

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

L2 Features > 802.1Q VLAN

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

Figure 4.60 – L2 Features > 802.1Q VLAN

The fields that can be configured for **802.1Q VLAN** are described below:

| Item | Description |
|---------------------|--|
| 802.1Q VLAN | |
| VID List | Enter the VLAN ID list that will be created. |
| Find VLAN | |
| VID (1-4094) | Enter the VLAN ID to be displayed. |

Table 4.39

Click **Apply** to make the configurations take effect.

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

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

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

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

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

L2 Features > Asymmetric VLAN

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

Figure 4.61 – L2 Features > Asymmetric VLAN

The fields that can be configured for **MAC Address Table** are described below:

| Item | Description |
|------------------------------|---|
| Asymmetric VLAN State | Select to enable or disable the Asymmetric VLAN function. |

Table 4.40

Click **Apply** to make the configurations take effect.

L2 Features > VLAN Interface

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

| Port | VLAN Mode | Ingress Checking | Acceptable Frame Type | Vlan Detail | Edit |
|-----------|-----------|------------------|-----------------------|-------------|------|
| eth1/0/1 | Hybrid | Enabled | Admit All | Vlan Detail | Edit |
| eth1/0/2 | Hybrid | Enabled | Admit All | Vlan Detail | Edit |
| eth1/0/3 | Hybrid | Enabled | Admit All | Vlan Detail | Edit |
| eth1/0/4 | Hybrid | Enabled | Admit All | Vlan Detail | Edit |
| eth1/0/5 | Hybrid | Enabled | Admit All | Vlan Detail | Edit |
| eth1/0/6 | Hybrid | Enabled | Admit All | Vlan Detail | Edit |
| eth1/0/7 | Hybrid | Enabled | Admit All | Vlan Detail | Edit |
| eth1/0/8 | Hybrid | Enabled | Admit All | Vlan Detail | Edit |
| eth1/0/9 | Hybrid | Enabled | Admit All | Vlan Detail | Edit |
| eth1/0/10 | Hybrid | Enabled | Admit All | Vlan Detail | Edit |

Figure 4.62 – L2 Features > VLAN Interface

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

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

| VLAN Interface Information | |
|----------------------------|-----------|
| Port | eth1/0/1 |
| VLAN Mode | Hybrid |
| Native VLAN | 1 |
| Hybrid Untagged VLAN | 1 |
| Hybrid Tagged VLAN | |
| Dynamic Tagged VLAN | |
| Ingress Checking | Enabled |
| Acceptable Frame Type | Admit All |

Back

Figure 4.63 – L2 Features > VLAN Interface – VLAN Detail

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

Configure VLAN Interface

Port: eth1/0/2

VLAN Mode: Hybrid

Acceptable Frame Type: Admit All

Ingress Checking: Enabled Disabled

Native VLAN: Native VLAN

VID (1-4094):

Action: Add

Add Mode: Untagged Tagged

Allowed VLAN Range:

Clone

From Port: eth1/0/1

To Port: eth1/0/1

Back Apply

Figure 4.64 – L2 Features > VLAN Interface – VLAN Detail

The fields that can be configured for **VLAN Interface** are described below:

| Item | Description |
|------------------------------|--|
| Port | Display the VLAN port number. |
| VLAN Mode | Select the VLAN mode option. Options to choose from are Access , Hybrid , and Trunk . |
| Acceptable Frame Type | Select the acceptable frame type behavior option. Options to choose from are Tagged Only , Untagged Only , and Admit All . |
| Ingress Checking | Select to enable or disable the ingress checking function. |
| Native VLAN | Tick the option to enable the native VLAN function. |
| VID (1-4094) | After ticking the Native VLAN check box, this option will be available. Enter the VLAN ID used for this configuration. 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. |
| Clone | Tick the Clone check box to copy the configuration to specified ports. |
| From Port / To Port | Copy the configuration of VLAN interface for specified port ranges. |

Table 4.41

Click **Apply** to make the configurations take effect.

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

L2 Features > Auto Surveillance VLAN > Auto Surveillance Properties

The Auto Surveillance Properties page 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 (1-4094)

Surveillance VLAN CoS

Aging Time (1-65535) min

Surveillance VLAN Log Enabled Disabled

Port Settings

From Port To Port State

| Port | State |
|-----------|----------|
| eth1/0/1 | Disabled |
| eth1/0/2 | Disabled |
| eth1/0/3 | Disabled |
| eth1/0/4 | Disabled |
| eth1/0/5 | Disabled |
| eth1/0/6 | Disabled |
| eth1/0/7 | Disabled |
| eth1/0/8 | Disabled |
| eth1/0/9 | Disabled |
| eth1/0/10 | Disabled |

Figure 4.65 – L2 Features > Auto Surveillance VLAN > Auto Surveillance Properties

The fields that can be configured for **Auto Surveillance Properties** are described below:

| Item | Description |
|------------------------------|--|
| Global Settings | |
| Surveillance VLAN | Specify to enable or disable the surveillance VLAN state. |
| Surveillance VLAN ID | Enter the surveillance VLAN ID. The range is from 1 to 4094. |
| Surveillance VLAN CoS | Specify the priority of the surveillance VLAN from 0 to 7. |
| Aging Time (1-65535) | Specify the aging time of the 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 counter will be reset and the timer will stop. |
| Surveillance VLAN Log | Specify to enable or disable the Surveillance VLAN log feature. |
| Port Settings | |
| From Port/To Port | Specify the port range used for the configuration. |
| State | Specify to enable or disable the state of the port. |

Table 4.42

Click **Apply** to make the configurations take effect.

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

The MAC Settings and Surveillance Device page is used to configure the user-defined surveillance device OUI and display the surveillance VLAN information.

MAC Settings and Surveillance Device

User-defined MAC Settings | Auto Surveillance VLAN Summary

To add more device(s) for Auto Surveillance VLAN by user-defined configuration as below.

Component Type: Description:

MAC Address: Mask:

Apply

Total Entries : 4

| ID | Component Type | Description | MAC Address | Mask | |
|----|----------------|------------------------|-------------------|-------------------|--------|
| 1 | Dlink | IP Surveillance Device | 28:10:7B:00:00:00 | FF:FF:FF:E0:00:00 | Delete |
| 2 | Dlink | IP Surveillance Device | 28:10:7B:20:00:00 | FF:FF:FF:F0:00:00 | Delete |
| 3 | Dlink | IP Surveillance Device | B0:C5:54:00:00:00 | FF:FF:FF:80:00:00 | Delete |
| 4 | Dlink | IP Surveillance Device | F0:7D:68:00:00:00 | FF:FF:FF:F0:00:00 | Delete |

Figure 4.66 – L2 Features > Auto Surveillance VLAN > MAC Settings and Surveillance Device

The fields that can be configured for **MAC Settings and Surveillance Device** are described below:

| Item | Description |
|-----------------------|---|
| Component Type | Specify the surveillance component type. Option to choose from are Vms , VmsClient , VideoEncoder , NetworkStorage and Other . |
| Description | Enter the description for the user-defined OUI with a maximum of 32 characters. |
| MAC Address | Enter the description for the user-defined OUI with a maximum of 32 characters. |
| Mask | Enter the OUI MAC address matching bitmask. |

Table 4.43

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

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

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

Figure 4.67 – L2 Features > Auto Surveillance VLAN > MAC Settings and Surveillance Device

L2 Features > Voice VLAN > Voice VLAN Global

The Voice VLAN is a VLAN used to carry voice traffic from an IP phone. As the sound quality of Voice over IP, is sensitive to delay Quality of service (QoS) for voice traffic should be configured to ensure that voice traffic is handled with a higher priority.

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

Figure 4.68 – L2 Features > Voice VLAN > Voice VLAN Global Settings

The fields that can be configured for **Voice VLAN Global Settings** are described below:

| Item | Description |
|-------------------------|--|
| Voice VLAN State | Select to enable or disable Voice VLAN. |
| VLAN ID (1-4094) | Enter the voice VLAN ID. The value is range from 1 to 4094. |
| Voice VLAN CoS | Specify the priority of the voice 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 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 counter will be reset and the timer will stop. |

Table 4.44

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

L2 Features > Voice VLAN > Voice VLAN Port

The Voice VLAN Port page is used to show the ports voice VLAN information.

Voice VLAN Port

Voice VLAN Port

From Port: To Port: State: Mode:

| Port | State | Mode |
|-----------|----------|---------------|
| eth1/0/1 | Disabled | Auto Untagged |
| eth1/0/2 | Disabled | Auto Untagged |
| eth1/0/3 | Disabled | Auto Untagged |
| eth1/0/4 | Disabled | Auto Untagged |
| eth1/0/5 | Disabled | Auto Untagged |
| eth1/0/6 | Disabled | Auto Untagged |
| eth1/0/7 | Disabled | Auto Untagged |
| eth1/0/8 | Disabled | Auto Untagged |
| eth1/0/9 | Disabled | Auto Untagged |
| eth1/0/10 | Disabled | Auto Untagged |

Figure 4.69 – L2 Features > Voice VLAN > Voice VLAN Port

The fields that can be configured for **Voice VLAN Port** are described below:

| Item | Description |
|----------------------------|--|
| From Port / To Port | Select the appropriate port range used for the configuration. |
| State | Specify to enable or disable the state of the port. |
| Mode | Specify the mode of the port. Options to choose from are Auto Untagged , Auto Tagged , and Manual . |

Table 4.45

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

L2 Features > Voice VLAN > Voice VLAN OUI

The Voice VLAN OUI page is used to configure the user-defined voice traffic's OUI. The OUI is used to identify 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"/> |
| 00-09-8E-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 4.70 – L2 Features > Voice VLAN > Voice VLAN OUI

The fields that can be configured for **Voice VLAN OUI** are described below:

| Item | Description |
|------|-------------|
|------|-------------|

| | |
|--------------------|---|
| OUI Address | Specify the OUI MAC address. |
| Mask | Specify the OUI MAC address matching bitmask. |
| Description | Enter the description for the user-defined OUI with a maximum of 32 characters. |

Table 4.46

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

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

L2 Features > Voice VLAN > Voice VLAN Device

The Voice VLAN Device page is used to show voice devices that are connected to the Switch. The Start Time is the time when the device was detected on the port and the Status displays the voice VLAN status of the port.

Figure 4.71 – L2 Features > Voice VLAN > Voice VLAN Device

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

The page displays the Voice VLAN LLDP-MED voice devices connected to the Switch.

Figure 4.72 – L2 Features > Voice VLAN > Voice VLAN LLDP-MED Device

L2 Features > STP > STP Global Settings

The Switch implements three versions of the Spanning Tree Protocol: Rapid Spanning Tree Protocol (RSTP) as defined by IEEE 802.1w, a version compatible with the IEEE 802.1D STP and Multiple Spanning Tree Protocol (MSTP), as defined by IEEE802.1. RSTP can operate with legacy equipment implementing IEEE 802.1D, however the advantages of using RSTP will be lost.

The Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1D STP standard and was developed in order to overcome some of the limitations of STP that impede the function of some recent switching innovations. The basic function and much of the terminology is the same and most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

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

By default, Rapid Spanning Tree is disabled. If enabled, the Switch will listen for Bridge Protocol Data Unit (BPDU) packets and its accompanying Hello packet. The BPDU packets are sent even if a BPDU packet is 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 therefore faster topology adjustment.

