

DGS-1210 Series

SMART MANAGED SWITCH WEB UI REFERENCE GUIDE

Ver. 1.10



Table of Contents

Table of Contents	i
About This Guide	1
Terms/Usage	1
Copyright and Trademarks	1
Product Introduction	2
DGS-1210-10	3
Front Panel	3
Rear Panel	3
DGS-1210-10P	4
Front Panel	4
Rear Panel	5
DGS-1210-10MP	5
Front Panel	5
Rear Panel	6
DGS-1210-20	6
Front Panel	6
Rear Panel	7
DGS-1210-26	7
Front Panel	7
Rear Panel	8
DGS-1210-28	8
Front Panel	8
Rear Panel	9
DGS-1210-28P	9
Front Panel	
Rear Panel	. 10
DGS-1210-28MP	
Front Panel	
Rear Panel	
DGS-1210-52	
Front Panel	
Rear Panel	
DGS-1210-52MP	
Front Panel	
Rear Panel	
LED Indicators	
2 Hardware Installation	
Safety Cautions	
Step 1: Unpacking	
Step 2: Switch Installation	
Desktop or Shelf Installation	
Rack Installation	
Step 3: Plugging in the AC Power Cord with Power Cord Clip	
Power Failure	
Grounding the Switch	
3 Getting Started	
Management Options	. 23

Using Web-based Management	23
Supported Web Browsers	
Connecting to the Switch	23
Login Web-based Management	
Smart Wizard	
Web-based Management	
D-Link Network Assistant	24
4 Web-based Switch Configuration	25
Web-based Management	25
Tool Bar > Save Menu	
Save Configuration	
Save Log	
Tool Bar > Tools Menu	
Reset System	
Reboot Device	
Configuration Backup and Restore	
System Log Backup	
Firmware Backup and Upgrade	
Firmware Information	
Tool Bar > Online Help	
Function Tree	
Device Information	
System > System Settings	
System > DHCP Auto Configuration	
System > Port Settings	
System > Port Description	
System > IPv6 Setting > IPv6 System Settings	
System > IPv6 Setting > IPv6 Default Gateway Settings	
System > IPv6 Setting > IPv6 Neighbor Settings	
System > DHCP Relay > DHCP Relay Global Settings	
System > DHCP Relay > DHCP Relay Interface Settings	
System > DHCP Local Relay Settings	
System > DHCPv6 Relay Settings	
System > System Log Configuration > System Log Settings	
System > System Log Configuration > SysLog Host	
System > Time Profile	
System > Power Saving	49
System > IEEE802.3az EEE Settings	
Configuration > 802.1Q VLAN	
Configuration > 802.1Q Management VLAN	
Configuration > 802.1Q VLAN PVID	52
Configuration > Voice VLAN > Voice VLAN Global Settings	53
Configuration > Voice VLAN > Voice VLAN Port Settings	
Configuration > Voice VLAN > Voice Device List	
Configuration > Auto Surveillance VLAN > Auto Surveillance Properties	
Configuration > Auto Surveillance VLAN > MAC Settings and Surveillance Device	
Configuration > Auto Surveillance VLAN > ONVIF IPC Information	
Configuration > Auto Surveillance VLAN > ONVIF NVR Information	
Configuration > Jumbo Frame	

Configuration > Port Mirroring	67
Configuration > Loopback Detection	67
Configuration > Multicast Forwarding & Filtering > Multicast Forwarding	80
Configuration > Multicast Forwarding & Filtering > Multicast Filter Mode	80
Configuration > Multicast Forwarding & Filtering > IP Multicast Profile Settings	81
Configuration > Multicast Forwarding & Filtering > Limited Multicast Range Settings	81
Configuration > Multicast Forwarding & Filtering > MAX Multicast Group Settings	82
Security > MAC Address Table > Static MAC	92
Security > MAC Address Table > Dynamic Forwarding Table	93
Security > Access Authentication Control > Authentication Policy Settings	93
Security > Access Authentication Control > Application Authentication Settings	93
Security > Access Authentication Control > Authentication Server Group	94
Security > Access Authentication Control > Authentication Server	95
Security > Access Authentication Control > Login Method Lists	95
Security > Access Authentication Control > Enable Method Lists	96
Security > Access Authentication Control > Local Enable Password Settings	97
Security > Traffic Segmentation	97
Security > DoS Prevention Settings	97
Security > Smart Binding > Smart Binding Settings	98
Security > Smart Binding > Smart Binding	99
Security > Smart Binding > White List	100
Security > Smart Binding > Black List	100
Security > Smart Binding > DHCP Snooping List	100
Security > Smart Binding > Smart Binding	101
Security > Smart Binding > White List	102
Security > Smart Binding > Black List	
Security > Smart Binding > DHCP Snooping List	
Monitoring > Session Table	
Monitoring > CPU Utilization	104
Monitoring > Memory Utilization	105
Monitoring > Port Utilization	
Monitoring > Packet Size	106
Monitoring > Packets > Transmitted (TX)	
Monitoring > Packets > Received (RX)	
Monitoring > Packets > UMB Cast (RX)	109
Monitoring > Errors > Received (RX)	110
Monitoring > Errors > Transmitted (TX)	
Monitoring > Cable Diagnostics	
Monitoring > System Log	
Monitoring > Browse ARP Table	
Monitoring > Ethernet OAM > Browse Ethernet OAM Event Log	
Monitoring > Ethernet OAM > Browse Ethernet OAM Statistics	
Monitoring > IGMP Snooping > IGMP Snooping Group	
Monitoring > IGMP Snooping > IGMP Snooping Host	
Monitoring > MLD Snooping > MLD Snooping Group	
Monitoring > Port Access Control > RADIUS Authentication	
Monitoring > Port Access Control > RADIUS Account Client	
ACL > ACL Configuration Wizard	
ACL > Access Profile List	119

ACL > ACL Finder	120
ACL > CPU Filter Configuration Wizard	120
ACL > CPU Filter Access Profile List	121
ACL > CPU Filter Finder	122
PoE > PoE Port Settings (DGS-1210-10P/10MP/28P/28MP/52MP only)	122
PoE > PoE System Settings (DGS-1210-10P/10MP/28P/28MP/52MP only)	124
LLDP > LLDP Global Settings	125
LLDP > Basic LLDP Port Settings	125
LLDP > 802.1 Extension LLDP Port Settings	126
LLDP > 802.3 Extension LLDP Port Settings	127
LLDP > LLDP Management Address Settings	128
LLDP > LLDP Statistics Table	128
LLDP > LLDP Management Address Table	129
LLDP > LLDP Local Port Table	129
LLDP > LLDP Remote Port Table	130
LLDP > LLDP-MED Settings	132
Appendix A - Ethernet Technology	133
Gigabit Ethernet Technology	133
Fast Ethernet Technology	133
Switching Technology	133
Appendix B - Technical Specifications	134
Hardware Specifications	134
Features	138
L2 Features	138
L3 Features	138
VLAN	138
QoS (Quality of Service)	138
Security	138
OAM	138
Management	138
D-Link Green Technology	
Appendix C – Rack mount Instructions	140

About This Guide

This guide provides instructions to install the D-Link Metro Ethernet Switch DGS-1210 series, and to configure Web-based Management step-by-step.

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

This guide is mainly divided into four parts:

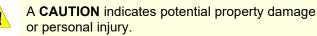
- 1. Hardware Installation: Step-by-step hardware installation procedures.
- 2. Getting Started: A startup guide for basic switch installation and settings.
- 3. Web Configuration: Information about the function descriptions and configuration settings via Web.
- 4. Command Line Interface: Information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

Terms/Usage

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



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



Copyright and Trademarks

Information in this document is subjected to change without notice.

© 2017 D-Link Corporation. All rights reserved.

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

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

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

1 Product Introduction

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

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

Flexible Port Configurations. The DGS-1210 series is the new generation of Metro Ethernet Switch series. DGS-1210 series including 10/100/1000BASE-T RJ-45 ports, 100/1000 Mbps combo ports, and 100/1000 Mbps SFP ports. The DGS-1210-10, DGS-1210-26, DGS-1210-10P, and DGS-1210-10MP models feature 2 100/1000 Mbps SFP ports, while all other DGS-1210 Series models feature 4 GbE/SFP combo ports, allowing you to choose the most suitable media type for your requirements.

D-Link Green Technology. D-Link Green devices are about providing eco-friendly alternatives without compromising performance. D-Link Green Technology includes a number of innovations to reduce energy consumption on DGS-1210 series such as shutting down a port, or turning off some LED indicators, or adjusting the power usage according to the Ethernet cable connected to it.

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

Traffic Segmentation, QoS and Auto Surveillance VLAN. The switches support 802.1Q VLAN standard tagging to enhance network security and performance. The switches also support 802.1p priority queues, enabling users to run bandwidth-sensitive applications such as streaming multimedia by prioritizing that traffic in network. These functions allow switches to work seamlessly with VLAN and 802.1p traffic in the network. Auto Surveillance VLAN will automatically place the vedio traffic from pre-defined IP surveillance devices to an assigned VLAN with higher priority, so it can be separated from normal data traffic. Asymmetric VLAN is implemented in these switches for a more efficient use of shared resources, such as server or gateway devices.

Network Security. D-Link's innovative Safeguard Engine function protects the switches against traffic flooding caused by virus attacks. Additional features like 802.1X port-based authentication provide access control of the network with external RADIUS servers. ACL is a powerful tool to screen unwanted IP or MAC traffic. 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 Metro Ethernet Switches provides growing businesses simple and easy management of their network. The multi-language Web-Based management interface allows administrators to remotely control their network down to the port level. The intuitive easily allows customers to discover multiple D-Link Metro Ethernet Switches in the same L2 network segment. With this utility, users do not need to change the IP address of PC and provides easy initial setting of smart switches. The switches within the same L2 network segment connected to user's local PC are displayed on the screen for instant access. It allows extensive switch configuration setting, and basic configuration of discovered devices such as a password change or firmware upgrade.

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

In addition, users can utilize the SNMP MIB (*Management Information Base*) to poll the switches for information about the status, or send out traps of abnormal events. SNMP support allows users to integrate

the switches with other third-party devices for management in an SNMP-enabled environment. D-Link Metro Ethernet Switches provides easy-to-use graphic interface and facilitates the operation efficiency.

DGS-1210-10

8-Port 10/100/1000Mbps, plus 2 SFP Ports (100/1000Mbps) Metro Ethernet switch.

Front Panel



Figure 1.1 – DGS-1210-10 Front Panel

The front panel of the **DGS-1210-10** switch consists out of the following:

- **Power LED**⁽¹⁾: The Power LED lights up when the Switch is connected to a power source.
- **Port Link/Act/Speed LED (1-8):** The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When a port has an amber light, this indicates that the port is running on 10M or 100M. When it has a green light it is running on 1000M.
- **Port Link/Act/Speed LED (9F, 10F):** The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When the port LED glows in amber, it indicates the port is running on 100M. When the port LED glows in green, it is running on 1000Mbps.
- **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 via image 1 and image 2, the device will enter the loader mode automatically.



Si le transceiveur optique n'est pas livré avec l'appareil, le manuel d'utilisation doit comporter la description ci-dessous ou son équivalent :« Ce produit est destiné à être utilisé avec un transceiveur optique homologué UL,tension DC3.3V, classe laser l.

NOTE: Once user enter in loader mode, you can use DNA tool (standalone version 2.0.2.4 only (No support by Chrome DNA3.x.x.x)) to download the image or call D-Link Technical Support for further help.

<u>Rear Panel</u>



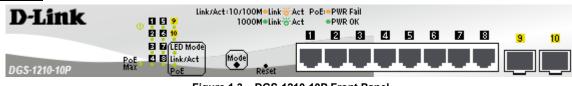
Figure 1.2 – DGS-1210-10 Rear Panel

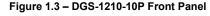
Power: Connect the supplied AC power cable to this port.

DGS-1210-10P

8-Port 10/100/1000Mbps, plus 2 SFP Ports (100/1000Mbps) Metro Ethernet PoE switch.

Front Panel





The front panel of the **DGS-1210-10P** switch consists out of the following:

- **Power LED**⁽¹⁾: The Power LED lights up when the Switch is connected to a power source.
- **PoE Max:** The solid amber of PoE Max LED indicates the Switch reaches the maximum power budget defined by the administrator via PoE System Settings page of Web GUI or the default power budget of 65 Watts. The blinking amber of PoE Max LED represents the switch is in guradband mode (available power left is less 7 watts).
- **Port Link/Act/Speed LED (1-8):** The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When a port has an amber light, this indicates that the port is running on 10M or 100M. When it has a green light it is running on 1000M.
- **Port Link/Act/Speed LED (9F-10F):** The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When the port LED glows in amber, it indicates the port is running on 100M. When the port LED glows in green, it is running on 1000Mbps.
- Mode: By pressing the Mode button, the Port LED will switch between Link/Act and PoE modes.
- **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 via image 1 and image 2, the device will enter the loader mode automatically.



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

- Si le transceiveur optique n'est pas livré avec l'appareil, le manuel d'utilisation doit comporter la description ci-dessous ou son équivalent :« Ce produit est destiné à être utilisé avec un transceiveur optique homologué UL,tension DC3.3V, classe laser l.
- 5

NOTE: The port 1 \sim port 8 are PoE ports. When user press the **Mode** button to PoE mode, only port 1 \sim port 8 will light up.