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

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

Figure 4.73 – L2 Features > STP > STP Global Settings

The fields that can be configured for **STP Global Settings** are described below:

| Item | Description |
|---------------------------------|---|
| STP State | |
| STP State | Select to enable or disable the Spanning Tree Protocol. |
| STP Traps | |
| STP New Root Trap | Select to enable or disable the STP new root trap option. |
| STP Topology Change Trap | Select to enable or disable the STP topology change trap option. |
| STP Mode | |
| STP Mode | Select the STP mode. The options to choose from are MSTP, RSTP and STP. |
| STP Priority | |
| Priority (0-61440) | This value is between 0 and 61440. By default, this value is 32768. The lower the value, the higher the priority. |
| STP Configuration | |
| Bridge Max Age (6-40) | Enter the bridge's maximum age value here. This value must be between 6 and 40 seconds. By default, this value is 20 seconds. The maximum age value may be set to ensure that old information does not endlessly circulate throughout the network. Set by the root bridge, this |

| | |
|-----------------------------------|--|
| | value ensures that the Switch has spanning tree configuration consistent with other devices on the LAN. |
| Bridge Forward Time (4-30) | Enter the bridge's forwarding time value. This value must be between 4 and 30 seconds. By default, this value is 15 seconds. Any port on the Switch spends this time in the listening state while moving from the blocking state to the forwarding state. |
| Max Hops (1-40) | Enter the maximum number of hops that are allowed. This value must be between 1 and 40 hops. By default, this value is 20 hops. This value is used to set the number of hops between devices in a spanning tree region before the BPDU packet sent by the Switch will be discarded. Each switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BPDU packet and the information held for the port will age out. |
| Bridge Hello Time (0-2) | After selecting RSTP/STP as the STP Mode , this parameter will be available. Enter the bridge's hello time value here. This value must be between 1 and 2 seconds. By default, this value is 2 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to all switches. This field will only appear when STP or RSTP is selected for the STP Version. For MSTP, the Hello Time must be set on a port by port basis. |
| TX Hop Count (1-10) | Enter the transmit hold count value. This value must be between 1 and 10. The default value is 6. This value is used to set the maximum number of Hello packets transmitted per interval. |

Table 4.47

Click **Apply** to make the configurations take effect.

L2 Features > STP > STP Port Settings

In addition to setting spanning tree parameters for use on the switch level, the Switch allows for the configuration of STP on a port level. Groups of ports can be configured in a port group, each of which can have its own spanning tree instance and configuration settings.

Port level spanning tree works in the same way as switch level spanning tree, but the root bridge is replaced with a root port. A root port in the group, which is elected based on port priority and port cost, and is 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.

STP Port Settings

STP Port Settings

From Port: To Port:

Cost (1-200000000, 0=Auto): State: Guard Root:

Link Type: Port Fast: TCN Filter:

BPDU Forward: Priority: Hello Time (1-2): sec

| Port | State | Cost | Guard Root | Link Type | Port Fast | TCN Filter | BPDU Forward | Priority |
|-----------|----------|-------------|------------|-------------|---------------|------------|--------------|----------|
| eth1/0/1 | Disabled | 0/200000000 | Disabled | Auto/Shared | Non-Edge/N... | Disabled | Enabled | 128 |
| eth1/0/2 | Disabled | 0/200000000 | Disabled | Auto/P2P | Non-Edge/N... | Disabled | Enabled | 128 |
| eth1/0/3 | Disabled | 0/200000000 | Disabled | Auto/Shared | Non-Edge/N... | Disabled | Enabled | 128 |
| eth1/0/4 | Disabled | 0/200000000 | Disabled | Auto/Shared | Non-Edge/N... | Disabled | Enabled | 128 |
| eth1/0/5 | Disabled | 0/200000000 | Disabled | Auto/Shared | Non-Edge/N... | Disabled | Enabled | 128 |
| eth1/0/6 | Disabled | 0/200000000 | Disabled | Auto/Shared | Non-Edge/N... | Disabled | Enabled | 128 |
| eth1/0/7 | Disabled | 0/200000000 | Disabled | Auto/Shared | Non-Edge/N... | Disabled | Enabled | 128 |
| eth1/0/8 | Disabled | 0/200000000 | Disabled | Auto/Shared | Non-Edge/N... | Disabled | Enabled | 128 |
| eth1/0/9 | Disabled | 0/200000000 | Disabled | Auto/P2P | Non-Edge/N... | Disabled | Enabled | 128 |
| eth1/0/10 | Disabled | 0/200000000 | Disabled | Auto/P2P | Non-Edge/N... | Disabled | Enabled | 128 |

Figure 4.74 – L2 Features > STP > STP Port Settings

The fields that can be configured for **STP Port Settings** are described below:

| Item | Description |
|--------------------------|---|
| From Port/To Port | Enter a consecutive group of ports to be configured starting with the selected port. |
| Cost | <p>This is the STP port cost, which is used to calculate the spanning tree topology. It represents the relative interface bandwidth and is the desirability of the link. The port cost can be set automatically or set manually as a metric value. The default value is 0 (auto).</p> <ul style="list-style-type: none"> ♦ 0 (auto): Setting 0 for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000. ♦ Value 1-200000000: Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets. |
| State | Select to enable or disable port based STP. It will be selectable after STP is enabled globally on the Switch. |
| Guard Root | Select to enable or disable the guard root function. |
| Link Type | Select the link type option. The options to choose from are Auto , P2P , and Shared . A full-duplex port is considered to have a point-to-point (P2P) connection. A half-duplex port is considered to have a Shared connection. The port cannot rapidly transition to the forwarding state if the link type is set to Shared . By default this option is Auto . |
| Port Fast | Select the port fast option. The options are Disabled and Edge . In the Disabled mode, the port will always be in the non-port fast state. It will wait for the forward-time delay to change to the forwarding state. In the Edge mode, the port will directly change to the forwarding state without waiting for the forward-time delay. If the interface receives a BPDU, its operation state changes to the non-port fast state. |

| | |
|---------------------|--|
| TCN Filter | Select to enable or disable the TCN filter option. Enabling TCN filtering on a port is useful for connecting to an external network, which may not be under full control of the administrator. When a port is set to the TCN filter mode, the topology change event received by the port will be ignored. By default, this option is disabled. |
| BPDU Forward | Bridges use Bridge Protocol Data Units (BPDUs) in the operation of spanning tree, BPDU. Forwarding is useful when a bridge interconnects two regions, with each region requiring a separate spanning tree. BPDU filtering functions only when STP is disabled either globally or on a single interface. The possible field values are: <ul style="list-style-type: none"> ♦ Disabled: BPDU filtering is enabled on the port. ♦ Enabled: BPDU forwarding is enabled on the port (STP must be disabled). |
| Priority | Select the priority of each port. Selectable range is from 0 to 240, and the default setting is 128. The lower the number, the greater the probability the port will be chosen as a root port. |
| Hello Time | The interval between two transmissions of BPDU packets sent by the Root Bridge to indicate to all other switches that it is indeed the Root Bridge. The default value is 2. |

Table 4.48

Click **Apply** to make the configurations take effect.

L2 Features > STP > MST Configuration Identification

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

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

Figure 4.75 – L2 Features > STP > MST Configuration Identification

The fields that can be configured for **MST Configuration Identification** are described below:

| Item | Description |
|---|--|
| MST Configuration Identification | |
| Configuration Name | Enter a name set on the switch to uniquely identify the MSTI (multiple |

| | |
|----------------------------------|---|
| | spanning tree instance). If a configuration name is not set, this field shows the MAC address of the device running MSTP. |
| Revision Level(0 - 65535) | This value, together with the configuration name and identical VLANs mapped for STP instance IDs identifies the MST region configured on the switch. |
| Instance ID Settings | |
| Instance ID (1 - 64) | Enter the MSTI ID associated with the VID List. The possible field range is 1-64. |
| Action | Action: The possible values are: <ul style="list-style-type: none"> ♦ Add VID - Indicates that the edit type is add. ♦ Remove VID - Indicates that the edit type is removed. |
| VID List | Enter the VID range from configured VLANs set on the Switch. |

Table 4.49

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

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

L2 Features > STP > STP Instance

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

| Total Entries : | | |
|-----------------|----------------|-------------------|
| Instance | Instance State | Instance Priority |
| CIST | Disabled | 32768 |

| Instance CIST | |
|---|-----------------------|
| | Instance Global Info |
| Bridge Address | 00-01-02-03-04-05 |
| 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 4.76 – L2 Features > STP > STP Instance

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

L2 Features > STP > MSTP Port Information

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

| Instance ID | Cost | Priority | Status | Role |
|-------------|-----------|----------|----------|----------|
| CIST | 200000000 | 128 | Disabled | Disabled |

Figure 4.77 – L2 Features > STP > MSTP Port Information

The fields that can be configured for **MSTP Port Information** are described below:

| Item | Description |
|------|------------------------------|
| Port | Select the port to be fined. |

Table 4.50

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

Click **Find** to search the MSTP port information.

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

L2 Features > ERPS(G.8032) > ERPS

ERPS (Ethernet Ring Protection Switching) is the first industry standard (ITU-T G.8032) for Ethernet ring protection switching. It is achieved by integrating mature Ethernet Operations, Administration, and Maintenance (OAM)* functions and a simple automatic protection switching (APS) protocol for Ethernet ring networks. ERPS provides sub-50ms failover for Ethernet traffic in a ring topology. It ensures that there are no loops formed at the Ethernet layer.

One link within a ring, the ring Protection Link (RPL), will be blocked to avoid a Layer 2 loop. When there is a failure, protection switching blocks the failed link and unblocks the RPL. When the failure clears, protection switching blocks the RPL again and unblocks the link on which the failure is cleared.

The ERPS page allows user to configure the ERPS instance and profile configuration of the Switch.

The screenshot shows the ERPS configuration interface. At the top, it says "ERPS" and "Ethernet Ring G.8032". Below that, there is a text input field for "Instance ID(1-16)" and an "Apply" button. Underneath, it says "Total Entries :". Below that is a table with two columns: "Instance ID" and "Ethernet Ring". The table is currently empty, with the text "<< Table is empty >>" at the bottom.

Figure 4.78 – L2 Features > ERPS(G.8032) > ERPS

The fields that can be configured for **ERPS** are described below:

| Item | Description |
|--------------------|--|
| Instance ID (1-16) | Specify the Instance ID to be created. |

Table 4.51

Click **Apply** to make the configurations take effect.



NOTE: STP and LBD should be disabled on the ring ports before enabling ERPS.

Enter **Instance ID** 1 and click **Apply** to create ERPS physical ring. Then the following page will be displayed.

The screenshot shows the ERPS configuration interface after creating an instance. It says "ERPS" and "Ethernet Ring G.8032". Below that, there is a text input field for "Instance ID(1-16)" and an "Apply" button. Underneath, it says "Total Entries : 1". Below that is a table with three columns: "Instance ID", "Ethernet Ring", and "Actions". The table has one row with "1" in the "Instance ID" column, "Ring1" in the "Ethernet Ring" column, and "Edit Instance", "Show Status", and "Delete" buttons in the "Actions" column.

Figure 4.79 – L2 Features > ERPS(G.8032) > ERPS - Create

Click **Edit Instance** button to modify the ERP instance, click **Show Status** button to display the ERPS physical ring's status information, or click **Delete** button to remove the Ethernet instance.

Click **Edit Instance** to modify the Ethernet Instance configuration:

Figure 4.80 – L2 Features > ERPS(G.8032) > ERPS – Edit Instance

The fields that can be configured for edit **ERPS** are described below:

| Item | Description |
|------------------------------------|---|
| Ethernet Ring Name | Enter the Ethernet ring name for the specified instance. |
| Sub Ring Name | Enter the sub ring name of a physical ring. |
| Port0 | Specifies the port as the first ring port and also specifies the virtual port channel used. |
| Port1 | Specifies the port as the second ring port and also specifies the virtual port channel used. |
| Description | Enter the description for the specified instance. |
| R-APS Channel VLAN (1-4094) | Specifies the R-APS channel of ERP instance. The range is between 1 and 4094. |
| Inclusion VLAN List | Specifies to add or delete the inclusion VLAN group. The VLANs specified here will be protected by the ERP mechanism. |
| MEL(0-7) | Specifies the ring MEL of the R-APS function. The default ring MEL is 1. |
| Profile Name | Specifies the profile name of Ethernet Instance. |
| RPL Port | Specifies the RPL port used. Options to choose from are Port0, Port1, and None. |
| RPL Owner | Specifies to enable or disable the RPL owner node. |
| Active | Specifies enable or disable to active this ERP instance. |

Table 4.52

Click **Apply** to make the configurations take effect.

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

Click **Show Status** button to display the ERPS status information.

ERPS Status

ERPS Status Information

| | |
|----------------------|-------------|
| Instance ID | 1 |
| Ethernet Ring | Ring1 |
| Description | |
| MEL | 0 |
| R-APS Channel | 0 |
| Protected VLAN | |
| Profile | |
| Guard Timer | 500 ms |
| Hold-Off Timer | 0 ms |
| WTR Timer | 5 min |
| Revertive | Enabled |
| Instance State | Deactivated |
| Admin RPL | none |
| Operational RPL | none |
| Port0 State | Forwarding |
| Port1 State | Forwarding |
| Admin RPL Port | none |
| Operational RPL Port | none |

Back

Figure 4.81 – L2 Features > ERPS(G.8032) > ERPS – Show Status

L2 Features > ERPS(G.8032) > ERPS Profile

The ERPS Profile page allows user to configure the ERPS profile information of the Switch.

ERPS Profile

Ethernet Ring G.8032 Profile

Profile Name Apply Delete

Total Entries :

| Profile | Instance ID | Status | Port Status |
|----------------------|-------------|--------|-------------|
| << Table is empty >> | | | |

Figure 4.82 – L2 Features > ERPS(G.8032) > ERPS Profile

The fields that can be configured for **ERPS Profile** are described below:

| Item | Description |
|---------------------|---|
| Profile Name | Specify the profile name to be created on the Switch. |

Table 4.53

Click **Apply** to make the configurations take effect.

Click the **Delete** button to remove the profile.

Enter **Profile Name** and click **Apply** button to associate the G.8032 profile with the ERP instance created.

ERPS Profile

Ethernet Ring G.8032 Profile

Profile Name Apply Delete

Total Entries : 1

| Profile | Instance ID | Status | Port Status |
|---------|-------------|--------|-------------|
| erps1 | | | Edit |

Figure 4.83 – L2 Features > ERPS(G.8032) > ERPS Profile - created

Click **Edit** button to configure the Ethernet Profile settings:

Figure 4.84 – L2 Features > ERPS(G.8032) > ERPS Profile - Edit

The fields that can be configured for edit **ERPS Profile** are described below:

| Item | Description |
|---------------------------------|--|
| Revertive | Specifies whether to enable or disable to the original state after a failure, for example, when the RPL was blocked. |
| Guard Time (10-2000) | Specifies the guard time of the R-APS function. The value is between 10 and 2000 milliseconds. The default guard time is 500 milliseconds. |
| Hold-Off Timer (0-10000) | Specifies the hold-off time of the R-APS function. The value is between 0 and 10000 milliseconds. The default hold-off time is 0 milliseconds. |
| WTR Timer (1-12) | Specifies the WTR time of the R-APS function. The value is between 1 and 12 minutes. The default WTR time is 5 minutes. |

Table 4.54

Click **Apply** to make the configurations take effect.

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

L2 Features > Loopback Detection

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

Loopback Detection

Loopback Detection Global Settings

Loopback Detection State: Mode:
 Enabled VLAN ID List: Interval (1-32767):
 Trap State: Action:

Loopback Detection Port Settings

From Port: To Port: State:

| Port | Loopback Detection State | Result | Time Left (sec) |
|-----------|--------------------------|--------|-----------------|
| eth1/0/1 | Disabled | Normal | 0 |
| eth1/0/2 | Disabled | Normal | 0 |
| eth1/0/3 | Disabled | Normal | 0 |
| eth1/0/4 | Disabled | Normal | 0 |
| eth1/0/5 | Disabled | Normal | 0 |
| eth1/0/6 | Disabled | Normal | 0 |
| eth1/0/7 | Disabled | Normal | 0 |
| eth1/0/8 | Disabled | Normal | 0 |
| eth1/0/9 | Disabled | Normal | 0 |
| eth1/0/10 | Disabled | Normal | 0 |

Figure 4.85 – L2 Features > Loopback Detection Settings

The fields that can be configured for **Loopback Detection Settings** are described below:

| Item | Description |
|---|--|
| Loopback Detection Global Settings | |
| Loopback Detection State | Enable or disable loopback detection. The default is <i>disabled</i> . |
| Mode | Select either Port-based or VLAN-based loopback detection. |
| Enabled VLAN ID List | Enter the VLAN ID for loopback detection. This only takes effect when VLAN-based is selected in the Mode drop-down list. |
| Interval (1-32767) | Set a Loop Detection Interval between 1 and 32767 seconds. The default is 2 seconds. |
| Trap State | Select to enable or disable the loopback detection trap state. |
| Action | Select Shut-down or None for loopback detection. |
| Loopback Detection Port Settings | |
| From Port / To Port | Enter a consecutive group of ports to be configured starting with the selected port. |
| From Port / To Port | Use the drop-down menu to toggle between <i>Enabled</i> and <i>Disabled</i> . Default is <i>disabled</i> . |

Table 4.55

Click **Apply** to make the configurations take effect.

L2 Features > Link Aggregation

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

Figure 4.86 – L2 Features > Link Aggregation

The fields that can be configured for **Link Aggregation** are described below:

| Item | Description |
|----------------------------------|---|
| Link Aggregation Settings | |
| System Priority (1-65535) | Enter the system's priority value. This must be between 1 and 65535. By default, the value is 32768. The system priority determines which ports can join a port-channel and which ports are put in stand-alone mode. The lower value has a higher priority. If two or more ports have the same priority, the port number determines the priority. |
| Load Balance Algorithm | Specify the load balancing algorithm that will be used. Options to choose from are: Source MAC , Destination MAC , Source Destination MAC , Source IP , Destination IP , and Source Destination IP . By default, this option is Source MAC . System ID: The System ID information. |
| Channel Group Information | |
| From Port / To Port | Select the appropriate port range used for the configuration. Group ID: Enter the channel-group number. This value must be between 1 and 32. The system will automatically create the port-channel when a physical port first joins a channel-group. An interface can only join one channel-group. |
| Mode | Select either On , Active , or Passive . If you selected On , the channel-group type is static. If Active or Passive is selected, the channel-group type is LACP. A channel-group can only consist of either static members or LACP members. Once the type of channel-group has been determined, other types of interfaces cannot join the channel-group. |

Table 4.56

Click **Apply** to make the configurations take effect.

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

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

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

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

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

With Internet Group Management Protocol (IGMP) snooping, the DMS-1100 Series Switch can make intelligent multicast forwarding decisions by examining the contents of each frame's Layer 2 MAC header.

IGMP snooping can help reduce cluttered traffic on the LAN. With IGMP snooping enabled globally, the DMS-1100 Series Switch will forward multicast traffic only to connections that have group members attached.

The settings of IGMP snooping is set by each VLAN individually.

Figure 4.87 – L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Settings

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

| Item | Description |
|-----------------------------|--|
| Global Settings | |
| Global State | Select to enable or disable the IGMP Snooping global state. |
| VLAN Status Settings | |
| VID (1-4094) | Enter the VLAN ID and select to enable or disable the IGMP snooping on the VLAN. |
| IGMP Snooping Table | |
| VID (1-4094) | Enter the VLAN ID between 1 and 4094. |

Table 4.57

Click **Apply** to make the configurations take effect.

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

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

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

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

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

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

IGMP Snooping VLAN Parameters

| IGMP Snooping VLAN Parameters | |
|-------------------------------|----------------------|
| VID | 1 |
| Status | Enabled |
| Fast Leave | Disabled(host-based) |
| Querier State | Disabled |
| Query Version | v3 |
| Query Interval | 125 seconds |
| Max Response Time | 10 seconds |
| Robustness Value | 2 |
| Last Member Query Interval | 1 seconds |

Figure 4.88 – L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping – Show Detail

Click the **Modify** button to edit the information in the following window:

IGMP Snooping VLAN Settings

| IGMP Snooping VLAN Parameters | |
|-----------------------------------|---|
| VID (1-4094) | 1 |
| Status | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled |
| Fast Leave | <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled |
| Querier State | <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled |
| Query Version | 3 ▾ |
| Query Interval (1-31744) | <input type="text" value="125"/> sec |
| Max Response Time (1-25) | <input type="text" value="10"/> sec |
| Robustness Value (1-7) | <input type="text" value="2"/> |
| Last Member Query Interval (1-25) | <input type="text" value="1"/> sec |

Figure 4.89 L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping – Modify

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

| Item | Description |
|-----------------------------------|---|
| Fast Leave | Select to enable or disable the IGMP snooping fast leave function. |
| Querier State | Select to enable or disable the querier state. |
| Query Version | Select the general query packet version sent by the IGMP snooping querier. |
| Query Interval (1-31744) | Enter the interval at which the IGMP snooping querier sends IGMP general query messages periodically. |
| Max. Response Time (1-25) | Enter the interval at which the IGMP snooping querier sends IGMP general query messages periodically. |
| Robustness Value (1-7) | Enter the robustness variable used in IGMP snooping. |
| Last Member Query Interval | Enter the interval at which the IGMP snooping querier sends IGMP |

| | |
|--------|---|
| (1-25) | group-specific or group-source-specific query messages. |
|--------|---|

Table 4.58

Click **Apply** to make the configurations take effect.

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

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

Figure 4.90 – L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Group Settings

The fields that can be configured for edit **IGMP Snooping Group Settings** are described below:

| Item | Description |
|----------------------------|---|
| VID (1-4094) | Enter the VLAN ID. |
| Group Address | Enter the IP multicast group address. |
| From Port / To Port | Select the range of ports to be configured. |

Table 4.59

Click **Apply** to make the configurations take effect.

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

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

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

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

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

| Item | Description |
|----------------------|---------------------------------------|
| VID (1-4094) | Specify the VLAN ID. |
| Group Address | Enter the IP multicast group address. |

Table 4.60

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

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

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

The IGMP Snooping Mrouter Settings page allows user to configure interfaces as multicast router ports or ports that cannot be multicast router ports on the Switch.

Figure 4.91 – L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Mrouter Settings

The fields that can be configured for **IGMP Snooping Mrouter Settings** are displayed below:

| Item | Description |
|----------------------------|--|
| VID (1-4094) | Enter the VLAN ID in the range 1 to 4094. |
| Configuration | Select the port configuration type. <ul style="list-style-type: none"> ◆ Port: Select to configure the port as a static multicast router port. ◆ Forbidden Port: Select to configure the port as a port that cannot be a static multicast router port. |
| From Port / To Port | Select the range of ports to be configured. |

Table 4.61

Click **Apply** to make the configurations take effect.