CAUTION: This equipment can be connected only to PoE networks without routing to the outside plant.

L'équipement est conçu pour une installation dans un bâtiment et ne doit pas être connecté à des réseaux exposés (installations extérieures), notamment des environnements de campus, et l'ITE doit être connecté uniquement à des réseaux PoE sans acheminement vers une installation extérieure." ou équivalent.

NOTE: Once user enter in loader mode, you can use DNA tool (standalone version 2.0.2.4 only (No support by Chrome DNA3.x.x.x)) to download the image or call D-Link Technical Support for further help.

Rear Panel

ß	SWITCH GND	
		54V1.574A ⊚ ⇔⊕
/		

Figure 1.4 – DGS-1210-10P Rear Panel

Power: Connect the supplied AC power cable to this port.

DGS-1210-10MP

8-Port 10/100/1000Mbps, plus 2 SFP Ports (100/1000Mbps) Metro Ethernet PoE switch.

Front Panel



Figure 1.5 – DGS-1210-10MP Front Panel

The front panel of the **DGS-1210-10MP** switch consists out of the following:

- **Power LED**⁽¹⁾: The Power LED lights up when the Switch is connected to a power source.
- **Fan Error:** The FAN LED shows the status of the fans, light off indicates all fans work fine and the red light indicates that one or multiple fans are working abnormally.
- **PoE Max:** The solid amber of PoE Max LED indicates the Switch reaches the maximum power budget defined by the administrator via PoE System Settings page of Web GUI or the default power budget of 130 Watts. The blinking amber of PoE Max LED represents the switch is in guradband mode (available power left is less 7 watts).
- **Port Link/Act/Speed LED (1-8):** The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When a port has an amber light, this indicates that the port is running on 10M or 100M. When it has a green light it is running on 1000M.
- **Port Link/Act/Speed LED (9F-10F):** The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When the port LED glows in amber, it indicates the port is running on 100M. When the port LED glows in green, it is running on 1000Mbps.
- Mode: By pressing the Mode button, the Port LED will switch between Link/Act and PoE modes.
- **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 via image 1 and image 2, the device will enter the loader mode automatically.

CAUTION: The MiniGBIC ports should use UL listed Optical Transceiver product, Rated Laser Class I. 3.3Vdc.
 Si le transceiveur optique n'est pas livré avec l'appareil, le manuel

d'utilisation doit comporter la description ci-dessous ou son équivalent :« Ce produit est destiné à être utilisé avec un transceiveur optique homologué UL,tension DC3.3V, classe laser I.

NOTE: The port 1 ~ port 8 are PoE ports. When user press the **Mode** button to PoE mode, only port 1 ~ port 8 will light up.



CAUTION: This equipment can be connected only to PoE networks without routing to the outside plant.

L'équipement est conçu pour une installation dans un bâtiment et ne doit pas être connecté à des réseaux exposés (installations extérieures), notamment des environnements de campus, et l'ITE doit être connecté uniquement à des réseaux PoE sans acheminement vers une installation extérieure." ou équivalent.



NOTE: Once user enter in loader mode, you can use DNA tool (standalone version 2.0.2.4 only (No support by Chrome DNA3.x.x.x)) to download the image or call D-Link Technical Support for further help.

Rear Panel



Figure 1.6 – DGS-1210-10MP Rear Panel

Power: Connect the supplied AC power cable to this port.

DGS-1210-20

20-Port 10/100/1000Mbps, includes 4 SFP Combo Ports (100/1000Mbps) Metro Ethernet Switch.



Figure 1.7 – DGS-1210-20 Front Panel

The front panel of the **DGS-1210-20** switch consists out of the following:

- **Power LED**⁽¹⁾: The Power LED lights up when the Switch is connected to a power source.
- **Port Link/Act/Speed LED (1-20):** The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When a port has an amber light, this indicates that the port is running on 10M or 100M. When it has a green light it is running on 1000M.
- **Port Link/Act/Speed LED (16F-20F):** The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When the port LED glows in amber, it indicates the port is running on 100M. When the port LED glows in green, it is running on 1000Mbps.
- **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 via image 1 and image 2, the device will enter the loader mode automatically.



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

Si le transceiveur optique n'est pas livré avec l'appareil, le manuel d'utilisation doit comporter la description ci-dessous ou son équivalent :« Ce produit est destiné à être utilisé avec un transceiveur optique homologué UL,tension DC3.3V, classe laser l.



NOTE: Once user enter in loader mode, you can use DNA tool (standalone version 2.0.2.4 only (No support by Chrome DNA3.x.x.x)) to download the image or call D-Link Technical Support for further help.

<u>Rear Panel</u>

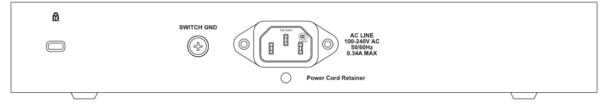


Figure 1.8 – DGS-1210-20 Rear Panel

Power: Connect the supplied AC power cable to this port.

DGS-1210-26

24-Port 10/100/1000Mbps plus 2 SFP Ports (100/1000Mbps) Metro Ethernet Switch.

Front Panel

D-Link Link/Act: 10/100M-Link Act 2 2 4 5 6 7 8			-	
			25 26	
0		****		
DGS-1210-26 •Reset			لبريها لبريها	
Firmer 4.0 D	00 4040 00 Enert Dama			



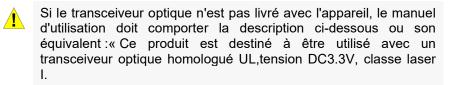
The front panel of the **DGS-1210-26** switch consists out of the following:

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

- **Port Link/Act/Speed LED (1-24):** The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When a port has an amber light, this indicates that the port is running on 10M or 100M. When it has a green light it is running on 1000M.
- **Port Link/Act/Speed LED (25F-26F):** The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When the port LED glows in amber, it indicates the port is running on 100M. When the port LED glows in green, it is running on 1000Mbps.
- **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 via image 1 and image 2, the device will enter the loader mode automatically.



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



NOTE: Once user enter in loader mode, you can use DNA tool (standalone version 2.0.2.4 only (No support by Chrome DNA3.x.x.x)) to download the image or call D-Link Technical Support for further help.

Rear Panel

ĉ.	SWITCH OND	AC LINE 100-2407 AC 3.2 A BAX

Figure 1.10 – DGS-1210-26 Rear Panel

Power: Connect the supplied AC power cable to this port

DGS-1210-28

28-Port 10/100/1000Mbps includes 4 SFP Combo Ports (100/1000Mbps) Metro Ethernet Switch.

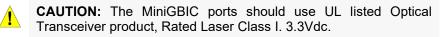
Front Panel D-Littlk Link/Act: 10/100M=Link/# Act I <

The front panel of the **DGS-1210-28** switch consists out of the following:

- **Power LED**⁽¹⁾: The Power LED lights up when the Switch is connected to a power source.
- **Port Link/Act/Speed LED (1-28):** The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to

the port. When a port has an amber light, this indicates that the port is running on 10M or 100M. When it has a green light it is running on 1000M.

- **Port Link/Act/Speed LED (25F-28F):** The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When the port LED glows in amber, it indicates the port is running on 100M. When the port LED glows in green, it is running on 1000Mbps.
- **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 via image 1 and image 2, the device will enter the loader mode automatically.



Si le transceiveur optique n'est pas livré avec l'appareil, le manuel d'utilisation doit comporter la description ci-dessous ou son équivalent :« Ce produit est destiné à être utilisé avec un transceiveur optique homologué UL,tension DC3.3V, classe laser I.

NOTE: Once user enter in loader mode, you can use DNA tool (standalone version 2.0.2.4 only (No support by Chrome DNA3.x.x.x)) to download the image or call D-Link Technical Support for further help.

<u>Rear Panel</u>



Figure 1.12 – DGS-1210-28 Rear Panel

Power: Connect the supplied AC power cable to this port

DGS-1210-28P

28-Port 10/100/1000Mbps includes 4 SFP Combo Ports (100/1000Mbps) Metro Ethernet PoE Switch.

Front Panel	
D-Link Link/Act:10/100M-Link & Act POE:-PWR Fail 2 3 4 5 8 7 8	Î Î Î Î Î Î Î Î Î Î Î Î Î Î Î Î Î Î Î
DGS-1210-28P	

Figure 1.13 – DGS-1210-28P Front Panel

The front panel of the **DGS-1210-28P** switch consists out of the following:

- **Power LED**⁽¹⁾: The Power LED lights up when the Switch is connected to a power source.
- **Fan Error:** The FAN LED shows the status of the fans, light off indicates all fans work fine and the red light indicates that one or multiple fans are working abnormally.
- **PoE Max:** The solid amber of PoE Max LED indicates the Switch reaches the maximum power budget defined by the administrator via PoE System Settings page of Web GUI or the default power budget of

Δ

193 Watts. The blinking amber of PoE Max LED represents the switch is in guradband mode (available power left is less 7 watts).

- **Port Link/Act/Speed LED (1-28):** The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When a port has an amber light, this indicates that the port is running on 10M or 100M. When it has a green light it is running on 1000M.
- **Port Link/Act/Speed LED (25F-28F):** The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When the port LED glows in amber, it indicates the port is running on 100M. When the port LED glows in green, it is running on 1000Mbps.
- Mode: By pressing the Mode button, the Port LED will switch between Link/Act and PoE modes.
- **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 via image 1 and image 2, the device will enter the loader mode automatically.

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

- Si le transceiveur optique n'est pas livré avec l'appareil, le manuel d'utilisation doit comporter la description ci-dessous ou son équivalent :« Ce produit est destiné à être utilisé avec un transceiveur optique homologué UL,tension DC3.3V, classe laser l.
 - **NOTE:** The port 1 ~ port 8 are PoE ports. When user press the **Mode** button to PoE mode, only port 1 ~ port 8 will light up.
- **CAUTION:** This equipment can be connected only to PoE networks without routing to the outside plant.
- L'équipement est conçu pour une installation dans un bâtiment et ne doit pas être connecté à des réseaux exposés (installations extérieures), notamment des environnements de campus, et l'ITE doit être connecté uniquement à des réseaux PoE sans acheminement vers une installation extérieure." ou équivalent.

NOTE: Once user enter in loader mode, you can use DNA tool (standalone version 2.0.2.4 only (No support by Chrome DNA3.x.x.x)) to download the image or call D-Link Technical Support for further help.

Rear Panel

ß	SWITCH GND	
		AC LINE 100-240V AC 5.00 AC
		Power Cord Retainer
		- .

Figure 1.14 – DGS-1210-28P Rear Panel

Power: Connect the supplied AC power cable to this port

DGS-1210-28MP

28-Port 10/100/1000Mbps includes 4 SFP Combo Ports (100/1000Mbps) Metro Ethernet PoE Switch.

Front Panel



Figure 1.15 – DGS-1210-28MP Front Panel

The front panel of the DGS-1210-28MP switch consists out of the following:

- **Power LED**⁽¹⁾: The Power LED lights up when the Switch is connected to a power source.
- **Fan Error:** The FAN LED shows the status of the fans, light off indicates all fans work fine and the red light indicates that one or multiple fans are working abnormally.
- **PoE Max:** The solid amber of PoE Max LED indicates the Switch reaches the maximum power budget defined by the administrator via PoE System Settings page of Web GUI or the default power budget of 370 Watts. The blinking amber of PoE Max LED represents the switch is in guradband mode (available power left is less 7 watts).
- **Port Link/Act/Speed LED (1-28):** The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When a port has an amber light, this indicates that the port is running on 10M or 100M. When it has a green light it is running on 1000M.
- Mode: By pressing the Mode button, the Port LED will switch between Link/Act and PoE modes.
- **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 via image 1 and image 2, the device will enter the loader mode automatically.



1

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

- Si le transceiveur optique n'est pas livré avec l'appareil, le manuel d'utilisation doit comporter la description ci-dessous ou son équivalent :« Ce produit est destiné à être utilisé avec un transceiveur optique homologué UL,tension DC3.3V, classe laser l.
 - **NOTE:** The port 1 ~ port 8 are PoE ports. When user press the **Mode** button to PoE mode, only port 1 ~ port 8 will light up.
 - **CAUTION:** This equipment can be connected only to PoE networks without routing to the outside plant.
- L'équipement est conçu pour une installation dans un bâtiment et ne doit pas être connecté à des réseaux exposés (installations extérieures), notamment des environnements de campus, et l'ITE doit être connecté uniquement à des réseaux PoE sans acheminement vers une installation extérieure." ou équivalent.



NOTE: Once user enter in loader mode, you can use DNA tool (standalone version 2.0.2.4 only (No support by Chrome DNA3.x.x.x)) to download the image or call D-Link Technical Support for further help.

Rear Panel

۵	SWITCH GND	
	6	AC LINE 100-2407 AC 3.3X MAX
		Power Cord Retainer
	Figure 1.16 – DGS-12	210-28MP Rear Panel

Power: Connect the supplied AC power cable to this port

DGS-1210-52

52-Port 10/100/1000Mbps includes 4 SFP Combo Ports (100/1000Mbps) Metro Ethernet Switch.

Front Panel

D-Link 1 2 3 4 5 6 7 8 8 10 11 12 13 14 15 16 17 18 13 20 21 22 23 24 25 28 27 28 29 30 31 52 33 34 35 36 97 58 59 40 41 42 43 44 45 45 47 48	49 50 51 52 49 50 51 52
	ŦŦ
DG \$-1210-52	

Figure 1.17 – DGS-1210-52 Front Panel

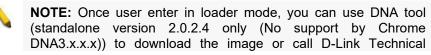
The front panel of the **DGS-1210-52** switch consists out of the following:

- **Power LED**⁽¹⁾: The Power LED lights up when the Switch is connected to a power source.
- **Port Link/Act/Speed LED (1-52):** The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When a port has an amber light, this indicates that the port is running on 10M or 100M. When it has a green light it is running on 1000M.
- **Port Link/Act/Speed LED (49F-52F):** The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When the port LED glows in amber, it indicates the port is running on 100M. When the port LED glows in green, it is running on 1000Mbps.
- **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 via image 1 and image 2, the device will enter the loader mode automatically.



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

Si le transceiveur optique n'est pas livré avec l'appareil, le manuel d'utilisation doit comporter la description ci-dessous ou son équivalent :« Ce produit est destiné à être utilisé avec un transceiveur optique homologué UL,tension DC3.3V, classe laser l.



Support for further help.

<u>Rear Panel</u>

AC LINE 109-2404C SURVAC SURVAC	SWITCH GND	0
Power Cord Retainer	0	

Figure 1.18 – DGS-1210-52 Rear Panel

Power: Connect the supplied AC power cable to this port

DGS-1210-52MP

52-Port 10/100/1000Mbps includes 4 SFP Combo Ports (100/1000Mbps) Metro Ethernet PoE Switch.

Front Panel
D-Link DG-1210-52MP U [LINAct] 10/1004 Link © Act DG-1210-52MP U [LINACt] 10/1004 Link © Act DG-1210-52MP D
Reset LEDMode

Figure 1.19 – DGS-1210-52MP Front Panel

The front panel of the **DGS-1210-52MP** switch consists out of the following:

- **Power LED**⁽¹⁾: The Power LED lights up when the Switch is connected to a power source.
- **Fan Error:** The FAN LED shows the status of the fans, light off indicates all fans work fine and the red light indicates that one or multiple fans are working abnormally.
- **PoE Max:** The solid amber of PoE Max LED indicates the Switch reaches the maximum power budget defined by the administrator via PoE System Settings page of Web GUI or the default power budget of 370 Watts. The blinking amber of PoE Max LED represents the switch is in guradband mode (available power left is less 7 watts).
- **Port Link/Act/Speed LED (1-52):** The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When a port has an amber light, this indicates that the port is running on 10M or 100M. When it has a green light it is running on 1000M.
- **Port Link/Act/Speed LED (49F-52F):** The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When the port LED glows in amber, it indicates the port is running on 100M. When the port LED glows in green, it is running on 1000Mbps.
- Mode: By pressing the Mode button, the Port LED will switch between Link/Act and PoE modes.
- **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 via image 1 and image 2, the device will enter the loader mode automatically.



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

Si le transceiveur optique n'est pas livré avec l'appareil, le manuel d'utilisation doit comporter la description ci-dessous ou son équivalent :« Ce produit est destiné à être utilisé avec un transceiveur optique homologué UL,tension DC3.3V, classe laser l.

NOTE: The port 1 ~ port 8 are PoE ports. When user press the **Mode** button to PoE mode, only port 1 ~ port 8 will light up.

- **CAUTION:** This equipment can be connected only to PoE networks without routing to the outside plant.
- L'équipement est conçu pour une installation dans un bâtiment et ne doit pas être connecté à des réseaux exposés (installations extérieures), notamment des environnements de campus, et l'ITE doit être connecté uniquement à des réseaux PoE sans acheminement vers une installation extérieure." ou équivalent.

NOTE: Once user enter in loader mode, you can use DNA tool (standalone version 2.0.2.4 only (No support by Chrome DNA3.x.x.x)) to download the image or call D-Link Technical Support for further help.

Rear Panel



Figure 1.20 – DGS-1210-52MP Rear Panel

Power: Connect the supplied AC power cable to this port

LED Indicators

The Switch supports LED indicators for Power, Fan, and Link/Act for each port. The following shows the LED indicators for the DGS-1210 series Metro Ethernet Switch along with an explanation of each indicator.

D-Link "	k/Act:10/100M=linköAct Po 1000M=linköAct	E:=PWR Fail 🔶 🗸 🛔
	PoE Max LED Mode Link/Act	i 📩 💼
	PoE Max Fan	Reset
DGS-1210-28MP		

Figure 1.21 –LED Indicators on DGS-1210 series

Location	LED Indicative	Color	Status	Description
	Power	Green	Solid Light	Power on
	rowei	Green	Light off	Power off
	Fan Error	Red	Solid light	The fan has runtime failure and is brought offline.
Per Device	PoE Max.	Amber	Solid light	The PoE Max LED lights up when the total PoE output of Switch reached or exceeded: DGS-1210-10P: 65 Watts DGS-1210-10MP: 130 Watts DGS-1210-28P: 193 Watts DGS-1210-28MP and DGS-1210- 52MP: 370 Watts

				In the meantime, no additional PoE device can be supported.
			Blinking Amber	Total PoE output of Switch reached guard band mode. (Max. PoE budget < 7 Watts)
			Light off	When the system power usage does not reach the guard band range.
			Solid Green	When there is a secure 1000Mbps Ethernet connection (or link) at any of the ports.
	Link/Act		Blinking Green	When there is reception or transmission (i.e. Activity—Act) of data occurring at a 1000Mbps Ethernet connected port.
LED Per		Green/Amber	Solid Amber	When there is a secure 10/100Mbps Ethernet connection (or link) at any of the ports.
10/100/1000Mbps Copper Port			Blinking Amber	When there is reception or transmission (i.e. Activity—Act) of data occurring at a 10/100Mbps Ethernet connected port.
			Light off	No link.
	PoE Mode	Green	Solid Light	Power feeding.
		Amber	Solid Light	Error Condition.
		Off	Solid Off	No Power feeding.
	Gi Link/Act	Green/Amber	Solid Green	When there is a secure 1000Mbps Ethernet connection (or link) at any of the ports.
LED Dor			Blinking Green	When there is reception or transmission (i.e. Activity—Act) of data occurring at a 1000Mbps Ethernet connected port.
LED Per 100/1000Mbps SFP Port			Solid Amber	When there is a secure 100Mbps 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 a 100Mbps Ethernet connected port.
		Off	Solid off	No link.

2 Hardware Installation

This chapter provides unpacking and installation information for the D-Link Metro Ethernet Switch.

Safety Cautions

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

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

- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:
 - Install the power supply before connecting the power cable to the power supply.
 - Unplug the power cable before removing the power supply.
 - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.
- Move products with care; ensure that all casters and/or stabilizers are firmly connected to the system. Avoid sudden stops and uneven surfaces.

Step 1: Unpacking

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

- One D-Link DGS-1210 Metro Ethernet 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.

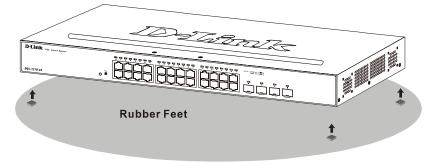


Figure 2.1 – Attach the adhesive rubber pads to the bottom

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

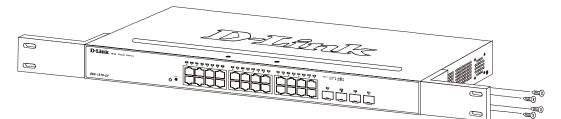


Figure 2.2 – Attach the mounting brackets to the Switch

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

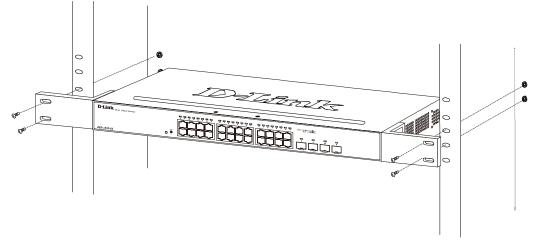


Figure 2.3 – Mount the Switch in the rack or chassis

Please be aware of following safety Instructions when installing:

A) Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (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)."

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.

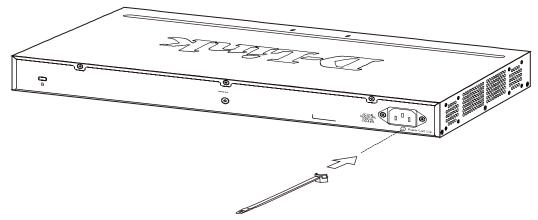


Figure 2.4 – Insert Tie Wrap to the Switch

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

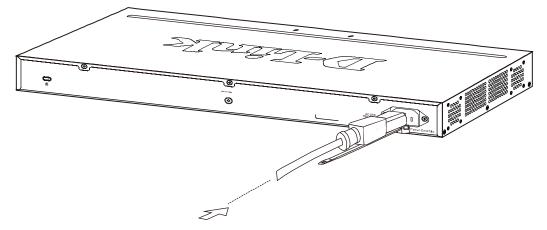


Figure 2.5 – Connect the power cord to the Switch

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

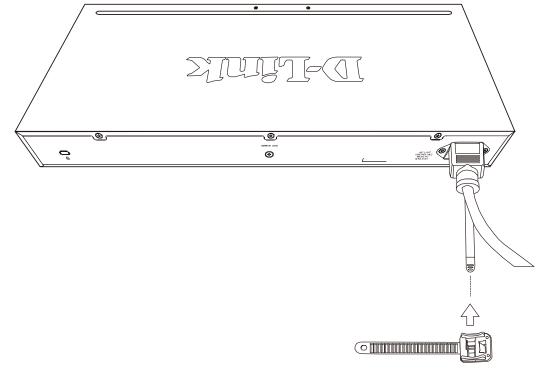


Figure 2.6 – Slide the Retainer through the Tie Wrap

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

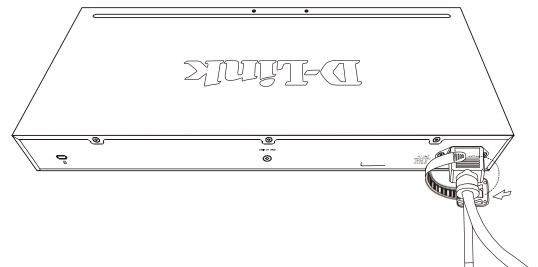


Figure 2.7 – Circle around the power cord

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

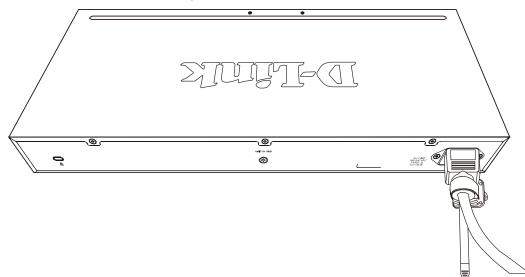


Figure 2.8 – Secure the power cord

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

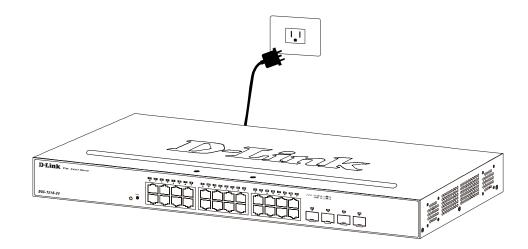


Figure 2.9 – Plugging the switch into an outlet

Power Failure

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

Grounding the Switch

This section describes how to connect the DGS-1210 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.

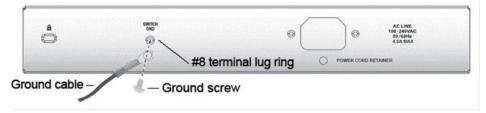


Figure 2.10 – Connect a Grounding Cable



CAUTION: The equipment power supply cord shall be connected to a socket-outlet with earthing connection.



Le cordon d'alimentation de l'équipement doit être branché sur une prise de courant dotée d'une connexion à la terre.

3 Getting Started

This chapter introduces the management interface of D-Link Metro Ethernet Switch.

Management Options

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

Each switch must be assigned its own IP Address, which is used for communication with Web-Based Management or a SNMP network manager. The PC should have an IP address in the same range as the switch. Each switch can allow up to four users to access to 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: Web Browser via IE8(or later version), Firefox, Chrome and 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.

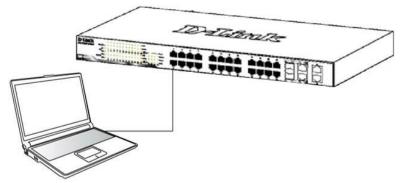


Figure 3.1 – Connected Ethernet cable

Login Web-based Management

In order to login and configure the switch via an Ethernet connection, the PC must have an IP address in the same subnet as the switch. For example, if the switch has an IP address of **10.90.90.90**, the PC should have an IP address of **10.x.y.z** (where x/y is a number between $0 \sim 254$ and z is a number between $1 \sim 254$), and a subnet mask of **255.0.0.0**. There are two ways to launch the Web-based Management, you may either click the Web Access button at the top of the SmartConsole Utility or open the web browser and enter **10.90.90.90**. (the factory-default IP address) in the address bar. Then press <Enter>.