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

The fields that can be configured for **IGMP Snooping Mrouter Table** are displayed below:

| Item | Description |
|---------------------|-----------------------------------|
| VID (1-4094) | Enter the VLAN ID to be searched. |

Table 4.62

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

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

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

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

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

Figure 4.92 – L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Statistics Settings

The fields that can be configured for **IGMP Snooping Statistics Settings** are displayed below:

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

Table 4.63

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

The fields that can be configured for **IGMP Snooping Statistics Table** are displayed below:

| Item | Description |
|---------------------|--|
| Find Type | Select the interface to be searched. The options are VLAN and Port . |
| VID (1-4094) | Enter the VLAN ID. |

Table 4.64

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

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

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

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

Figure 4.93 – L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Setting

The fields that can be configured for **MLD Snooping Settings** are described below:

| Item | Description |
|-----------------------------|---|
| Global Settings | |
| Global State | Select to enable or disable the MLD Snooping state. |
| VLAN Status Settings | |
| VID (1-4094) | Enter the VLAN ID and select to enable or disable MLD snooping on the VLAN. |
| MLD Snooping Table | |
| VID (1-4094) | Enter the VLAN ID to be searched. |

Table 4.65

Click **Apply** to make the configurations take effect.

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

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

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

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

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

The screenshot shows a window titled "MLD Snooping VLAN Parameters". Inside the window, there is a table of parameters and their values:

| MLD Snooping VLAN Parameters | |
|------------------------------|-----------------------|
| VID | 1 |
| Status | Enabled |
| Fast Leave | Disabled |
| Querier State | Disabled (Non-active) |
| Query Version | v2 |
| Query Interval | 125 seconds |
| Max Response Time | 10 seconds |
| Robustness Value | 2 |
| Last Member Query Interval | 2 seconds |

At the bottom right of the window, there is a button labeled "Modify".

Figure 4.94 – L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Setting – Show Detail

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

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

Figure 4.95 – L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Setting – Edit

The fields that can be configured for **MLD Snooping Settings** are displayed below:

| Item | Description |
|--|--|
| Fast Leave | Select to enable or disable the MLD snooping fast leave function. |
| Querier State | Select to enable or disable the querier state. |
| Query Version | Select the general query packet version sent by the MLD snooping querier. |
| Query Interval (1-31744) | Enter the interval at which the MLD snooping querier sends MLD general query messages periodically. |
| Max. Response Time (1-25) | Enter the maximum response time, in seconds, advertised in MLD snooping queries. The range is 1 to 25. |
| Robustness Value (1-7) | Enter the robustness variable used in MLD snooping. |
| Last Member Query Interval (1-25) | Enter the interval at which the MLD snooping querier sends MLD group-specific or group-source-specific (channel) query messages. |

Table 4.66

Click **Apply** to make the configurations take effect.

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

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

Figure 4.96 – L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Group Settings

The fields that can be configured for **MLD Snooping Group Settings** are displayed below:

| Item | Description |
|----------------------------|---|
| VID (1-4094) | Enter the VLAN ID. |
| Group Address | Enter the IP multicast group address. |
| From Port / To Port | Select the range of ports to be configured. |

Table 4.67

Click **Apply** to make the configurations take effect.

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

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

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

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

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

| Item | Description |
|----------------------------|---|
| VID (1-4094) | Enter the VLAN ID. |
| Group Address | Enter the IP multicast group address. |
| From Port / To Port | Select the range of ports to be configured. |

Table 4.68

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

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

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

The MLD Snooping Mrouter Settings page allows user to configure the interfaces as router ports or ports that cannot be multicast router ports on the Switch.

Figure 4.97 – L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Mrouter Settings

The fields that can be configured for the **MLD Snooping Mrouter Table** are described below:

| Item | Description |
|----------------------------|--|
| VID (1-4094) | Enter the VLAN ID. |
| Configuration | Select the port configuration type. <ul style="list-style-type: none"> ◆ Port: Select to configure the port as being connected to a multicast-enabled router. |
| From Port / To Port | Select the range of ports to be configured. |

Table 4.69

Click **Apply** to make the configurations take effect.

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

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

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

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

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

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

Figure 4.98 – L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Statistics Settings

The fields that can be configured for the **MLD Snooping Statistics Settings** are described below:

| Item | Description |
|---------------------|--|
| Statistics | Select the type of statistics to display. Available options are All and VLAN . |
| VID (1-4094) | Enter the VLAN ID to be specified. |

Table 4.70

Click the **Clear** button to remove the entries.

The fields that can be configured to display the **MLD Snooping Statistics Table** are described below:

| Item | Description |
|---------------------|---|
| Find Type | Select the type to find the statistics table. |
| VID (1-4094) | Enter the VLAN ID to be displayed. |

Table 4.71

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

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

L2 Features > LLDP > LLDP Global Settings

Link Layer Discovery Protocol (LLDP) is an IEEE 802.1AB standards-compliant 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 for each LLDP device. The LLDP function is enabled by default.

LLDP Global Settings

LLDP Global Settings

LLDP State Enabled Disabled

LLDP Forward State Enabled Disabled

LLDP Trap State Enabled Disabled

LLDP-MED Trap State Enabled Disabled Apply

LLDP-MED Configuration

Fast Start Repeat Count (1-10) times Apply

LLDP Configurations

Message TX Interval (5-32768) sec

Message TX Hold Multiplier (2-10)

Reinit Delay (1-10) sec

TX Delay (1-8192) sec Apply

LLDP System Information

Chassis ID Subtype MAC Address

Chassis ID 00-50-43-3E-3E-3E

System Name Switch

System Description DMS-1100-10TP 2.5GbE Smart Managed Switch

System Capabilities Supported Repeater,Bridge

System Capabilities Enabled Repeater,Bridge

LLDP-MED System Information

Device Class Network Connectivity

Hardware Revision A1

Firmware Revision 1.00.001

Software Revision V1.00.002

Serial Number QQDMS12345600

Figure 4.99 – L2 Features > LLDP > LLDP Global Settings

The fields that can be configured for **LLDP Global Settings** are described below:

| Item | Description |
|--|---|
| LLDP Global Settings | |
| LLDP State | Select to enable or disable LLDP globally on the Switch. With this enabled, the Switch will transmit receive and process LLDP packets. |
| LLDP Forward State | Select 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 to enable or disable the LLDP trap state. |
| LLDP-MED Trap State | Select to enable or disable the LLDP-MED trap state. |
| LLDP-MED Configuration | |
| Fast Start Repeat Count (1-10) | Enter the LLDP-MED fast start repeat count value. This value must be between 1 and 10. |
| LLDP Configurations | |
| Message TX Interval (5-32768) | This parameter indicates the interval at which LLDP frames are transmitted on behalf of this LLDP agent. The default value is 30 seconds. |
| Message TX Hold Multiplier (2-10) | This parameter is a multiplier that determines the actual TTL value used in an LLDPDU. The default value is 4. |
| LLDP Reinit Delay (1-10) | This parameter indicates the amount of delay from the time adminStatus becomes disabled until re-initialization is attempted. The default value is 2 seconds. |
| LLDP TX Delay (1-8192) | This parameter indicates the delay between successive LLDP frame transmissions initiated by value or status changes in the LLDP local systems MIB. The value for txDelay is set by the following range formula: $1 < \text{txDelay} < (0.25 \times \text{msgTxInterval})$. The default value is 2 seconds. |

Table 4.72

Click **Apply** to make the configurations take effect.

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: eth1/0/1 To Port: eth1/0/1 Subtype: Local Admin State: TX and RX IP Subtype: IPv4 Action: Remove Address: . . .

Note: The address should be the switch's address. Apply

| Port | Subtype | Admin State | IPv4 (IPv6) Address |
|-----------|---------|-------------|---------------------|
| eth1/0/1 | Local | TX and RX | |
| eth1/0/2 | Local | TX and RX | |
| eth1/0/3 | Local | TX and RX | |
| eth1/0/4 | Local | TX and RX | |
| eth1/0/5 | Local | TX and RX | |
| eth1/0/6 | Local | TX and RX | |
| eth1/0/7 | Local | TX and RX | |
| eth1/0/8 | Local | TX and RX | |
| eth1/0/9 | Local | TX and RX | |
| eth1/0/10 | Local | TX and RX | |

Figure 4.100 – L2 Features> LLDP > LLDP Port Settings

The fields that can be configured for the **LLDP Port Settings** are described below:

| Item | Description |
|---------------------------|---|
| From Port/ To Port | Select the range of ports to be configured. |
| Subtype | Select the subtype of LLDP Type Length Value (TLV). Options to choose from are MAC Address , and Local . |
| Admin Status | Select the LLDP transmission mode on the port. The available options are: <ul style="list-style-type: none"> ◆ TX: Enables transmitting LLDP packets only. ◆ RX: Enables receiving LLDP packets only. ◆ TX and RX: Enables transmitting and receiving LLDP packets. This is the default value. ◆ Disabled: Disables LLDP on the port. |
| IP Subtype | Select the type of the IP address information to be sent. Options to choose from are All , IPv4 and IPv6 . |
| Action | Select to remove or add the action field. |
| Address | Enter the IP address to be sent. |

Table 4.73

Click **Apply** to make the configurations take effect.

L2 Features > LLDP > LLDP Management Address List

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

LLDP Management Address List

All Find

| Subtype | Address | IF Type | OID | Advertising Ports |
|---------|-------------|---------|---------------------|-------------------|
| IPv4 | 10.90.90.90 | lindex | 1.3.6.1.2.1.2.2.1.1 | - |

Figure 4.101 – L2 Features > LLDP > LLDP Management Address List

The fields that can be displayed for the **LLDP Management Address List** are described below:

| Item | Description |
|---------------------------|---|
| Management Address | Select IPv4, IPv6 or All address to be displayed. |
| Subtype | Displays the managed address subtype (e.g. MAC or IPv4) |
| Address | Displays the IP address. |
| IF Type | Displays the IF Type. |
| OID | Displays the SNMP OID. |
| Advertising Ports | Displays the advertising ports. |

Table 4.74

Click **Find** and the table will update and display the values required.

L2 Features > LLDP > LLDP Basic TLVs Settings

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

LLDP Basic TLVs Settings

From Port: eth1/0/1 To Port: eth1/0/1 Port Description: Disabled System Name: Disabled System Description: Disabled System Capabilities: Disabled

| Port | Port Description | System Name | System Description | System Capabilities |
|-----------|------------------|-------------|--------------------|---------------------|
| eth1/0/1 | Disabled | Disabled | Disabled | Disabled |
| eth1/0/2 | Disabled | Disabled | Disabled | Disabled |
| eth1/0/3 | Disabled | Disabled | Disabled | Disabled |
| eth1/0/4 | Disabled | Disabled | Disabled | Disabled |
| eth1/0/5 | Disabled | Disabled | Disabled | Disabled |
| eth1/0/6 | Disabled | Disabled | Disabled | Disabled |
| eth1/0/7 | Disabled | Disabled | Disabled | Disabled |
| eth1/0/8 | Disabled | Disabled | Disabled | Disabled |
| eth1/0/9 | Disabled | Disabled | Disabled | Disabled |
| eth1/0/10 | Disabled | Disabled | Disabled | Disabled |

Figure 4.102 – L2 Features > LLDP > LLDP Basic TLVs Settings

The fields that can be configured for the **LLDP Basic TLVs Settings** are described below:

| Item | Description |
|----------------------------|--|
| From Port / To Port | Select the range of ports to be configured. |
| Port Description | Select to enable or disable the Port Description option. |
| System Name | Select the system name to be enabled or disabled in the LLDP port. If enabled is selected, users can specify the content of the system Name. |
| System Description | Select to enable or disable the System Description option. |
| System Capabilities | Select to enable or disable the System Capabilities option. |
| Advertising Ports | Displays the advertising ports. |

Table 4.75

Click **Apply** to make the configurations take effect.