🥖 D-Link Welcome - Windows Internet Explorer						
Eile	<u>E</u> dit	⊻iew	F <u>a</u> vorites	<u>T</u> ools	Help	

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.

The web configuration can also be accessed through the SmartConsole Utility. Open the SmartConsole Utility and double-click the switch as it appears in the Monitor List. This will automatically load the web configuration in your web browser.

When the following logon dialog box appears, enter the password and choose the language of the Webbased 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 password is **admin** and the language is **English**.

Connect to 10.90.90).90
Enter your usernar	ne and password
Username	
Password	
	OK Cancel

Figure 3.3 – Logon Dialog Box

Smart Wizard

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

Web-based Management

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

D-Link Network Assistant

D-Link Network Assistant (DNA) is a program that is used to discover switches which are in the same layer 2 network segment as your PC. You can download the DNA utility from <u>http://tools.dlink.com/intro/dna/</u>. Please go to above link for details.

4 Web-based Switch Configuration

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

Web-based Management

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

	The Transformation of the International Inte		**********		
D-Link	D-Link link/Act:10/100M=Link@Act PoE= 1000M=Link@Act =1				Refresh I 10 secs
Building Networks for People			루루루 루루루!		Apply
💾 Save 🚽 🌠 Tools 🚽 🔇 Oi	nline Help			Logged in as Administrator, an	onymous - 10.90.90.123 <u>ທ</u> Lo
DGS-1210-28MP					
E Bustem	Device Information				O Safeguard
E Configuration					
±∭QoS t∭RMON	Device Information Device Type	DGS-1210-28MP	System Time	11:07:36 01 01 2019	
	System Name	D03-1210-20MP	System Up Time	0 days, 11 hours, 7 mins, 13 seconds	
🖬 🥌 Monitoring	System Location		MAC Address	EC-AD-E0-62-AF-A0	
- ACL	System Contact		IP Address	10.90.90.90	
E~ILDP	Boot Version	2.00.004	Subnet Mask	255.0.0.0	
	Firmware Version	2.00.005	Hardware Version	R1	
	Default Gateway	0.0.0.0	Serial Number	QBDES12105200	
	Login Timeout (minutes)	5			
	Device Status and Quick Cont	figurations			
	SNMP Status	Enabled Settings	Port Mirroring	Disabled Settings	
	802.1X Status	Enabled Settings	QinQ Settings	Disabled Settings	
	802.1Q Management VLAN	Enabled Settings	Safeguard Engine	Enabled Settings	
	DHCP Client	Disabled Settings	IGMP Snooping	Disabled Settings	
	Jumbo Frame	Disabled Settings	Power Saving	Disabled Settings	
					-

Figure 4.1 – 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**.

Item Area	Description		
Tool Bar	To provide a quick and convenient way for essential utility functions like firmware and configuration management.		
Function Tree	By choosing different functions in the Function Tree , you can change all the settings in the Main Configuration Screen .		
Main Configuration Screen	To display 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.

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

Tool Bar > Save Menu

The Save Menu provides Save Configuration and Save Log functions.

H Save	-	*	Tools
Save Confi	gura	tion	
Save Log			
Figure 4.2	– Sa	ave l	Menu

Save Configuration

Select to save the entire configuration changes to configuration ID 1 or 2 you have made to the device to switch's non-volatile RAM.

Save Config 0 s	Bafeguard
Please press the button to save the config of device. Save Config	
Figure 4.2 – Save Configuration	

Save Log

Save the log entries to your local drive and a pop-up message will prompt you for the file path. You can view or edit the log file by using text editor (e.g. Notepad).

Save Log	Safeguard
Save log to file : Save Log	
Figure 4.3 – Save Log	

Tool Bar > Tools Menu

The Tools Menu offers global function controls such as Reset, Reset System, Reboot Device, Configuration Backup & Restore, Firmware Backup & Upgrade and Flash Information.

H :	Save	-	*	Tools	-		Online	
	Rese	et Sys	stem				-	
🚬 D	Rebo	oot D	evice					
÷	E Configuration Backup & Restore							
÷	🗄 🗐 System Log Backup							
+)	Firm	ware	Back	up & U	pgra	de		
+	Firm	ware	Infor	mation				
141		Figu	re 4.4	– Tool	Menu	ı		

Reset System

Provide variable safe reset options for the Switch. User may chose any one of these options to perform system reset.

Reset System	O Safeguard
Reset System:	
Reset system. (Reset everything.)	
 Reset system exclude system IP. (Reset everything but keep system IP address.) 	
 Reset system exclude VLAN and system IP. (Reset everything but keep system IP address and VLAN configuration.) 	
	Apply
Figure 4.9 – Tool Menu > Reset	

Reboot Device

Provide a safe way to reboot the system. Select **YES** or **NO** to save the current settings before action. And click **Reboot** to restart the switch.



Figure 4.11 – Tool Menu > Reboot Device

Configuration Backup and Restore

Allow the current configuration settings to be saved to a file (not including the password), and if necessary, you can restore configuration settings from this file. Two methods can be selected: **HTTP** or **TFTP**.

Configuration	on Backup and Restore		O Safeguard
HTTP			
	Backup current settings to file :	Backup	
	Restore saved settings from file :	選擇檔案 未選擇任何檔案	
		Restore	
TFTP			
	TFTP Server IP Address :	IPv4	
		O IPv6	
	TFTP File Name		
	Backup current settings to file :	Backup	
	Restore saved settings from file :	Restore	

Figure 4.12 – Tool Menu > Configure Backup and Restore

HTTP: Backup or restore the configuration file to or from your local drive.

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

Click Choose File to browse your inventories for a saved backup settings file.

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

TFTP: TFTP (Trivial File Transfer Protocol) is a file transfer protocol that allows you to transfer files to a remote TFTP server. **TFTP Server IP Address** with IPv4 or IPv6 address and **TFTP File Name** for the configuration file you want to save to / restore from.

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

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



Note: Switch will reboot after restore, and all current configurations will be lost.

System Log Backup

Backup system logs via HTTP or TFTP.

System Lo	g Backup		O Safeguard
 HTTP TFTP 	Backup current log to file :	Backup	
0	TFTP Server IP Address :	IPv4 IPv6	
	TFTP File Name Backup current settings to file :	Backup	

HTTP: Backup log to your local drive directly from HTTP.

TFTP: Specify IP address (IPv4 or IPv6) and file name. Click Backup to start process.

Firmware Backup and Upgrade

Allow for the firmware to be saved, or for an existing firmware file to be uploaded to the Switch. Two methods can be selected: **HTTP** or **TFTP**.

Firmware Backup	and Upgrade		😑 Safeguard
HTTP			
Backup fi	rmware to file :	Image_id 1 T Backup	
Upgrade 1	firmware from file :	Choose File No file chosen	
		Upgrade	
TFTP			
TFTP Ser	ver IP Address :	IPv4	
		□ IPv6	
TFTP File	Name		
Backup fi	mware to file :	Image_id 1 V Backup	
Upgrade f	firmware from file :	Upgrade	

Figure 4.13 – Tool Menu > Firmware Backup and Upload

HTTP: Backup or upgrade the firmware to or from your local PC drive.

Backup firmware to file: Select image_id 1 or image_id 2.

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

Click Choose File to browse your inventories for a saved firmware file.

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

TFTP: Specifies the Image_id 1 or Image_id 2 to backup or upgrade the firmware to or from a remote TFTP server. Specifies **TFTP Server IP Address** with IPv4 or IPv6 address and **TFTP File Name** for the configuration file you want to save to / restore from.

Backup firmware to file: Select Image_id1 or Image_id 2.

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

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



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

Firmware Information

This page displays the firmware information and allow user to identify the image used for system boot.

irmware Information					
Version	Size(B)	Update Time	Boot up firmware		
2.00.005	11082096	2/1/2019 05:57:17	Boot Up		
2.00.005	11082096	1/1/2019 00:42:16	Boot Up		
	Version 2.00.005	Version Size(B) 2.00.005 11082096	Version Size(B) Update Time 2.00.005 11082096 2/1/2019 05:57:17		

Figure 4.14 – Tool Menu > Flash Information

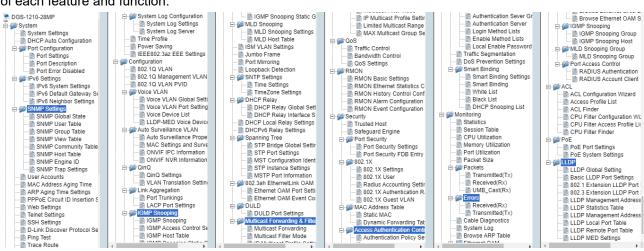
Tool Bar > Online Help

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



Function Tree

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





Device Information

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

				O Safeguard
DGS-1210-28MP	System Time	11:41:07 01 01 2019		
	System Up Time	0 days, 11 hours, 40 min	is, 45 seconds	
	MAC Address	EC-AD-E0-62-AF-A0		
	IP Address	10.90.90.90		
2.00.004	Subnet Mask	255.0.0.0		
2.00.005	Hardware Version	R1		
0.0.0.0	Serial Number	QBDES12105200		
5				
rations				
Enabled Settings	Port Mirroring	Disabled Settings		
Enabled Settings	QinQ Settings	Disabled Settings		
Enabled Settings	Safeguard Engine	Enabled Settings		
Disabled Settings	IGMP Snooping	Disabled Settings		
Disabled Settings	Power Saving	Disabled Settings		
Enabled Set	ings Port M	lirroring	Disabled	Settings
		-		
Enabled Set	ungs QinQ	Settings	Disabled	<u>Settings</u>
Enabled Set	tings Safeg	lard Engine	Enabled	<u>Settings</u>
Disabled Set	tings IGMP	Snooping	Disabled	Settings
			Disabled	Settings
	2.00.004 2.00.005 0.0.0 5 rations Enabled Settings Enabled Settings Disabled Settings Disabled Settings Disabled Settings Disabled Settings Disabled Settings	2.00.004 2.00.004 2.00.005 0.0.0 5 rations Enabled Settings Enabled Settings Disabled Settings Enabled Se	System Up Time 0 days, 11 hours, 40 min MAC Address EC-AD-E0-62-AF-A0 IP Address 10.90.90.90 2.00.004 Subnet Mask 255.0.0 2.00.005 Hardware Version R1 0.0.0 Serial Number OBDES12105200 5 GinQ Settings Disabled Settings Enabled Settings QinQ Settings Disabled Settings Disabled Settings IGMP Snooping Disabled Settings Disabled Settings Power Saving Disabled Settings Enabled Settings QinQ Settings QinQ Settings Disabled Settings QinQ Settings Safeguard Engine Enabled Settings QinQ Settings Safeguard Engine Enabled Settings QinQ Settings Safeguard Engine IBabled Settings QinQ Settings Safeguard Engine IBabled Settings QinQ Settings Safeguard Engine IBabled Settings IGMP Snooping IGMP Snooping	System Up Time MAC Address 0 days, 11 hours, 40 mins, 45 seconds MAC Address EC-AD-E0-62-AF-A0 IP Address 10.90.90.90 2.00.004 Subnet Mask 255.0.0 2.00.005 Hardware Version R1 0.0.0 Serial Number QBDES12105200 5 GinQ Settings Disabled Enabled Settings QinQ Settings Disabled Settings IGMP Snooping Disabled Settings Disabled Settings IGMP Snooping Disabled Enabled Settings Disabled Settings IGMP Snooping Disabled Enabled Settings Disabled Settings QinQ Settings Disabled Disabled Settings Disabled Settings IGMP Snooping Disabled Enabled Settings Disabled

Figure 4.17 – Device Information

It also offers an overall status of common software features:

SNMP Status: Click Settings to link to SNMP > SNMP > SNMP Global Settings. Default is disabled.

802.1X Status: Click **Settings** to link to AAA > 802.1X > 802.1X Settings. Default is disabled.

802.1Q Management VLAN: Click Settings to configure management VLAN.

DHCP Client: Click **Settings** to link to System > System Settings. Default is disabled.

Jumbo Frame: Click Settings to link to L2 Functions > Jumbo Frame. Default is disabled.

Port Mirroring: Click Settings to link to L2 Functions > Port Mirroring. Default is disabled.

QinQ Setting: Click Settings to link to Configuration > QinQ > QinQ Settings. Default is disabled.
Safeguard Engine: Click Settings to link to Security > Safeguard Engine. Default is enabled.
IGMP Snooping: Click Settings to link to L2 Functions > Multicast > IGMP Snooping. Default is disabled.
Power Saving: Click Settings to link to System > Power Saving. Default is disabled

System > System Settings

The System Setting allows the user to configure the IP address and the basic system information of the Switch.

System Settings		O Safeguard
IP Information		
Static DHCP IP Address Subnet Mask Gateway DHCP Option 12 State DHCP Option 12 Host Name	DHCP retry time(5~120) 7 times Note: DHCP retry interval:5 seconds 10 . 90 . 90 . 90 255 . 0 . 0 . 0 0 . 0 . 0 . 0 Disabled • DGS-1210-28MP	
System Information		Apply
System Name System Location System Contact Login Timeout (3-30 minutes)	 5	
		Apply

Figure 4.18 – System > System Settings

IPv4 Information: There are three ways for the switch to obtain an IP address: Static, DHCP (Dynamic Host Configuration Protocol) and BOOTP.