L2 Features > LLDP > LLDP Dot1 TLVs Settings

This LLDP Dot1 TLVs Settings page allows user 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: eth1/0/1 To Port: eth1/0/1 Port VLAN: Disabled Protocol VLAN: Disabled VLAN Name: Disabled Protocol Identity: Disabled None

Apply

| Port | Port VLAN ID | Enabled Port and Protocol VID | Enabled VLAN Name | Enabled Protocol Identity |
|-----------|--------------|-------------------------------|-------------------|---------------------------|
| eth1/0/1 | Disabled | | | |
| eth1/0/2 | Disabled | | | |
| eth1/0/3 | Disabled | | | |
| eth1/0/4 | Disabled | | | |
| eth1/0/5 | Disabled | | | |
| eth1/0/6 | Disabled | | | |
| eth1/0/7 | Disabled | | | |
| eth1/0/8 | Disabled | | | |
| eth1/0/9 | Disabled | | | |
| eth1/0/10 | Disabled | | | |

Figure 4.103 – L2 Features > LLDP > LLDP Dot1 TLVs Settings

The fields that can be configured for the **LLDP Dot1 TLVs Settings** are described below:

| Item | Description |
|----------------------------|---|
| From Port / To Port | Select the range of ports to be configured. |
| Port VLAN | Select to enable or disable the port VLAN ID TLV to send. The Port VLAN ID TLV is an optional fixed length TLV that allows a VLAN bridge port to advertise the port's VLAN identifier (PVID) that will be associated with untagged or priority tagged frames. |
| Protocol VLAN | Select to enable or disable Port and Protocol VLAN ID (PPVID) TLV to send, and enter the VLAN ID in PPVID TLV. |
| VLAN Name | Select to enable or disable the VLAN name TLV to send, and enter the ID of the VLAN in the VLAN name TLV. |
| Protocol Identity | Select to enable or disable the Protocol Identity TLV to send, and the protocol name. Options for protocol name to choose from are None , EAPOL , LACP , GVRP , STP , and All . |

Table 4.76

Click **Apply** to make the configurations take effect.

L2 Features > LLDP > LLDP Dot3 TLVs Settings

The LLDP Dot3 TLVs Settings page allows user 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: eth1/0/1 To Port: eth1/0/1 MAC/PHY Configuration/Status: Disabled Link Aggregation: Disabled Maximum Frame Size: Disabled Power Via MDI: Disabled

| Port | MAC/PHY Configuration/Status | Link Aggregation | Maximum Frame Size | Power Via MDI |
|-----------|------------------------------|------------------|--------------------|---------------|
| eth1/0/1 | Disabled | Disabled | Disabled | Disabled |
| eth1/0/2 | Disabled | Disabled | Disabled | Disabled |
| eth1/0/3 | Disabled | Disabled | Disabled | Disabled |
| eth1/0/4 | Disabled | Disabled | Disabled | Disabled |
| eth1/0/5 | Disabled | Disabled | Disabled | Disabled |
| eth1/0/6 | Disabled | Disabled | Disabled | Disabled |
| eth1/0/7 | Disabled | Disabled | Disabled | Disabled |
| eth1/0/8 | Disabled | Disabled | Disabled | Disabled |
| eth1/0/9 | Disabled | Disabled | Disabled | Disabled |
| eth1/0/10 | Disabled | Disabled | Disabled | Disabled |

Figure 4.104 – L2 Features > LLDP > LLDP Dot3 TLVs Settings

The fields that can be configured for the **LLDP Dot3 TLVs Settings** are described below:

| Item | Description |
|-------------------------------------|---|
| From Port / To Port | A consecutive group of ports may be configured starting with the selected port. |
| MAC/PHY Configuration/Status | Select whether the MAC/PHY Configuration Status is enabled on the port. The possible field values are: <ul style="list-style-type: none"> ◆ Enabled: Enables the MAC/PHY Configuration Status on the port. ◆ Disabled: Disables the MAC/PHY Configuration Status on the port. |
| Link Aggregation | Specifies whether the link aggregation is enabled on the port. The possible field values are: <ul style="list-style-type: none"> ◆ Enabled: Enables the link aggregation configured on the port. ◆ Disabled: Disables the link aggregation configured on the port. |
| Maximum Frame Size | Specifies whether the link aggregation is enabled on the port. The possible field values are: <ul style="list-style-type: none"> ◆ Enabled: Enables the Maximum Frame Size configured on the port. ◆ Disabled: Disables the Maximum Frame Size configured on the port. |
| Power via MDI | Advertises the Power via MDI implementations supported by the port. The possible field values are: <ul style="list-style-type: none"> ◆ Enabled: Enables the Power via MDI configured on the port. ◆ Disabled: Disables the Power via MDI configured on the port. |

Table 4.77

Click **Apply** to make the configurations take effect.

L2 Features > LLDP > LLDP-MED Port Settings

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

LLDP-MED Port Settings

LLDP-MED Port Settings

From Port: eth1/0/1 To Port: eth1/0/1 Capabilities: Disabled Network Policy: Disabled Inventory: Disabled

| Port | Capabilities | Network Policy | Inventory |
|-----------|--------------|----------------|-----------|
| eth1/0/1 | Disabled | Disabled | Disabled |
| eth1/0/2 | Disabled | Disabled | Disabled |
| eth1/0/3 | Disabled | Disabled | Disabled |
| eth1/0/4 | Disabled | Disabled | Disabled |
| eth1/0/5 | Disabled | Disabled | Disabled |
| eth1/0/6 | Disabled | Disabled | Disabled |
| eth1/0/7 | Disabled | Disabled | Disabled |
| eth1/0/8 | Disabled | Disabled | Disabled |
| eth1/0/9 | Disabled | Disabled | Disabled |
| eth1/0/10 | Disabled | Disabled | Disabled |

Figure 4.105 – L2 Features > LLDP > LLDP-MED Port Settings

The fields that can be configured for the **LLDP-MED Port Settings** are described below:

| Item | Description |
|----------------------------|---|
| From Port / To Port | Select the range of ports to be configured. |
| Capabilities | Select to enable or disable transmitting the LLDP-MED capabilities TLV. |
| Network Policy | Select to enable or disable transmitting the LLDP-MED network policy TLV. |
| Inventory | Select to enable or disable transmitting the LLDP-MED inventory management TLV. |

Table 4.78

Click **Apply** to make the configurations take effect.

L2 Features > LLDP > LLDP Statistics Information

The LLDP Statistics Information page displays an overview of the LLDP information.

| LLDP Statistics Information | | | | | | | | |
|-----------------------------|--------------------|----------------|--------------|----------------|--------------------|--------------------|---------------|-----------|
| LLDP Statistics Information | | | | | | | | |
| Last Change Time | 0 days 00h:00m:00s | | | | | | Clear Counter | |
| Total Inserts | 0 | | | | | | | |
| Total Deletes | 0 | | | | | | | |
| Total Drops | 0 | | | | | | | |
| Total Ageouts | 0 | | | | | | | |
| LLDP Statistics Ports | | | | | | | | |
| Port | eth1/0/1 | | | | | | Clear Counter | Clear All |
| Port | Total Transmits | Total Discards | Total Errors | Total Receives | Total TLV Discards | Total TLV Unknowns | Total Ageouts | |
| eth1/0/1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| eth1/0/2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| eth1/0/3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| eth1/0/4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| eth1/0/5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| eth1/0/6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| eth1/0/7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| eth1/0/8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| eth1/0/9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| eth1/0/10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |

Figure 4.106 – L2 Features > LLDP > LLDP Statistics Information

The fields that can be displayed for the **LLDP Statistics information** are described below:

| Item | Description |
|-------------------------|---|
| Last Change Time | Displays the time of the last change. It also displays the amount of time that has elapsed since the change was detected. |
| Total Inserts | Displays the number of new entries, since the last switch reboot. |
| Total Deletes | Displays the number of new entries, since the last switch reboot. |
| Total Drops | Displays the number of LLDP frames dropped due to the table was full. |
| Total Ageouts | Displays the number of entries deleted due to the Time-To-Live expiring. |

Table 4.79

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

The fields that can be displayed for the **LLDP port Statistics** are described below:

| Item | Description |
|---------------------------|--|
| Port | Select the port to be displayed. |
| Total Transmits | Displays the total number of LLDP frames transmitted on the port. |
| Total Discards | Displays the total discarded frame number of LLDP frames received on the port. |
| Total Errors | Displays the Error frame number of LLDP frames received on the port. |
| Total Receives | Displays the total number of LLDP frames received on the port. |
| Total TLV Discards | Each LLDP frame can contain multiple pieces of information, known as TLVs. If a TLV is malformed, it is counted and discarded. |
| Total TLV Unknowns | Displays the number of well-formed TLVs, but with a known type value. |

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

Table 4.80

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

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

L2 Features > LLDP > LLDP Local Port Information

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

| Port | Port ID Subtype | Port ID | Port Description |
|-----------|-----------------|-----------|---------------------------------|
| eth1/0/1 | Local | eth1/0/1 | DMS-1100-10TP V1.00.002 Port 01 |
| eth1/0/2 | Local | eth1/0/2 | DMS-1100-10TP V1.00.002 Port 02 |
| eth1/0/3 | Local | eth1/0/3 | DMS-1100-10TP V1.00.002 Port 03 |
| eth1/0/4 | Local | eth1/0/4 | DMS-1100-10TP V1.00.002 Port 04 |
| eth1/0/5 | Local | eth1/0/5 | DMS-1100-10TP V1.00.002 Port 05 |
| eth1/0/6 | Local | eth1/0/6 | DMS-1100-10TP V1.00.002 Port 06 |
| eth1/0/7 | Local | eth1/0/7 | DMS-1100-10TP V1.00.002 Port 07 |
| eth1/0/8 | Local | eth1/0/8 | DMS-1100-10TP V1.00.002 Port 08 |
| eth1/0/9 | Local | eth1/0/9 | DMS-1100-10TP V1.00.002 Port 09 |
| eth1/0/10 | Local | eth1/0/10 | DMS-1100-10TP V1.00.002 Port 10 |

Figure 4.107 – L2 Features > LLDP > LLDP Local Port Information

The fields that can be displayed for the **LLDP Local Port information** are described below:

| Item | Description |
|-------------------------|---|
| Port | Displays the port number. |
| Port ID Subtype | Displays the port ID subtype. |
| Port ID | Displays the port ID (Unit number/Port number). |
| Port Description | Displays the port description. |

Table 4.81

Click **Find** to displays more information for the specified port.

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

LLDP Local Port Information

LLDP Local Information Table

| | |
|---------------------------------|---------------------------------|
| Port | eth1/0/1 |
| Port ID Subtype | Local |
| Port ID | eth1/0/1 |
| Port Description | DMS-1100-10TP V1.00.002 Port 01 |
| Port PVID | 1 |
| Management Address Count | 1 |
| PPVID Entries | 0 |
| VLAN Name Entries Count | 1 |
| Protocol Identity Entries Count | 1 |
| MAC/PHY Configuration/Status | Show Detail |
| Link Aggregation | Show Detail |
| Maximum Frame Size | 1536 |
| LLDP-MED Capabilities | Show Detail |
| Network Policy | Show Detail |

[<< Back](#)

Figure 4.108 – L2 Features > LLDP > LLDP Local Port Information – Show Detail

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

L2 Features > LLDP > LLDP Neighbor Port Information

This LLDP Neighbor Port Information page allows user to view the information on a per-port basis for populating outbound LLDP advertisements in the local port brief table shown below.

LLDP Neighbor Port Information

LLDP Neighbor Port Brief Table

Port:

Total Entries : 0

| Entity | Chassis ID Subtype | Chassis ID | Port ID Subtype | Port ID | Port Description |
|----------------------|--------------------|------------|-----------------|---------|------------------|
| << Table is empty >> | | | | | |

Figure 4.109 – L2 Features > LLDP > LLDP Neighbors Port Information

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

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

L3 Features > IPv4 Interface

The IPv4 Interface page allows displays the information of IPv4 Interface entries.

IPv4 Interface

IPv4 Interface

Total Entries : 1

| Management VLAN | State | IP Address | Link Status | Edit | Delete |
|-----------------|---------|------------------------------|-------------|-------------------------------------|---------------------------------------|
| vian1 | Enabled | 10.90.90.90/255.0.0.0 Manual | Up | <input type="button" value="Edit"/> | <input type="button" value="Delete"/> |

Figure 4.110 – L3 Features > IPv4 Interface

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

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

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

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

IPv4 Interface Configuration

IPv4 Interface Settings | DHCP Client

Management VLAN Settings

VID (1-4094)

IP Settings

Get IP Form

IP Address

Mask

Figure 4.111 – L3 Features > IPv4 Interface Settings - Edit

The fields that can be configured for **IPv4 Interface Settings** are described below:

| Item | Description |
|---------------------------------|--|
| Management VLAN Settings | |
| VID (1-4094) | Enter the VLAN ID on which the associated management VLAN ID. |
| IP Settings | |
| Get IP From | Select Static or DHCP. When the Static option is selected, users can enter the IPv4 address of this interface manually. When the DHCP option is selected, this interface will obtain IPv4 information from a DHCP server located on the local network. |
| IP Address | Enter the IPv4 Address for this interface. |
| Mask | Enter the IPv4 subnet mask for this interface. |

Table 4.82

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

Click **Apply** to make the configurations take effect.

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

IPv4 Interface Configuration

IPv4 Interface Settings | DHCP Client

DHCP Client Client-ID (1-4094)

Class ID String Hex

Host Name

Lease Days (0-10000) Hours Minutes

DHCP Retry Times (5-120) times

Note: DHCP retry interval: 5 seconds

Figure 4.112 – L3 Features > IPv4 Interface – DHCP Client

The fields that can be configured for the **DHCP Client** are described below:

| Item | Description |
|---------------------------------------|--|
| DHCP Client Client-ID (1-4094) | Enter the VLAN interface, whose hexadecimal MAC address will be used as the client ID to be sent with the discover message. |
| Class ID String | Enter the vendor class identifier with the maximum of 32 characters. Tick the Hex check box to have the class identifier in the hexadecimal form. |

| | |
|---------------------------------|--|
| Host Name | Enter the host name. |
| Lease | Enter the preferred lease time for the IP address to request from the DHCP server. Enter the day duration of the lease, or select the hour and minute duration of the lease. |
| DHCP Retry Times (5-120) | Enter the DHCP retry times. The value is between 5 and 120 and default is 7 times. |

Table 4.83

Click **Apply** to make the configurations take effect.

L3 Features > IPv4 Default Gateway

The IPv4 Default Gateway page allows user to view and configure the IPv4 default gateway settings.

Figure 4.113 – L3 Features > IPv4 Default Gateway

The fields that can be configured for the **IPv4 Default Gateway** are described below:

| Item | Description |
|----------------|---|
| Gateway | Enter the gateway address for IPv4 route. If this is a default route, then this is the default gateway. |

Table 4.84

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

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

L3 Features > IPv6 Interface

The IPv6 Interface page is used to view the IPv6 interface's settings.

Figure 4.114 – L3 Features > IPv6 Interface

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

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

Figure 4.115 – L3 Features > IPv6 Interface - Detail

The fields that can be configured for **IPv6 Interface Settings** are described below:

| Item | Description |
|-------------------------------------|--|
| IPv6 Interface Settings | |
| IPv6 State | Select to enable or disable the IPv6 interface's global state. |
| Static IPv6 Address Settings | |
| IPv6 Address | Enter the IPv6 address for this IPv6 interface. Select the EUI-64 option to configure an IPv6 address on the interface using the EUI-64 interface ID. Select the Link Local option to configure a link-local address for the IPv6 interface. |
| NS Interval Settings | |
| NS Interval (1-3600) | Specify the NS interval and the values are between 1 and 3600. |

Table 4.85

Click **Apply** to make the configurations take effect.

After clicking the **Interface IPv6 Address** tab located at the top of the page, the following page will appear:

Figure 4.116 – L3 Features > IPv6 Interface – Interface IPv6 Address

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

L3 Features > IPv6 Default Gateway

The IPv6 Default Gateway is used to configure the IPv6 default gateway.

Figure 4.117 – L3 Features > IPv6 Default Gateway

The fields that can be configured for the **IPv6 Default Gateway** are described below:

| Item | Description |
|--------------------------------|--|
| Interface VLAN (1-4094) | Enter interface's VLAN ID that will be associated with this route. |
| Next Hop IPv6 Address | Enter the router's next hop IPv6 address. |

Table 4.86

Click **Apply** to make the configurations take effect.

QoS > Port Default CoS

The Port Default CoS page allows user to view and configure the port's default CoS settings.

Port Default CoS

From Port: eth1/0/1 To Port: eth1/0/1 Default CoS: 0 Override None

| Port | Default CoS | Override |
|-----------|-------------|----------|
| eth1/0/1 | 0 | No |
| eth1/0/2 | 0 | No |
| eth1/0/3 | 0 | No |
| eth1/0/4 | 0 | No |
| eth1/0/5 | 0 | No |
| eth1/0/6 | 0 | No |
| eth1/0/7 | 0 | No |
| eth1/0/8 | 0 | No |
| eth1/0/9 | 0 | No |
| eth1/0/10 | 0 | No |

Figure 4.118 – QoS > Port Default CoS

The fields that can be configured for the **Port Default Cos** are described below:

| Item | Description |
|----------------------------|---|
| From Port / To Port | Select the range of ports to be configured. |
| Default CoS | Select the default CoS option for the specified ports. The values are from 0 to 7. Click the Override check box to apply the port's default CoS to all packets (tagged or untagged) received by the port. Select the None option to use the default settings. |

Table 4.87

Click **Apply** to make the configurations take effect.

QoS > Port Scheduler Method

The Port Scheduler Method page allows user to view and configure the port scheduler method settings.

| Port | Scheduler Method |
|-----------|------------------|
| eth1/0/1 | SP |
| eth1/0/2 | SP |
| eth1/0/3 | SP |
| eth1/0/4 | SP |
| eth1/0/5 | SP |
| eth1/0/6 | SP |
| eth1/0/7 | SP |
| eth1/0/8 | SP |
| eth1/0/9 | SP |
| eth1/0/10 | SP |

Figure 4.119 – QoS > Port Scheduler Method

The fields that can be configured for the **Port Scheduler Method** are described below:

| Item | Description |
|----------------------------|---|
| From Port / To Port | Select the range of ports to be configured. |
| Scheduler Method | Select the scheduler method for the specified ports. Available options are Strict Priority (SP), and Weighted Round-Robin (WRR). By default, the output queue scheduling algorithm is SP . |

Table 4.88

Click **Apply** to make the configurations take effect.

QoS > Queue Settings

The Queue Settings page allows user to configure the queue settings.

| Queue ID | WRR Weight |
|----------|------------|
| 0 | 1 |
| 1 | 2 |
| 2 | 3 |
| 3 | 4 |
| 4 | 5 |
| 5 | 6 |
| 6 | 7 |
| 7 | 8 |

Figure 4.120 – QoS > Queue Settings

The fields that can be configured for the **Queue Settings** are described below:

| Item | Description |
|---------------------------|---|
| Queue ID | Select the queue ID value. The range is between 0 and 7. |
| WRR Weight (0-127) | Enter the WRR weight value. The value is between 0 and 127. |

Table 4.89

Click **Apply** to make the configurations take effect.

QoS > CoS to Queue Mapping

The CoS to Queue Mapping page allows user to view and configure the CoS-to-Queue mapping settings.

| CoS | Queue ID |
|-----|----------|
| 0 | 2 |
| 1 | 0 |
| 2 | 1 |
| 3 | 3 |
| 4 | 4 |
| 5 | 5 |
| 6 | 6 |
| 7 | 7 |

Figure 4.121 – QoS > CoS to Queue Mapping

The fields that can be configured for the **Queue Settings** are described below:

| Item | Description |
|-----------------|---|
| Queue ID | Select the queue ID that will be mapped to the corresponding CoS value. The value is from are 0 to 7. |

Table 4.90

Click **Apply** to make the configurations take effect.

QoS > Port Rate Limiting

The Port Rate Limiting page allows user to view and configure the port rate limiting settings.

| Port | Input | | Output | |
|-----------|----------|----------|----------|----------|
| | Rate | Burst | Rate | Burst |
| eth1/0/1 | No Limit | No Limit | No Limit | No Limit |
| eth1/0/2 | No Limit | No Limit | No Limit | No Limit |
| eth1/0/3 | No Limit | No Limit | No Limit | No Limit |
| eth1/0/4 | No Limit | No Limit | No Limit | No Limit |
| eth1/0/5 | No Limit | No Limit | No Limit | No Limit |
| eth1/0/6 | No Limit | No Limit | No Limit | No Limit |
| eth1/0/7 | No Limit | No Limit | No Limit | No Limit |
| eth1/0/8 | No Limit | No Limit | No Limit | No Limit |
| eth1/0/9 | No Limit | No Limit | No Limit | No Limit |
| eth1/0/10 | No Limit | No Limit | No Limit | No Limit |

Figure 4.122 – QoS > Port Rate Limiting

The fields that can be configured for the **Port Rate Limiting** are described below:

| Item | Description |
|----------------------------|---|
| From Port / To Port | Select the range of ports to be configured. |

| | |
|-------------------|--|
| Direction | Select the direction. Available options are Input and Output . When Input is selected, the rate limit for ingress packets is configured. When Output is selected, the rate limit for egress packets is configured. |
| Rate Limit | <p>Enter the Rate Limit for the specified port.</p> <p>When Bandwidth is selected, enter the input/output bandwidth value used in the space provided. This value must be between 64 and 10000000 kbps. Also, enter the Burst Size value in the space provided. This value must be between 0 and 128000 kilobytes.</p> <p>When Percent is selected, enter the input/output bandwidth percentage value used in the space provided. This value must be between 1 and 100 percent (%). Also, enter the Burst Size value in the space provided. This value must be between 0 and 128000 kilobytes.</p> <p>Select the None option to remove the rate limit on the specified port(s). The specified limitation cannot exceed the maximum speed of the specified interface. For the ingress bandwidth limitation, the ingress can trigger a pause frame or a flow control frame when the received traffic exceeds the limitation.</p> |

Table 4.91

Click **Apply** to make the configurations take effect.

Security > Safeguard Engine

D-Link's **Safeguard Engine** is a robust and innovative technology that automatically throttles the impact of packet flooding into the switch's CPU. This function helps to protect the Switch from being interrupted by malicious viruses or worm attacks. This option is enabled by default.



Figure 4.123 – Security > Safeguard Engine

Click **Apply** to make the configurations take effect.

Security > Trusted Host

The Trusted Host page allows user to view and configure the trusted host settings.



Figure 4.124 Security > Trusted Host

The fields that can be configured for the **Trusted Host** are described below:

| Item | Description |
|------|-------------|
|------|-------------|

| | |
|------------------|---|
| IPv4 Host | Specify the IPv4 host address. |
| Type | Specify the trusted host type. The options are Ping , HTTP and HTTPS . |

Table 4.92

Click **Apply** to make the configurations take effect.

Security > Traffic Segmentation Settings

This feature provides administrators to limit traffic flow from a single port to a group of ports on a single Switch. This method of segmenting the flow of traffic is similar to using VLANs to limit traffic, but is more restrictive.

Figure 4.125 – Security > Traffic Segmentation Settings

The fields that can be configured for the **Traffic Segmentation Settings** are described below:

| Item | Description |
|--|---|
| From Port / To Port | Select the range of ports to be configured. |
| From Forward Port / To Forward Port | Select the range of forward ports to be configured. |

Table 4.93

Click the **Add** button to add a new entry.

Click the **Delete** button to remove an entry based on the information entered.