When using static mode, the **Interface Name**, **VLAN Name**, **Interface Admin State**, **IPv4 Address**, **NetMask** and **Gateway** can be manually configured. When using DHCP mode, the Switch will first look for a DHCP server to provide it with an IP address (including network mask and default gateway) before using the default or previously entered settings. By default the IP setting is static mode with IP address is **10.90.90.90** and subnet mask is **255.0.0.0**.

DHCP Option 12 State: Specifies the DHCP option 12 state is enabled or disabled.

DHCP Option 12 Host Name: Specifies the host name for DHCP.

DHCP Retry Times: Specifies the retry time of DHCP.

System Information: The fields for **System Name** and **System Location** which provide network administrator unique identification information for different switches. Also, system information can be read and printed on SmartConsole utility.

Login Timeout: The Login Timeout controls the idle time-out period for security purposes, and when there is no action for a specific time span in the Web-based Management. If the current session times out (expires), the user is required a re-login before using the Web-based Management again. Selective range is from 3 to 30 minutes, and the default setting is 5 minutes.

System > DHCP Auto Configuration

The DHCP Auto Configuration page allows user to enable the DHCP Auto Configuration feature on the Switch. When enabled, the Switch becomes a DHCP client and gets the configuration file from a TFTP server automatically on next boot up. To accomplish this, the DHCP server must deliver the TFTP server IP address and configuration file name information in the DHCP reply packet. The TFTP server must be up and running and store the necessary configuration file in its base directory when the request is received from the Switch.

DHCP Auto Configuration			0	Safeguard
Auto Configuration State: Timeout (1-65535) 5	Enabled	Disabled	[Apply
The DHCP autoconfiguration function on the sw	witch will load a previous	y saved configuration file for current use.		
Note: If the switch is unable to complete the aut	toconfiguration process,	the previously saved local configuration file pres	sent in switch memory will be load	led.

Figure 4.22 – System > DHCP Auto Configuration

System > Port Settings

In the Port Setting page, the status of all ports can be monitored and adjusted for optimum configuration. By selecting a range of ports (**From Port** and **To Port**), the **Speed** can be set for all selected ports by clicking **Apply**. Press the **Refresh** button to view the latest information.

Port Setti	ngs						O Safegua
From Port 01	To Port Z8	Media Copper ▼	Speed Auto	MDI/MDIX Auto 🔻	Flow Control Disabled ▼	Address Learning Enabled ▼	Apply
							Refresh
Port	Link Status	Speed		MDI/MDIX	Flow Control	Address Learning	
1	1000M Full	Auto		Auto	Disabled	Enabled	
2	Down	Auto		Auto	Disabled	Enabled	
3	Down	Auto		Auto	Disabled	Enabled	
4	Down	Auto		Auto	Disabled	Enabled	
5	Down	Auto		Auto	Disabled	Enabled	
6	Down	Auto		Auto	Disabled	Enabled	
7	Down	Auto		Auto	Disabled	Enabled	
8	Down	Auto		Auto	Disabled	Enabled	
9	Down	Auto		Auto	Disabled	Enabled	
10	Down	Auto		Auto	Disabled	Enabled	
11	Down	Auto		Auto	Disabled	Enabled	
12	Down	Auto		Auto	Disabled	Enabled	
13	Down	Auto		Auto	Disabled	Enabled	
14	Down	Auto		Auto	Disabled	Enabled	
15	Down	Auto		Auto	Disabled	Enabled	
16	Down	Auto		Auto	Disabled	Enabled	•

Figure 4.20 – System > Port Settings

Speed: Gigabit Fiber connections can operate in 1000M Auto or Disabled. Copper connections can operate in Forced Mode settings (2500M Full, 1000M Full, 100M Full, 100M Half, 10M Full, 10M Half), Auto, or Disabled. The default setting for all ports is **Auto**.



NOTE: Be sure to adjust port speed settings appropriately after changing the connected cable media types.



NOTE: All ports do not support MDI/MDI-X function when the speed links to 1000M force mode.

MDI/MDIX:

A **medium dependent interface (MDI)** port is an Ethernet port connection typically used on the Network Interface Card (NIC) or Integrated NIC port on a PC. Switches and hubs usually use **Medium dependent interface crossover (MDIX)** interface. When connecting the Switch to end stations, user have to use straight through Ethernet cables to make sure the Tx/Rx pairs match up properly. When connecting the Switch to other networking devices, a crossover cable must be used.

This switch provides a configurable **MDI/MDIX** function for users. The switches can be set as an MDI port in order to connect to other hubs or switches without an Ethernet crossover cable.

Auto MDI/MDIX is designed on the switch to detect if the connection is backwards, and automatically chooses MDI or MDIX to properly match the connection. The default setting is "**Auto**" **MDI/MDIX**.

Flow Control: You can enable this function to mitigate the traffic congestion. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use backpressure flow control. The default setting is Disabled.

Auto Downgrade: Enable or disable automatically downgrading advertised speed. This function only takes effect, when **Speed** is configured as Auto.

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

System > Port Description

Port description can be given on this page.

Port Description	1		😑 Safeguard
From Port 01 T	To Port 52 ▼	Description	Apply
Port		Description	
01			
02			
03			
04			
05			
06			
07			
08			
09			
10			
11			
12			
13			

Figure 4.21 – System > Port Description

From Port / To Port: Specifies the range of ports to describe.

Description: Specifies the description for the chosen ports.

Click **Apply** to set the description in the table.

System > Port Configuration > Port Error Disabled

The Port Error Disabled page displays the information about ports that have had their connection status disabled, for reasons such as STP loopback detection or link down status.

F	ort Error Disabled				
	Port	Port State	Connection Status	Reason	

Figure 4.26 – System > Port Configuration > Port Error Disabled

Port: Displays the port that has been error disabled.

Port State: Describes the current running state of the port, whether Enabled or Disabled.

Connection Status: This field will read the uplink status of the individual ports, whether Enabled or Disabled. **Reason:** Describes the reason why the port has been error-disabled, such as a STP loopback occurrence.

System > IPv6 Setting > IPv6 System Settings

Used to configure IPv6 parameters for system interface.

IPv6 System Settings							0	Safeguard
IPv6 System Settings Interface Name DHCPv6 Client	System Disabled	¥	IPv6 State IPv6 Network Address (e.g.: 3710)::1/64)	Enabled	T		Apply
NS Retransmit Time Settings NS Retransmit Time (1-3600)		1	sec.					Apply
Automatic Link Local State Set Automatic Link Local Address	ttings	Disabled •						Apply
View All IPv6 Address	•		IPv6 A	ddress				
			< < Table is empty >					

IPv6: Options to **enable/disable** IPv6 address of system interface.

DHCPv6 Client: Options to enable/disable DHCPv6 client mode on system interface.

NS Retransmit Time Settings: Specify the time period for sending NS.

Automatic Link Local State Setting: Options to enable/disable Link Local address of system interface.

System > IPv6 Setting > IPv6 Default Gateway Settings

IPv6 Default Gatewa	y Settings		0) Safeguard
IPv6 Default Gateway IP Interface Default Gateway Metric	System	(e.g.: 3FFE::1)	Create	Delete
Total Entries: 0				
Prefix	Next Hop < < `	IP Interface Table is empty > >	Protocol	Metric

Default Gateway: Configure the specific IPv6 address as default by click Create.

System > IPv6 Setting > IPv6 Neighbor Settings

IPv6 Neighbor Settings				Safeguard
Interface Name Neighbor IPv6 Address Link Layer MAC Address	System]		Apply
Interface Name State	System All ▼			Find Clear
Total Entries: 0				
Neighbor	r IPv6 Address	Link Layer MAC Address < < Table is empty > >	Interface Name	State

Neighbor IPv6 Address: Specifies the neighbor IPv6 address.

Link Layer MAC Address: Specifies the link layer MAC address.

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

To search for all the current interfaces on the Switch, go to the second Interface Name field in the middle part of the window, tick the **All** check box. Tick the Hardware option to display all the neighbor cache entries which were written into the hardware table.

State: Use the drop-down menu to select All, Address, Static or Dynamic. When the user selects address from the drop-down menu, the user will be able to enter an IP address in the space provided next to the state option.

System > SNMP Settings > SNMP Global State

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 in the Switch or LAN.

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 click **Apply** to enable the SNMP function.

SNMP Global S	tate Settin	js	 O Safeguard
SNMP Global State:	Enabled	O Disabled	Apply

Figure 4.28 – System > SNMP Settings > SNMP Global State

System > SNMP Settings > SNMP User Table

This page is used to maintain the SNMP user table for the use of SNMPv3. SNMPv3 allows or restricts users using the MIB OID, and also encrypts the SNMP messages sent out between users and Switch.

SNMP User Tab	ble				O Safegua
User Name] *			
Group Name		_]*			
SNMP Version	v1 •		encrypted		
Auth-Protocol	MD5				
			Password		
Priv-Protocol	DES T		Password		
					Apply
(Maximum Entries : 50))				
User Name	Group Name	SNMP Version	Auth Protocol	Priv-Protocol	
ReadOnly	ReadOnly	v1	None	None	Delete
ReadOnly	ReadOnly	v2c	None	None	Delete
ReadWrite	ReadWrite	v1	None	None	Delete
ReadWrite	ReadWrite	v2c	None	None	Delete

Figure 4.29 – System > SNMP Settings > SNMP User Table

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

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

SNMP Version: Specify the SNMP version of the user. Only SNMPv3 encrypts the messages.

Encrypt: Specifies the Encrypt is enabled or disabled when the SNMP Version is V3.

Auth-Protocol/Password: Specify either HMAC-MD5-96 or HMAC-SHA to be the authentication protocol. Enter a password for SNMPv3 encryption in the right column.

Priv-Protocol/Password: Specify either **no authorization** or **DES 56-bit encryption** and then enter a password for SNMPv3 encryption in the right column.

Click **Apply** to create a new SNMP user account, and click **Delete** to remove any existing data.

System > SNMP Settings > SNMP Group Table

This page is used to maintain the SNMP Group Table associating to the users in SNMP User Table. SNMPv3 can control MIB access policy, security policy for a user group directly.

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

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

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

Security Model: Select the SNMP security model.

SNMPv1 - SNMPv1 does not support the security features.

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

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

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

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

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

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

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

SNMP Group	Table					O Safeguar
Group Name Read View Name Write View Name		*	Seci	urity Model urity Level Y View Name	VI NoAuthNoPriv	V V
(Maximum Entries						Apply
Group Name	Read View	Write View	Notify View	Security Model	Security Level	
ReadOnly	ReadWrite		ReadWrite	v1	NoAuthNoPriv	Delete
ReadOnly	ReadWrite		ReadWrite	v2c	NoAuthNoPriv	Delete
	D # 41 11 -	ReadWrite	ReartWrite	v1	NoAuthNoPriv	Delete
ReadWrite	ReadWrite	Readwhite	Readwhite	VI.	INO/Addition The	Delete

Figure 4.30– System > SNMP Settings > SNMP Group Table

System > SNMP Settings > SNMP View Table

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

SNMP View Table Co	onfiguration			O Safeguard
View Name	*			
Subtree OID OID Mask				
View Type	Included T			Apply
(Maximum Entries : 50) View Name	Subtree OID	OID Mask	View Type	
ReadWrite	1	1	Included	Delete

Figure 4.31 – System > SNMP Settings > SNMP View Table

View Name: 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.

OID Mask: The mask of the Subtree OID. 1 means this object number is concerned, 0 means do not concerned. For example 1.3.6.1.2.1.1 with mask 1.1.1.1.1.0 means 1.3.6.1.2.1.X.

View Type: Specify the configured OID is Included or Excluded that a SNMP manager can access.

Click **Apply** to create a new view, **Delete** to remove an existing view.

System > SNMP Settings > SNMP Community Table

This page is used to maintain the SNMP community string of the SNMP managers using the same community string are permitted to gain access to the Switch's SNMP agent.

Community Name: Name of the community string

User Name (View Policy): Specify the read/write or read-only level permission for the MIB objects accessible to the SNMP community.

SNMP Community Table Configuration		O Safeguard
Community Name User Name (View Policy)	r ReadOnly ▼	Apply
(Maximum Entries:10)		
Community Name	User Name	
public	ReadOnly	Delete
private	ReadWrite	Delete

Figure 4.32 – System > SNMP Settings > SNMP Community Table

Click Apply to create a new SNMP community, Delete to remove an existing community.

System > SNMP Settings > SNMP Host Table

This page is to configure the SNMP trap recipients.

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

SNMP Version: Specify the SNMP version to be used to the management host.

Community String/SNMPv3 User Name: Specify the community string or SNMPv3 user name for the management host.

SNMP Host Table			O Safeguard
Host IP Address		● IPv4 ○ IPv6	
SNMP Version	V1	▼	
Community String/ SNMPv3 User Name		*	
			Apply
(Maximum Entries : 10)			
Host IP Address	SNMP Version	Community Name/SNMPv3 User Name	

Figure 4.33– System > SNMP Settings > SNMP Host Table

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

System > SNMP Settings > SNMP Engine ID

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

Input the E	Engine ID then clic	k Apply to apply the changes and click Default resets to	o default value.
	SNMP Engine ID		O Safeguard
	Engine ID	4447532d313231302d3238509cd643604fa4	ly Default
	Note: Engine ID length is 10-64, 1	he accepted character is from 0 to F.	

Figure 4.34 – System > SNMP Settings > SNMP Engine ID

System > SNMP Settings > SNMP Trap Settings

The SNMP Trap Settings page provide user to Specify whether the device can send SNMP notifications.

NMP Trap Configuration	O Safegu
Trap Settings	
SNMP Authentication Traps	
System Coldstart Traps	
System Warmstart Traps	
Port Link Up / Link Down	
RSTP Port State Change	
Firmware Upgrade State	
Trap notification if PoE Power On / Off	
Trap notification if PoE Power Error	
Trap notification if over max power budget	
Port Security Violation	
IMPB Violation	
Loopback Detection occuring / recovery	
DHCP Server Screening	
Duplicate IP Detected	
DHCPv6 Server Screening	
ICMPv6 RA All Node Filter	
Login / Logout	Apply
DULD Traps	Арріу

Figure 4.35 – System > SNMP Settings > SNMP Trap Settings

Туре	Description
SNMP Authentication Traps	Trap event of authentication failure.
System Coldstart Traps	Trap event of device cold boot up.
System Warmstart Traps	Trap event of device warn boot up.
Port Link Up / Link Down	Trap event of link state changes (link down/link up).
RSTP Port State Change	Trap event of Spanning Tree port state change.
Firmware Upgrade State	Trap event of firmware upgrade status (success/failure).
Trap notification if PoE Power On / Off	Trap event of PoE powering state in port basis.
Trap notification if PoE Power Error	Trap event of PoE error.
Trap notification if over max power budget	Trap event when device supplies power over the max power budget.
Port Security Violation	Trap event of violations for port security.
IMPB Violation	Trap event of violations of IP-MAC-Port binding feature.
Loopback Detection occuring / recovery	Trap events of state changes (detected/recovery) for loopback detection.
DHCP Server Screening	Trap events of DHCP sever screening.
Duplicate IP Detected	Trap event when duplicate IP address detected.
DHCPv6 Server Screening	Trap events of DHCPv6 sever screening.
ICMPv6 RA All Node Filter	Trap events of ICMPv6 RA filter feature.
Login / Logout	Trap events for account login/logout.
DULD Traps	Trap events of DULD feature.

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

System > User Accounts

The **User Accounts** page provides user to control user privileges. To add a new user by typing in a **User Name**, **Password** and retype the same password in the **Confirm Password** and choose the level of privilege (*Admin*, *Operator*, or *User*) from the **Access Right** drop-down menu, then click the **Apply** button.

User can modify existing user account in the User Account Table. To change the password, type in the **Old Password**, **New Password** and retype it in the Confirm New Password entry field and select the Encrypt, then click the **Edit** button. To delete the user account, click on the **Delete** button.

Also, the Password Encryption mechanism offer encryption of account password in config file.

User Accounts		O Safeguard
Password Encryption Settings Password Encryption State	Enabled Isabled	Apply
Add User Accounts User Name Access Right Admin Note: Password/User Name should be les	Password Confirm Password s than 15 characters.	Apply
Total Entries : 0 User Name Access Right	Old Password New Password Confirm Password Encrypt	
	< < Table is empty > >	

Figure 4.36– System > User Accounts

System > MAC Address Aging Time

The MAC Address Aging Time page specifies the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC address is allowed to remain idle). To change this, type in a different value representing the MAC address age-out time in seconds.

MAC Address Aging Time		O Safeguard
MAC Address Aging Time (10-1000000)	300 seconds	
·		Apply

Figure 4.37 – System > MAC Address Aging Time

MAC Address Aging Time (10-1000000): Specifies the aging time of MAC address on the Switch. The range is from 10 to 1000000, and the default is 300 seconds.

System > ARP Aging Time Settings

The ARP Aging Time Settings page provides user to globally set the maximum amount of time, in minutes, and Address Resolution Protocol (ARP) entry can remain in the Switch's ARP table, without being accessed, before it is dropped from the table.

ARP Aging Time Settings		Safeguard
ARP Aging Time (0-65535) :	5 minutes	
		Apply

Figure 4.38 – System > ARP Aging Time Settings

ARP Aging Time (0-65535): Specifies the ARP aging time on the Switch. The range is from 0 to 65535 with a default setting of 5 minutes.

System > PPPoE Circuit ID Insertion Settings

The PPPoE Circuit ID Insertion Settings page specifies the configuration of settings. When enabled, the system will insert the circuit tag to the received PPPoE discover request and the request packet if the tag is absent. It will remove the circuit ID tag from the received PPPoE offer and session confirmation packet.

PPPoE Circuit ID Inserti	on Settings		Safeguard
PPPoE Circuit ID Insertion State		 Enabled Disabled 	Apply
From Port To Port	State Circuit ID Disabled Switch I) ¥	Apply
Port 1	State Disabled	Circuit ID Switch IP	
2	Disabled	Switch IP	
3	Disabled	Switch IP	
4	Disabled	Switch IP	
5	Disabled	Switch IP	
6	Disabled	Switch IP	
7	Disabled	Switch IP	
8	Disabled	Switch IP	
9	Disabled	Switch IP	
10	Disabled	Switch IP	
11	Disabled	Switch IP	
12	Disabled	Switch IP	
13	Disabled	Switch IP	-
4.4	Disabled	0	

PPPoE Circuit ID Insertion State: Enable or disable the PPPoE circuit insertion state, and Click Apply to make the configurations take effect.

From Port/ To Port: Specifies the ports to be configured.

State: Enable or disable the state of specified ports.

Circuit ID: Specifies the Circuit ID is Switch IP, Switch MAC, UDF String, Vendor2 and Vendor3.

Switch IP – The Switch's IP address will be used to encode the circuit ID option. This is the default.

Switch MAC – The MAC address of the Switch will be used to encode the circuit ID option.

UDF String – A user specified string to be used to encode the circuit ID option. Enter a string with the maximum length of 32.

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

System > Web Settings

The WEB State is **Enabled** by default. If user chooses to disable this by selecting Disabled, user will lose the ability to configure the system through the web interface as soon as these settings are applied.

Web Settings		O Safeguard
WEB State Port (1-65535)	Enabled Obisabled 80	
		Apply

Figure 4.40– System > Web Settings

Port (1-65535): Specifies the Port number. The range is between 1 and 65535 with the well-known default is 80.

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

System > Telnet Settings

Telnet configuration is **Enabled** by default. If user does not want to allow the Telnet configuration, they only need to disable the Telnet State.

Telnet Settings		O Safeguard
Telnet State Port (1-65535)	Olisabled Inabled	
		Apply

Figure 4.41 – System > Telnet Settings

Port (1-65535): The TCP port number. TCP ports are numbered between 1 and 65535. The well-known TCP port for the Telnet protocol is 23.

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

System > D-Link Discover Protocol Settings

For the D-Link Discovery Protocol (DDP) supported device, this page is an option for user to disable DDP or configure the DDP packet report timer.

D-Link Discover Protocol State: The default setting is Disabled.

D-Link Discover Protocol Settings		O Safeguard
DDP Global Settings D-Link Discover Protocol State D-Link Discover Protocol Report Timer(Senonds)	○ Enabled	Apply
DDP Port Settings		
01 •	28 • State Disabled •	Apply
6	Enabled	▲
7	Enabled	
8	Enabled	
9	Enabled	
10	Enabled	
11	Enabled	
12	Enabled	
13	Enabled	
14	Enabled	
15	Enabled	
16	Enabled	
17	Enabled	
18	Enabled	
19	Enabled	•

Figure 4.52 – System > D-Link Discover Protocol Settings

D-Link Discover Protocol Report Timer (Seconds): Configure the report timer of D-Link Discover Protocol in seconds. The values are 30, 60, 90, 120 or Never. The default is 30 seconds.

Click Apply to make the configurations take effect.

System > Ping Test

The Ping Test is a small program that sends ICMP Echo packets to the IP address user specified. The destination node then responds to or "echoes" the packets sent the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.

Ping Test		O Safeguard
Start Enter the IP address of the device or station you want to ping, the	en click Start.	
Target IP Address :	0.0.0.0	
Repeat Pinging for:	Infinite times	
	(1-255 times)	
Timeout :	1 (1-99 sec)	

Figure 4.43 – System > Ping Test

Target IP address allows both IPv4 and IPv6 addresses format.

The time of ping can be configured in **Repeat Pinging** filed; **Infinite** and range of **1-255** are available options to use.

Timeout filed specifies the timeout value of every single ping packet. The timeout range from **1-99** seconds. Click **Start** to initiate the Ping Program

System > Trace Route

Perform trace route command direct on system interface. This command used to probe path to the specific destination address.

Trace Route		O Safeguard	
Enter the IP Address of the device or station that you want to trace the route to and click Start.			
IP Address	0.0.0.0		
	O IPv6		
TTL (1-60)	30		
Port (30000-64900)	33434		
Timeout (1-60)	3 sec		
Probe (1-9)	1	Start	

IP address: Specify the destination IP address

TTL: Specify the maximum Time-to-Live

Timeout: Specify the maximum time for response in a hop.

Probe: Specify the time to probe the destination.

System > MAC Notification Settings

MAC Notification page is used to monitor MAC addresses learned and entered into the forwarding database. To globally set MAC notification on the Switch, user should enabled or disabled state, input the Time **Interval** between notification and **History Size** then click the **Apply** button.

MAC Notification Setting	js		O Safeguard
MAC Notification Global Settings			
State	0 E	nabled 🖲 Disabled	
, Interval (1-2147483647 sec)		1 sec	
History Size (1-500)		1	Apply
MAC Notification Port Settings			
From Port	To Port	State	
1 🔻	28 🔻	Disabled •	Apply
MAC Notification Port State Table	3		
Port		Status	
1	Disabled		
2	Disabled		
3	Disabled		
4	Disabled		
5		Disabled	

Figure 4.44 – System > MAC Notification Settings

State: Enabled or Disabled MAC notification globally on the Switch.

Interval (1-2147483647 sec): The time in seconds between notifications.

History Size (1-500): The maximum number of entries listed in the history log used for notification. Up to *500* entries can be specified.

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

To change MAC notification settings for a port or group of ports on the Switch, configure the following parameters., then click the **Apply** button.

From Port / To Port: Select a port or group of ports to enable for MAC notification using the pull-down menus.

State: Enable MAC Notification for the ports selected using the pull-down menu.

System > System Log Configuration > System Log Settings

System Logs record and manage events, as well as report errors and informational messages. Message severity determines a set of event message will be sent. Click **Enable** so user can start to configure the related settings of remote system log server, then press **Apply** for the changes to take effect.

System Log Settings	O Safeguard
System Log O Enabled	Apply
System Log Save Mode Settings	
Save Mode On Demand 🔻	30 minutes (1-65535) Apply

Figure 4.45 – System > System Log Configuration > System Log Settings

Save Mode: Use this drop-down menu to choose the method that will trigger a log entry. User can choose between **On Demand**, **Time Interaval** and **Log Trigger**.

Minutes: Enter a time intervel, in minutes, for which user would like a log entry to be made.

System > System Log Configuration > System Log Server

The user can send Syslog messages to up to four designated servers using the **System Log Server**. It supports maximum 500 system log entries. To set the System Log Server configuration, click **Apply**.

System Log Sei	rver	_		_			0	Safeguard
Add System Log Serve Server ID Server IPv4 Addre Facility Status		1 Local O Disabled	•		Severity O Server IPv6 Address UDP Port (514 or 6000-65535)	Warning •		Apply
System Log Server L	ist							
Server ID	Server IP Address			Severity	Facility	UDP Port S	Status	

Figure 4.46 - System > System Log Configuration > System Log Server

Server ID: Specifies the Server ID. The field range is 1-4.

Severity: Specifies the minimum severity from which warning messages are sent to the server. There are three levels. When a severity level is selected, all severity level choices above the selection are selected automatically. The possible levels are:

Warning - The lowest level of a device warning. The device is functioning, but an operational problem has occurred.

Informational - Provides device information.

All - Displays all levels of system logs.

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

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

Facility: Specifies an application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility is overwritten. There are up to eight facilities can be assigned (Local $0 \sim \text{Local } 7$).

UDP Port: Specifies the UDP port to which the server logs are sent. The possible range is 6000 – 65535, and the default value is 514.

Status: Specifies the status is enable or disable

System > Time Profile

The Time Profile page allows users to configure the time profile settings of the device.

Time Range S	etting					O Safeguard
Time Range						
Range Name						
Date 📃	From Day 2009 🔻 1 🔻	1 •			To Day 2009 🔻 1 🔻 1 🔻	
Hours(HH MM)	Start Time 00 🔻 00 🔻			I	End Time 00 🔻 00 🔻	
Weekdays	🔲 Mon 🔲 Tue 🔲 Wed 🔲 Th	ı 🔲 Fri 🔲 Sat 🔲 Sur	ı		Select All Days	Apply
Note:If the End Time	e is before the Start Time the End Ti	ne will be set to the foll	lowing day.			
Total Entries:0						
Time Range Inform	ation					
Range Name	Weekdays	From Day To	Day	Start Time	End Time	

Figure 4.47 – System > Time Profile Settings

Range Name: Specifies the profile name for the time profile to be configured.

Date: Select Date and specifies the From Day and To Day of the time profile.

Hours (HH MM): Specifies the Start Time and End Time.