Security > Storm Control Settings

The Storm Control Settings page allows user to view and configure the storm control settings.

Storm Control Settings

Storm Control Trap Settings

Trap State:

Storm Control Polling Settings

Interval (5-600): sec Retries (0-360): times Infinite

Storm Control Port Settings

From Port: To Port: Type: Action: PPS Rise (0-2147483647): pps PPS Low (0-2147483647): pps

When set "Drop" action, all types of packet that need to limit rate can only share one threshold.

Total Entries : 30

| Port | Storm | Action | Threshold | Current | State |
|----------|-----------|--------|-----------|---------|----------|
| eth1/0/1 | Broadcast | Drop | - | - | Inactive |
| | Multicast | | - | - | Inactive |
| | Unicast | | - | - | Inactive |
| eth1/0/2 | Broadcast | Drop | - | - | Inactive |
| | Multicast | | - | - | Inactive |
| | Unicast | | - | - | Inactive |
| eth1/0/3 | Broadcast | Drop | - | - | Inactive |
| | Multicast | | - | - | Inactive |
| | Unicast | | - | - | Inactive |
| eth1/0/4 | Broadcast | Drop | - | - | Inactive |
| | Multicast | | - | - | Inactive |
| | Unicast | | - | - | Inactive |

Figure 4.126 – Security > Storm Control Settings

The fields that can be configured for **Storm Control Settings** are described below:

| Item | Description |
|--|--|
| Storm Control Trap Settings | |
| Trap State | Select the storm control trap state. The options are None , Storm Occur , Storm Clear , and Both . When None is selected, no traps will be sent. When Storm Occur is selected, a trap notification will be sent when a storm event is detected. When Storm Clear is selected, a trap notification will be sent when a storm event is cleared. |
| Storm Control Trap Polling Settings | |
| Interval (1-300) | Enter the interval value. The range is from 1 to 300. |
| Retries (0-360) | Enter the retry value. The range is from 0 to 360. |
| Storm Control Port Settings | |
| From Port / To Port | Select the range of ports to be configured. |
| Type | Select the type of storm attack. The values are Broadcast , Multicast , and Unicast . |
| Action | Select the action for the specified ports. The values are None , Shutdown and Drop . |
| PPS Rise (1-2147483647) | Enter the rise packets per second value. The value is from 1 to 2147483647. |
| PPS Low (1-2147483647) | Enter the low packets per second value. The value is from 1 to 2147483647. |

Table 4.94

Click **Apply** to make the configurations take effect.

Security > DoS Attack Prevention Settings

The DoS Attack Prevention Settings page allows user to view and configure the Denial-of-Service (DoS) attack prevention settings.

| DoS Type | State | Action |
|----------------------|----------|--------|
| Land Attack | Disabled | Drop |
| TCP null | Disabled | Drop |
| TCP Xmas | Disabled | Drop |
| TCP SYN-FIN | Disabled | Drop |
| Ping of Death Attack | Disabled | Drop |

Figure 4.127 – Security > DoS Attack Prevention Settings

The fields that can be configured for **DoS Attack Prevention Settings** are described below:

| Item | Description |
|---------------------------------------|---|
| DoS Attack Prevention Settings | |
| DoS Type Selection | Tick the DoS type to be prevented. The options are Land Attack , TCP Null , TCP Xmas , TCP SYN-FIN , Ping of Death Attack and All Types . |
| DoS Settings | |
| State | Select to enable or disable the DoS attack prevention state. |
| Action | Select the action for the DoS attack. |

Table 4.95

Click **Apply** to make the configurations take effect.

Security > SSL > SSL Global Setting

Secure Sockets Layer (SSL) is a security feature that provides a secure communication path between the management PC and the Switch Web UI by using authentication, digital signatures and encryption. These security functions are implemented by Ciphersuite, a security string that determines the cryptographic parameters, encryption algorithms and key sizes.

This page allows user to configure the SSL global state settings.

Figure 4.128 – Security > SSL > SSL Settings

The fields that can be configured for **SSL Settings** are described below:

| Item | Description |
|-----------------------|--|
| SSL Status | Select to enable or disable the SSL feature's global status. |
| Service Policy | Enter service policy name. |

Table 4.96

Click **Apply** to make the configurations take effect.



NOTE: When SSL is enabled, it will take longer to open a web page due to the extra processing required for encryption. After saving, please wait about 10 seconds for the system summary page to load.

Security > SSL > SSL Service Policy

The SSL Service Policy page allows user to view and configure the SSL service policy settings.

Figure 4.129 – Security > SSL > SSL Service Policy

The fields that can be configured for **SSL Service Policy** are described below:

| Item | Description |
|---|---|
| Policy Name | Enter a policy name for SSL. |
| Session Cache Timeout (60-86400) | Enter the session cache timeout value. The value is between 60 and 86400 seconds. |
| Cipher Suites | Select the cipher suites that will be associated with this profile. |

Table 4.97

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

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

Click **Apply** to make the configurations take effect.

OAM > Cable Diagnostics

The Cable Diagnostics page is designed primarily for administrators and customer service representatives to examine the copper cable quality. It determines the type of cable errors in the cable. Select the range of ports and then click the **Test** button to start the diagnosis.

| Port | Link Status | Test Result | Cable Length (M) | |
|----------|-------------|-------------|------------------|-------|
| eth1/0/1 | Down | - | - | Clear |
| eth1/0/2 | Up | - | - | Clear |
| eth1/0/3 | Down | - | - | Clear |
| eth1/0/4 | Down | - | - | Clear |
| eth1/0/5 | Down | - | - | Clear |
| eth1/0/6 | Down | - | - | Clear |
| eth1/0/7 | Down | - | - | Clear |
| eth1/0/8 | Down | - | - | Clear |

Figure 4.130 – OAM > Cable Diagnostic

Click the **Clear** button to clear all the information for the specific port.

Click the **Clear All** button to clear all the information in this table.



NOTE: Please be sure that the Power Saving feature is disabled before enabling the Cable Diagnostics function.

Monitoring > Statistics > Port

This Port page allows user to display the port traffic statistics.

| port | RX | | | | TX | | | | Show Detail |
|-----------|-----------|-------------|---------|---------|-----------|-------------|---------|---------|-------------|
| | Rate | | Total | | Rate | | Total | | |
| | bytes/sec | packets/sec | bytes | packets | bytes/sec | packets/sec | bytes | packets | |
| eth1/0/1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |
| eth1/0/2 | 0 | 0 | 5389000 | 31033 | 0 | 0 | 8839967 | 22486 | Show Detail |
| eth1/0/3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |
| eth1/0/4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |
| eth1/0/5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |
| eth1/0/6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |
| eth1/0/7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |
| eth1/0/8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |
| eth1/0/9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |
| eth1/0/10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Detail |

Figure 4.131 – Monitoring > Statistics > Port

The fields that can be displayed for **Port** information are described below:

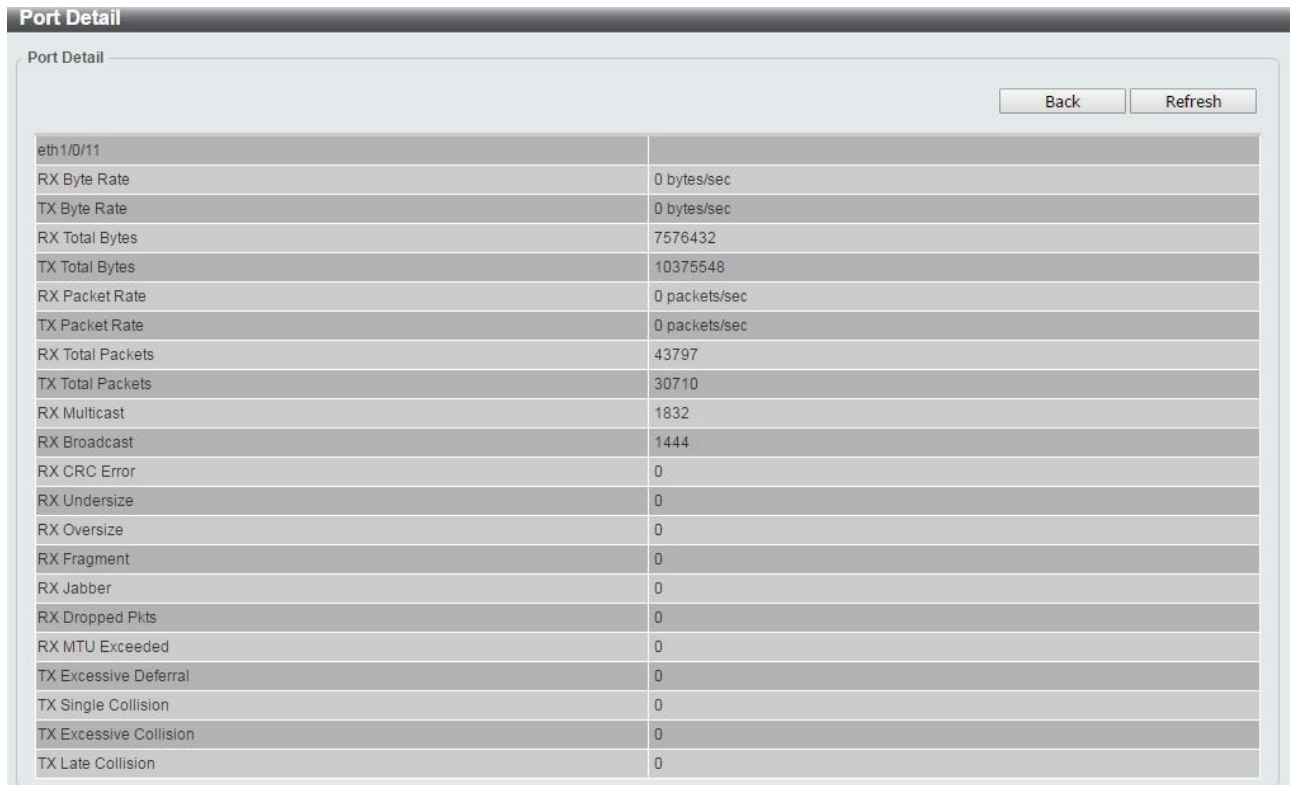
| Item | Description |
|----------------------------|---|
| From Port / To Port | Select the range of ports to be configured. |

Table 4.98

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

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

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



| Port Detail | |
|------------------------|---------------|
| eth1/0/11 | |
| RX Byte Rate | 0 bytes/sec |
| TX Byte Rate | 0 bytes/sec |
| RX Total Bytes | 7576432 |
| TX Total Bytes | 10375548 |
| RX Packet Rate | 0 packets/sec |
| TX Packet Rate | 0 packets/sec |
| RX Total Packets | 43797 |
| TX Total Packets | 30710 |
| RX Multicast | 1832 |
| RX Broadcast | 1444 |
| RX CRC Error | 0 |
| RX Undersize | 0 |
| RX Oversize | 0 |
| RX Fragment | 0 |
| RX Jabber | 0 |
| RX Dropped Pkts | 0 |
| RX MTU Exceeded | 0 |
| TX Excessive Deferral | 0 |
| TX Single Collision | 0 |
| TX Excessive Collision | 0 |
| TX Late Collision | 0 |

Figure 4.132 – Monitoring > Statistics > Port – Show Detail

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

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

Monitoring > Statistics > Port Counters

The Port Counters page allows user to display port counter statistics.

| Port | InOctets | InUcastPkts | InMcastPkts | InBcastPkts | OutOctets | OutUcastPkts | OutMcastPkts | OutBcastPkts | Show Errors |
|-----------|----------|-------------|-------------|-------------|-----------|--------------|--------------|--------------|-------------|
| eth1/0/1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |
| eth1/0/2 | 5467538 | 29754 | 914 | 794 | 8961685 | 22791 | 0 | 4 | Show Errors |
| eth1/0/3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |
| eth1/0/4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |
| eth1/0/5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |
| eth1/0/6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |
| eth1/0/7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |
| eth1/0/8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |
| eth1/0/9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |
| eth1/0/10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Show Errors |

Figure 4.133 – Monitoring > Statistics > Port Counters

The fields that can be displayed for **Port Counters** are described below:

| Item | Description |
|----------------------------|---|
| From Port / To Port | Select the range of ports to be viewed. |

Table 4.99

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

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

Click the **Show Errors** button to see all error counters of the specific port.