Weekdays: Specifies the work day for the time profile. Or tick Select All Days to select all days for the time profile.

Click Apply to create a new time profile or click Delete to delete a time profile from the table.



NOTE: The time must be set after current time, otherwise it will take effect on the next cycle time.

System > Power Saving

The Power Saving mode feature reduces power consumption automatically when the RJ-45 port is link down or the connected devices are turned off. Less power will be consumed also when the short cable is used (less than 20 meters).

By reducing power consumption, less heat is produced, resulting in extended product life and lower operating costs. By default, the Cable Length Detection and Link Status Detection are enabled. Click **Apply** to make the change effective.



Figure 4.48 – System > Power Saving

Advanced Power Saving Settings:

Type: Specifies the Power Saving type to be LED Shut-off, Port Shut-off, Port Standby or System Hibernation.

LED Shut-off - The LED Shut-off gets high priority. If the user select LED Shut-off, the profile function will not take effect. It means the LED cannot be turned on after Time Profile time's up when the state is disabled. On the contrary, if the LED is enabled, the Time Profile function will work.

Port Shut-off - The Port Shut-off state has high priority (the priority rule is the same as LED.) Therefore, if the Port Shut-off sate is already disabled the Time Profile function will not take effect.

System Hibernation - In this mode, switches get most power-saving figures since main chipsets (both MAC and PHY) are disabled for all ports, and energy required to power the CPU is minimal.

State: Specifies the power saving state to be Enabled or Disabled.

Time Profile 1: Specifies the time profile or None.

Time Profile 2: Specifies the time profile or None.

Port: Specifies the ports to be configure of the Power Saving.

Click **Select All** configure all ports, or click **Clear** to uncheck all port. Then Click Apply to make the configurations take effect.

System > IEEE802.3az EEE Settings

The IEEE 802.3 EEE standard defines mechanisms and protocols intended to reduce the energy consumption of network links during periods of low utilization, by transitioning interfaces into a low-power state without interrupting the network connection. The transmitted and received sides should be IEEE802.3az EEE compliance. By default, the switch enabled the 802.3az EEE function. Users can disable this feature by individual port via the IEEE802.3az EEE setting page.

IEEE802.3az	EEE settings		O Safeguard
From Port	To Port	State Disabled	Apply
IEEE802.3az EEE s			
Port	State		
1	Enabled		
2	Enabled		
3	Enabled		
4	Enabled		
5	Enabled		
6	Enabled		
7	Enabled		
8	Enabled		
9	Enabled		
10	Enabled		
11	Enabled		
12	Enabled		

Figure 4.49 – System > IEEE802.3az EEE Settings

From Port / To Port: A consecutive group of ports may be configured starting with the selected port. **State:** Enabled or Disabled the IEEE802.3az EEE for the specified ports. By default, all ports are disabled. Click Apply to make the configurations take effect.

If the connection speed drops down from 1000M to 100M, or the first link up takes longer time, please follow below steps and check again:

- 1. Upgrade driver of Ethernet adapter or LAN controller for the host PC.
- 2. Disable EEE function on the switch port

System > DHCP Relay > DHCP Relay Global Settings

User can enable and configure DHCP Relay Global Settings on the Switch.

DHCP Relay Global Settings		😑 Safeguard
DHCP Relay State DHCP Relay Hops Count Limit (1-16)	Disabled •	
DHCP Relay Time Threshold (0-65535)	0	
DHCP Relay Agent Information Option 82 State	Enabled v	
DHCP Relay Agent Information Option 82 Check	Disabled •	
DHCP Relay Agent Information Option 82 Policy	Replace 🔻	
DHCP Relay Agent Information Option 82 Remote ID	Default • 4A-6F-6E-01-01-01	Apply

Figure 4.23 – System > DHCP Relay > DHCP Relay Global Settings

DHCP Relay State: This field can be toggled between Enabled and Disabled using the pull-down menu. It is used to enable or disable the DHCP Relay service on the Switch. The default is *Disabled*.

DHCP Relay Hops Count Limit (1-16): This field allows an entry between *1* and *16* to define the maximum number of router hops DHCP messages can be forwarded across. The default hop count is 4.

DHCP Relay Time Threshold (0-65535): Allows an entry between *0* and *65535* seconds, and defines the maximum time limit for routing a DHCP packet. If a value of 0 is entered, the Switch will not process the value in the **seconds** field of the DHCP packet. If a non-zero value is entered, the Switch will use that value, along with the hop count to determine whether to forward a given DHCP packet.

DHCP Relay Agent Information Option 82 State: This field can be toggled between Enabled and Disabled using the pull-down menu. It is used to enable or disable the DHCP Agent Information Option 82 on the Switch. The default is *Disabled*.

Enabled – When this field is toggled to Enabled the relay agent will insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients. When the relay agent receives the DHCP request, it adds the option 82 information, and the IP address of the relay agent (if the relay agent is configured), to the packet. Once the option 82 information has been added to the packet it is sent on to the DHCP server. When the DHCP server receives the packet, if the server is capable of option 82, it can implement policies like restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option 82 field in the DHCP reply. The DHCP server unicasts reply to the back to the relay agent if the request was relayed to the server by the relay agent. The switch verifies that it originally inserted the option 82 data. Finally, the relay agent removes the option 82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request.

Disabled - If the field is toggled to Disabled the relay agent will not insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the check and policy settings will have no effect.

DHCP Relay Agent Information Option 82 Check: This field can be toggled between Enabled and Disabled using the pull-down menu. It is used to enable or disable the Switches ability to check the validity of the packet's option 82.

Enabled – When the field is toggled to Enabled, the relay agent will check the validity of the packet's option 82 fields. If the switch receives a packet that contains the option-82 field from a DHCP client, the switch drops the packet because it is invalid. In packets received from DHCP servers, the relay agent will drop invalid messages.

Disabled - When the field is toggled to Disabled, the relay agent will not check the validity of the packet's option 82 fields.

DHCP Relay Agent Information Option 82 Policy: This field can be toggled between Replace, Drop, and Keep by using the pull-down menu. It is used to set the Switches policy for handling packets when the **DHCP Agent Information Option 82 Check** is set to Disabled. The default is *Replace*.

Replace - The option 82 field will be replaced if the option 82 field already exists in the packet received from the DHCP client.

Drop - The packet will be dropped if the option 82 field already exists in the packet received from the DHCP client.

Keep -The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client.

DHCP Relay Agent Information Option 82 Remote ID: This field can be toggled between Default and User Define.

NOTE: If the Switch receives a packet that contains the option-82 field from a DHCP client and the information-checking feature is enabled, the switch drops the packet because it is invalid. However, in some instances, you might configure a client with the option-82 field. In this situation, you should disable the information-check feature so that the switch does not remove the option-82 field from the packet. You can configure the action that the switch takes when it receives a packet with existing option-82 information by configuring the **DHCP Agent Information Option 82 Policy**.

System > DHCP Relay > DHCP Relay Interface Settings

This page allows the user to set up a server, by IP address, for relaying DHCP information the switch. The user may enter a previously configured IP interface on the Switch that will be connected directly to the DHCP server using the following window. Properly configured settings will be displayed in the **DHCP Relay Interface Table** at the bottom of the following window, once the user clicks the **Add** button under the **Apply** heading. The maximum capacity allows user to configure 4 sets of IP addresses of DHCP server.

DHCP Re	lay Interface Setting	js		🥚 Safeguard
Interface	System			
Server IP]		Apply
DHCP Relay	Interface Table			
Interface	Server1	Server2	Server3	Server4

Figure 4.24 – System > DHCP Relay > DHCP Relay Interface Settings

Interface: The IP interface on the Switch that can reach the DHCP Server.

Server IP: Enter the IP address of the DHCP server. Up to four IP addresses can be configured. Click **Apply** to implement changes made.

System > DHCP Local Relay Settings

The DHCP Local Relay Settings page allows the user to configure DHCP Local Relay. DHCP broadcasts are trapped by the switch CPU and replay forwarded with Option 82. Replies from the DHCP servers are trapped by the switch CPU, the Option 82 is removed and the reply is sent to the DHCP Client.

DHCP Local Relay Status	O Ena	abled	Disabled	 	Арр
Config DHCP Local Relay	for VLAN				

Figure 4.25 - System > DHCP Local Relay Settings

DHCP Local Relay Status: Specifies whether DHCP Local Relay is enabled on the device.

Enabled – Enables DHCP Local Relay on the device.

Disabled – Disables DHCP Local Relay on the device. This is the default value.

Config VLAN by: Configure the VLAN by VID or VLAN Name of drop-down menu.

State: Specifies whether DHCP Local Relay is enabled on the VLAN.

Enabled – Enables DHCP Local Relay on the VLAN.

Disabled – Disables DHCP Local Relay on the VLAN.

DHCP Local Relay VID List: Displays the list of VLANs on which DHCP Local Relay has been defined.

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

System > DHCPv6 Relay Settings

The DHCPv6 Relay Settings page allows user to configure the DHCPv6 settings.

DHCPv6 Relay State Disabled DHCPv6 Relay Hops Count Limit (1-32) 4 DHCPv6 Relay Option37 State Enabled DHCPv6 Relay Option37 Check Enabled DHCPv6 Relay Option37 Remote ID Type Default AA-6F-6E-01-01-01 Apply Interface System Server IP DHCPv6 Relay Interface Table	DHCPv6 Rela	y Settings		😑 Safeguard
Apply Apply Interface System Server IP Apply	DHCPv6 Relay Hop DHCPv6 Relay Op DHCPv6 Relay Op	os Count Limit (1-32) ion37 State ion37 Check	4 Enabled Enabled	
Server IP Apply	DHCPv6 Relay Opt	ion37 Remote ID Type		Apply
DHCPv6 Relay Interface Table		System		Apply
Interface Server Address Delete				Delete

Figure 4.26 - System > DHCPv6 Relay Settings

DHCPv6 Relay Status: Specifies whether DHCPv6 Relay is enabled on the device.

Enabled - Enables DHCPv6 Relay on the device.

Disabled – Disables DHCPv6 Relay on the device. This is the default value.

DHCPv6 Relay Hops Count Limit (1-32): The field allows and entry between 1 and 32 to define the maximum number of router hops DHCPv6 messages can be forwarded. The default hop count is 4.

DHCPv6 Relay Option37 State: Specifies the DHCPv6 Relay Option37 State to be enabled or disabled. DHCPv6 Relay Option37 Check: Specifies the DHCPv6 Relay Option37 Check to be enabled or disabled. DHCPv6 Relay Option37 Remote ID Type: Specifies the DHCPv6 Relay Option37 Remote ID type is CID with User Defined, User Defined or Default.

Interface: Enter a name of the interface.

Server IP: Enter the server IP address.

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

System > System Log Configuration > System Log Settings

System Log Configuration feature contains information for configuring various attributes and properties. The System Log Settings page allows user to enable or disable the System Log and specify a method for which to save the switch log to the flash memory of the Switch.

System Log Settings		Safeguard
System Log O Enabled		Apply
Save Mode Settings Save Mode On Demand 30 minutes (1-65535)		
	Apply	Save Log

Figure 4.27 – System > System Log Configuration > System Log Settings

System Log: To enable or disable the system log feature.

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

System Log Save Mode Settings:

Save Mode: Use this drop-down menu to choose the method that will trigger a log entry. Choose among *On Demand*, *Time Interval*, and *Log Trigger*.

On Demand – Users who choose this method will only save log files when they manually tell the Switch to do so, either using the Save Log link in the Save folder.

Time Interval – Users who choose this method can configure a time interval by which the Switch will save the log files, in the box adjacent to this configuration field. The user may set a time between 1 and 65535 minutes.

Log Trigger – Users who choose this method will have log files saved to the Switch every time a log event occurred.

Minutes (1-65535): To specify the time interval in minutes, for which a log entry is to be made.

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

Click the Save Log button to save switch log to the flash memory of the Switch.

System > System Log Configuration > SysLog Host

System Logs record and manage events, as well as report errors and informational messages. Message severity determines a set of event messages that will be sent. Click **Enable** so you can start to configure the related settings of the remote system log server, then press **Apply** for the changes to take effect.

				Safeguard
Server IP Address	 IPv4 0.0.0.0 IPv6 	Severity Facility	All T	
UDP Port (1-65535) Time Stamp	514 Enabled		Looding	
				Apply

Figure 4.28 – System > System Log Configuration > SysLog Host

Server IP Address: Select IPv4 or IPv6 then specify the IP address of the system log server.

UDP Port: Specifies the UDP port to which the server logs are sent. The possible range is 1 - 65535, and the default value is 514.

Time Stamp: Select Enable to time stamp log messages.

Severity: Specifies the minimum severity from which warning messages are sent to the server. There are three levels. When a severity level is selected, all severity level choices above the selection are selected automatically. The possible levels are:

Warning – Transmit the logs only in warning level. This is the highest level events which includes system failure, system reboot, function failure, etc.

Informational – Transmit the logs in information level. This level of events includes port state changes, user login, configuration saved, etc.

All – Transmit all events of logs to syslog server. This is the default value of severity.

Facility: Specifies an application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility is overwritten. There are up to eight facilities can be assigned (Local 0 ~ Local 7).

System > Time Profile

The Time Profile page allows users to configure the time profile settings of the device.