After clicking the **Show Errors** button, the following page will appear.

| eth1/0/2 Counters Errors | |
|--------------------------|---|
| Align-Err | 0 |
| Fcs-Err | 0 |
| UnderSize | 0 |
| OutDiscard | 0 |
| Single-Col | 0 |
| Multi-Col | 0 |
| Late-Col | 0 |
| Excess-Col | 0 |
| Carri-Sen | 0 |
| SQE-Test-Err | 0 |
| DeferredTx | 0 |
| IntMacTx | 0 |
| IntMacRx | 0 |

Figure 4.134 – Monitoring > Statistics > Port Counters – Show Errors

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

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

Monitoring > Statistics > Counters

The Counters page allows user to display all port counters, and clear the port counters of the specified or all ports.

| Port | linkChange | |
|-----------|------------|-------------|
| eth1/0/1 | 0 | Show Detail |
| eth1/0/2 | 1 | Show Detail |
| eth1/0/3 | 0 | Show Detail |
| eth1/0/4 | 0 | Show Detail |
| eth1/0/5 | 0 | Show Detail |
| eth1/0/6 | 0 | Show Detail |
| eth1/0/7 | 0 | Show Detail |
| eth1/0/8 | 0 | Show Detail |
| eth1/0/9 | 0 | Show Detail |
| eth1/0/10 | 0 | Show Detail |

Figure 4.135 – Monitoring > Statistics > Counters

The fields that can be displayed for **Counters** are described below:

| Item | Description |
|----------------------------|---|
| From Port / To Port | Select the range of ports to be viewed. |

Table 4.100

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

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

Click the **Clear** button to clear all the information for the specific ports.

Click the **Clear All** button to clear all the information in this table.

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

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

| eth1/0/2 Counters | |
|-------------------------|---------|
| rxHCTotalPkts | 32261 |
| txHCTotalPkts | 23388 |
| rxHCUnicastPkts | 30536 |
| txHCUnicastPkts | 23388 |
| rxHCMulticastPkts | 922 |
| txHCMulticastPkts | 0 |
| rxHCBroadcastPkts | 803 |
| txHCBroadcastPkts | 4 |
| rxHCOctets | 5606965 |
| txHCOctets | 9193071 |
| rxHCPkt64Octets | 31427 |
| rxHCPkt65to127Octets | 10079 |
| rxHCPkt128to255Octets | 2055 |
| rxHCPkt256to511Octets | 1913 |
| rxHCPkt512to1023Octets | 4180 |
| rxHCPkt1024to1518Octets | 0 |
| rxHCPkt1519to2047Octets | 0 |
| rxHCPkt2048to4095Octets | 0 |
| rxHCPkt4096to9216Octets | 0 |
| txHCPkt64Octets | 0 |
| txHCPkt65to127Octets | 0 |
| txHCPkt128to255Octets | 0 |
| txHCPkt256to511Octets | 0 |
| txHCPkt512to1023Octets | 0 |
| txHCPkt1024to1518Octets | 0 |
| txHCPkt1519to2047Octets | 0 |
| txHCPkt2048to4095Octets | 0 |
| txHCPkt4096to9216Octets | 0 |

Figure 4.136 – Monitoring > Statistics > Counters – Show Detail

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

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

Monitoring > Mirror Settings

The Mirror Settings page allows user to view and configure the port mirroring feature.

| Mirror Settings | | | | | |
|----------------------|--------------------------|-------------------------------------|----------|--|------------------|
| Session Number | 1 | | | | |
| Destination | <input type="checkbox"/> | Port | eth1/0/1 | | |
| Source | <input type="checkbox"/> | From Port | To Port | Frame Type | |
| | | eth1/0/1 | eth1/0/1 | Both | |
| | | | | <input type="button" value="Add"/> <input type="button" value="Delete"/> | |
| Mirror Session Table | | | | | |
| All Session | 1 | <input type="button" value="Find"/> | | | |
| Session Number | Session Type | Source Ports | | | Destination Port |
| | | Both | RX | TX | |
| << Table is empty >> | | | | | |

Figure 4.137 – Monitoring > Mirror Settings

The fields that can be configured for **Mirror Settings** are described below:

| Item | Description |
|------------------------|---|
| Mirror Settings | |
| Session Number | Select the mirror session number for the entry. |

| | |
|-----------------------------|--|
| Destination | Select the destination port for mirror settings. |
| Source | Select the range of ports to be the source port and Frame Type to be mirrored. |
| Mirror Session Table | |
| Mirror Session Table | Select the Mirror Session Type to be displayed. |

Table 4.101

Click the **Add** button to add the newly configured mirror entry based on the information entered.

Click the **Delete** button to delete an existing mirror entry based on the information entered.

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

Green > Power Saving

The Power Saving page allows user to configure the power saving settings of the Switch.

Figure 4.138 – Green > Power Saving

The fields that can be configured for **Power Saving** are described below:

| Item | Description |
|-------------------------------|---|
| Administrative Dim-LED | Select to enable or disable the scheduled port shutdown power saving feature. |

Table 4.102

Click **Apply** to make the configurations take effect for each individual section.

Green > EEE

The Energy Efficient Ethernet (EEE) is defined in IEEE 802.3az. It is designed to reduce the energy consumption of a link when no packets are being sent.

| Port | State |
|-----------|----------|
| eth1/0/1 | Disabled |
| eth1/0/2 | Disabled |
| eth1/0/3 | Disabled |
| eth1/0/4 | Disabled |
| eth1/0/5 | Disabled |
| eth1/0/6 | Disabled |
| eth1/0/7 | Disabled |
| eth1/0/8 | Disabled |
| eth1/0/9 | Disabled |
| eth1/0/10 | Disabled |

Figure 4.139 – Green > EEE

The fields that can be configured for **EEE** are described below:

| Item | Description |
|----------------------------|--|
| From Port / To Port | Select the range of ports to be configured. |
| State | Select to enable or disable the EEE feature. |

Table 4.103

Click **Apply** to make the configurations take effect.

Appendix A - Technical Specifications

This appendix contains the device specifications, and contains the topics:

- **Hardware Specifications**
- **Features**

Hardware Specifications

| Key Components / Performance | |
|--|--|
| Switching Capacity | DMS-1100-10TS: 80Gbps DMS-1100-10TP: 80Gbps |
| Max. Forwarding Rate | DMS-1100-10TS: 59.52Mpps DMS-1100-10TP: 59.52Mpps |
| Forwarding Mode | Store and Forward |
| Packet Buffer memory | DMS-1100-10TS: 1.5Mbytes DMS-1100-10TP: 1.5Mbytes |
| DDRIII for CPU | 256M bytes |
| Flash Memory | 128M Bytes |
| Priority Queues | 8 Priority Queues per port |
| Port Functions | |
| 10/100/1000/2.5GBASE-T Ethernet Ports | <p>DMS-1100-10TS: 8 x 10/100/1000/2.5GBASE-T ports DMS-1100-10TP: 8 x 10/100/1000/2.5GBASE-T ports</p> <p>1000Base-T ports compliant to following standards:</p> <ul style="list-style-type: none"> • IEEE 802.3 compliance • IEEE 802.3u compliance • IEEE 802.3ab compliance • IEEE 802.3bz compliance <p>Support Half/Full-Duplex operations</p> <ul style="list-style-type: none"> • IEEE 802.3x Flow Control support for Full-Duplex mode • Back Pressure for Half-Duplex mode • Head-of-line blocking prevention <p>Support manual/auto MDI/MDIX configuration Support Auto-Negotiation for each port Hardware interrupt signal to CPU when port link down for ERPS</p> |
| SFP+ Ports | <p>DMS-1100-10TS: 2 x 1000/10G ports (Port 9 and Port 10) DMS-1100-10TP: 2 x 1000/10G ports (Port 9 and Port 10)</p> <p>Supported SFP+ Direct Attached Cables:</p> <ul style="list-style-type: none"> • DEM-CB100S: 10-GbE SFP+ 1m Direct Attach Cable • DEM-CB300S: 10-GbE SFP+ 3m Direct Attach Cable |

| | |
|-----------------------------------|---|
| | <ul style="list-style-type: none"> DEM-CB700S: 10-GbE SFP+ 7m Direct Attach Cable |
| Physical & Environment | |
| Power Consumption | <p>DMS-1100-10TS: Maximum power consumption: 33.7 Watts Standby power consumption: 21.6 Watts</p> <p>DMS-1100-10TP: Maximum power consumption: 293.4 Watts (PoE on), 38.1 Watts (PoE Off) Standby power consumption: 27.3 Watts</p> |
| Power Supply | AC input, 100~240 VAC, 50/60Hz, internal universal power supply |
| Fans | <p>DMS-1100-10TS: 1 Smart Fan</p> <p>DMS-1100-10TP: 3 Smart Fans</p> |
| Operating Temperature | -5~50°C |
| Storage Temperature | -40~70°C |
| Humidity | Storage: 0%~95% non-condensing |
| Dimensions | <p>DMS-1100-10TS: 440mm x 210mm x 44mm</p> <p>DMS-1100-10TP: 440mm x 250mm x 44mm</p> |
| Weight | <p>DMS-1100-10TS: 2.53kg</p> <p>DMS-1100-10TP: 3.43kg</p> |
| EMI | CE, FCC/IC, VCCI, BSMI, C-Tick, CCC |
| Safety | UL, CB, BSMI, CCC |

Features

L2 Features

- › Supports up to 16K MAC address
- › Jumbo frame: Supports up to 9KB
- › IGMP snooping: Supports 192 multicast group (shared with MLD Snooping)
- › MLD Snooping: Supports 192 multicast group (shared with IGMP Snooping)
- › 802.1D Spanning Tree
- › 802.1s MSTP
- › ERPS
- › Loopback Detection
- › 802.3ad Link Aggregation:
 - DMS-1100-10TS: up to 8 groups per device and 8 ports per group
 - DMS-1100-10TP: up to 8 groups per device and 8 ports per group
- › Port mirroring

L3 Features

- › Support 1 IPv4 and 1 IPv6 interfaces

VLAN

- › 802.1Q VLAN standard (VLAN Tagging)
- › Up to 4094 static VLAN groups
- › Asymmetric VLAN
- › Management VLAN
- › Auto Voice VLAN

QoS (Quality of Service)

- › Priority queue mapping by :
 - 802.1p
 - CoS
- › Up to 8 queues per port
- › Supports Strict in queue handling
- › Bandwidth Control

Security

- › Trusted Host
- › Traffic Segmentation
- › D-Link Safeguard Engine
- › Broadcast Storm Control
- › SSL: Support v1/v2

OAM

- › Cable Diagnostics
- › Reset button (reset to factory default)

Management

- › Web-based GUI
- › SNMP support
- › DHCP client
- › Trap setting for destination IP, system events, fiber port events, twisted-pair port events

D-Link Green Technology

- › Power Saving: Enabled by default to save power:
 - 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 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.

Appendix B – Rack mount Instructions

Safety Instructions - Rack Mount Instructions - The following or similar rack-mount instructions are included with the installation instructions:

- 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 (Tma) 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).