Time Profile S	ettings					😑 Safeguard
Time Profile Profile Name Time(HH MM) Weekdays Date	Sun 🔲 I	00 V 00 V Mon Tue V 2011 V 1	Ned 🗍 Thu 🦳 Fri 🗍 Sat 🔻 1 💌	End Time 00 🔻	00 V V 1 V 1 V	Add
Total Entries:0						
Profile Name	Start Time	End Time	Weekdays	From Day	To Day	Delete

Figure 4.29 – System > Time Profile

Profile Name: Specifies the profile name.

Time(HH MM): Specifies the Start Time and End Time.

Weekdays: Specifies the work day.

Date: Select Date and specifies the From Day and To Day of the time profile.

Click Add to create a new time profile or click Delete to delete a time profile from the table.

System > Power Saving

Power Saving feature helps to reduce power consumption by scheduled plan to shut LED off; shutting port off or shut chips off.

By reducing power consumption, less heat is produced, resulting in extended product life and lower operating costs. By default, the Link Status Detection is disabled. Click **Apply** to make the change effective.

Power Saving Settings Osfeguard														
Global Settings Link Status Detection					• Enal	bled	O Disat	oled					A	pply
Advanced Power Saving Settings														
Type LED Shut-				~			State	•	Dis	abled	ł	~		
Time Profile 1 None		e	~			Time	Profile	2 No	ne		~			
									Select All		Clea	ar	A	pply
Port	01	02	03	04	05	06	07	08	09	10	11	12	13	14
Port	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Summar	v													
Туре			State	Time	e Profile	e 1	Time Pro	file 2	Port					
LED Sh	ut-off		Disabled						None					
Port Sh	ut-off		Disabled						None					
System	Hiberna	tion	Disabled						All Port					

Figure 4.30 – System > Power Saving

Advanced Power Saving Settings:

Type: Specifies the Power Saving type to be LED Shut-off, Port Shut-off or System Hibernation.

LED Shut-off – Specify the Power saving method to turning port LED off. The action would be executed in time range of specified time profile. The connection would remain but just LED lights off. **Port Shut-off** - Specify the Power saving method to turning port off. The action would be executed in

time range of specified time profile. Be noted, the port connection would be off during time profile.

System Hibernation - In this mode, switches get most power-saving figures since main chipsets (both MAC and PHY) are disabled for all ports, and energy required to power the CPU is minimal. System is still running but all ports are shut off.

State: Specifies the power saving state to be Enabled or Disabled.

Time Profile 1: Specifies the time profile or None.

Time Profile 2: Specifies the time profile or None.

Port: Specifies the ports to be configure of the Power Saving.

Click **Select All** configure all ports, or click **Clear** to uncheck all port. Then click **Apply** to implement changes made.

System > IEEE802.3az EEE Settings

The IEEE 802.3 EEE standard defines mechanisms and protocols intended to reduce the energy consumption of network links during periods of low utilization, by transitioning interfaces into a low-power state without interrupting the network connection. The transmitted and received sides should be

IEEE802.3az EEE compliance. By default, the 802.3az EEE function is disabled of the switch. Users can enable this feature by individual port via the IEEE802.3az EEE setting page.

EEE802.3az	EEE settings		🥚 Safeguard
From Port	To Port	State Disabled ▼	Apply
IEEE802.3az EEE	settings		
Port	State		×
1	Disabled		
2	Disabled		
3	Disabled		
4	Disabled		
5	Disabled		
6	Disabled		
7	Disabled		
8	Disabled		
9	Disabled		
10	Disabled		
11	Disabled		
12	Disabled		
13	Disabled		

Figure 4.31 – System > IEEE802.3az EEE Settings

From Port / To Port: A consecutive group of ports may be configured starting with the selected port. **State:** Enabled or Disabled the IEEE802.3az EEE for the specified ports. By default, all ports are disabled. Click **Apply** to implement changes made.

If the connection speed drops down from 1000M to 100M, or the first link up takes longer time, please follow below steps and check again:

- 3. Upgrade drivers of your Ethernet adapter or LAN controller for the host PC.
- 4. Disable EEE function on the switch port.

Configuration > 802.1Q VLAN

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

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

The IEEE 802.1Q VLAN Configuration page provides powerful VID management functions. The original settings have the VID as 1, no default name, and all ports as "Untagged"

Rename: Click to rename the VLAN group.

Delete VID: Click to delete the VLAN group.

Add New VID: Click to create a new VID group, assigning ports from 01 to 28 as Untag, Tag, or Not Member. A port can be untagged in only one VID. To save the VID group, click Apply.

You may change the name accordingly to the desired groups, such as R&D, Marketing, email, etc.

802.10	Q VLAN Settings					0	Safeguard
Asymme	etric VLAN [Example]	O Enabled	Disabled				Apply
	atic VLAN entries: 1 num 256 entries.						Add
VID	VLAN Name	Untagged		Tagged			Delete
1	default	01-28					Delete
				Page 01	▶ В	ack	Next

Figure 4.35 – Configuration > 802.1Q VLAN

Click Add to create a new VID group, entering the VID and VLAN name, assigning ports role as Untag, Tag or Not Member. To save the VID group, click Apply.

/ID Setting	S												s	afeg	uar
VID															
VLAN Name				=											
Maximum 20	characters.									[B	ack		App	oly
Port	Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14
Untagged	All	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tagged	All	•		0		0			0	0		0		•	0
Not member	All	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲
Port	Select All	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Untagged	All	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tagged	All	•		0		•		•	•	0		0			•
Not member	All	۲				\bullet	•	•		۲		۲			

Figure 4.36 – Configuration > 802.1Q VLAN > Add VID

After click **Apply**, the 802.1Q VLAN Configuration Table will displayed with updates.

802.1	Q VLAN Settings					Safeguard
Asymm	etric VLAN [Example]	O Enabled	Oisabled			Apply
	tatic VLAN entries: 2 mum 256 entries.					Add
VID	VLAN Name	Untagged	_	Tagged		Delete
1 2	default VLAN2	01-28	_	01-28		Delete Delete
				Page 01 🗸	Back	Next

Figure 4.37 – Configuration > 802.1Q VLAN > Add VLAN

Click the VID number, the configuration of VLAN group which selected by user will displayed. Change the port assignment then click **Apply** to implement changes made.

/ID Setting	IS											- (s	afeg	uar
VID	1														
VLAN Name	default									В	ack		Арр	ly	
Port	Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14
Untagged	All	۲	۲	۲		\bullet	۲	\bullet		۲	۲		۲	۲	۲
Tagged	All	•		0	0		0		0	0	0		0	0	
Not Member	All	0	0	0	0	0	0	0	0	0	\circ	0	0	0	0
Port	Select All	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Untagged	All	۲	۲	۲						۲	۲		۲	۲	
Tagged	All			0	0		0		0	0	0		0	0	
Not Member	All	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 4.38 - Configuration > 802.1Q VLAN > VID Assignments

Configuration > 802.1Q Management VLAN

The particular VID to access management interface.

IEEE 802.1Q Man	agement VLAN Configuration	Safeguard
Management VLAN	Enabled Disabled	
VID VLAN Name	1 V default	Apply

Management VLAN: Option for **Enable/Disable** management VLAN. Please be caution, DISABLING management VLAN will cause lost of management.

VID: Specify the VID for management access.

Configuration > 802.1Q VLAN PVID

The 802.1Q VLAN PVID setting allows user to configure the PVID for each ports. Click **Apply** to implement changes made.

	(VLA	NPV	ID Se	ttings								0	Safe	guar
Port	01	02	03	04	05	06	07	08	09	10	11	12	13	14
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Port	15	16	17	18	19	20	21	22	23	24	25	26	27	28
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Figure 4.39 – Configuration > 802.1Q VLAN PVID

Configuration > Voice VLAN > Voice VLAN Global Settings

Voice VLAN is a feature that allows you to automatically place the voice traffic from IP phone to an assigned VLAN to enhance the VoIP service. With a higher priority and individual VLAN, the quality and the security of VoIP traffic are guaranteed. If a VoIP packet comes with a VLAN tag, the Voice VLAN function won't replace the original VLAN tag.

Voice VLAN Glob	al Settings					😑 Safeguard
Voice VLAN VLAN ID 1	C Enabled	Disable	d Aging Time (1~120)		1 hour	
Priority 5	Ψ					Apply
Voice VLAN OUI Settings	D	escription 3COM	¥ .	Telephony OUI 00-E0-BB-00-00	0-00	
User defined OUI					(XX-XX-XX-XX-XX)	
🤌 Maximum number of	user defined OUI i	s 10 entries.				Add
r						
ID	Descr	iption	Telephony	OUI	OUI Mask	Delete
	5	iauro 4.40 - 1			AN Global Settings	

Figure 4.40 – VLAN > Voice VLAN > Voice VLAN Global Settings

Voice VLAN: Select to enable or disable Voice VLAN. The default is *Disabled*. After you enabled Voice VLAN, you can configure the **Voice VLAN Global Settings**.

VLAN ID: The ID of VLAN that user wants to assign voice traffic to. 802.1Q VLAN group must be created before assigned it into Voice VLAN. The member port that configured in 802.1Q VLAN setting page will be the static member port of voice VLAN. To dynamically add ports into the voice VLAN, please enable the **Auto Detection** function

Priority: The 802.1p priority levels of the traffic in the Voice VLAN.

Aging Time (1-120): Enter a period of time (in hours) to remove a port from the 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 start. The port will be removed from the voice VLAN after the expiration of the voice VLAN aging timer. Selectable range is from 1 to 120 hours, and default is 1.

Click **Apply** to implement changes made.

Voice VLAN OUI Settings: This allows the user to configure the user-defined voice traffic's OUI. An Organizationally Unique Identifier (OUI) is the first three bytes of the MAC address. This identifier uniquely identifies a vendor, manufacturer, or other organization.

There are some pre-defined OUIs and when the user configures personal OUI, these pre-defined OUIs must be avoided. Below are the pre-defined voice traffic's OUI:

OUI	Vendor	Mnemonic Name
00:E0:BB	3Com	3com
00:03:6B	Cisco	cisco
00:E0:75	Veritel	veritel
00:D0:1E	Pingtel	pingtel
00:01:E3	Siemens	siemens
00:60:B9	NEC/ Philips	nec&philips
00:0F:E2	Huawei-3COM	huawei&3com
00:09:6E	Avaya	avaya

Default OUI: Pre-defined OUI values, including brand names of 3COM, Cisco, Veritel, Pingtel, Siemens, NEC/Philips, Huawei3COM, and Avaya.

User defined OUI: It is able to manually create a Telephony OUI with a description. The maximum number of user defined OUIs is 10.

Select the OUI and press Add to the lower table to complete the Auto Voice VLAN setting.



Note: Voice VLAN has higher priority than any other features (including QoS). Therefore the voice traffic will be operated according to the Voice VLAN setting and not impacted by the QoS feature.



Note: It is recommended setting the highest priority for Voice VLAN to guarantee the quality of VoIP traffic.

Configuration > Voice VLAN > Voice VLAN Port Settings

The Voice VLAN Port Settings page allows users to automatically place the voice traffic from IP phone to an assigned VLAN to enhance the VoIP service. With a higher priority and individual VLAN, the quality and the security of VoIP traffic are guaranteed.

rom Port	To F	Port	Auto De	etection	Tagged / Ur	ntagged			
01	~	28 🗸	Disab	led	✓ Untagged	~	Refresh	Apply	,
Port		Auto Detect	tion	Tagge	d / Untagged	Current	State	Status	
01		Disabled		U	ntagged	Non	9	Static	1
02		Disabled		Ur	ntagged	Non	9	Static	
03		Disabled		U	ntagged	Non	9	Static	_
04		Disabled		Ur	ntagged	Non	9	Static	_
05		Disabled		UI	ntagged	Non	9	Static	
06		Disabled			ntagged	None	e	Static	
07		Disabled			ntagged	None	e	Static	
08		Disabled			ntagged	Non	9	Static	
09		Disabled		UI	ntagged	Non	e	Static	
10		Disabled			ntagged	None	e	Static	_
11		Disabled			ntagged	None	e	Static	_
12		Disabled			ntagged	Non	e	Static	
13		Disabled			ntagged	Non	9	Static	
14		Disabled			ntagged	None	e	Static	_
15		Disabled			ntagged	None	e	Static	_
16		Disabled			ntagged	Non	e i	Static	
17		Disabled			ntanned	Non	<u> </u>	Static	_

Figure 4.41 – VLAN > Voice VLAN > Voice VLAN Port Settings

From Port / To Port: A consecutive ports may be selected by From Port and To Port dropdown lists.

Auto Detection: Switch will add ports to the voice VLAN automatically if it detects the device OUI matches the Telephony OUI configured in Voice VLAN OUI Setting page. Use the drop-down menu to enable or disable the OUI auto detection function. The default is *Disabled*

Tagged / Untagged: Tagged or untagged the ports.

Click **Apply** to implement changes made and **Refresh** to refresh the voice vlan table.

Note: Voice VLAN has higher priority than any other features even QoS. Therefore the voice traffic will be operated according to Voice VLAN setting and not impacted by QoS feature.



Note: It is recommended setting the highest priority for Voice VLAN to guarantee the quality of VoIP traffic.

Configuration > Voice VLAN > Voice Device List

The Voice Device List page displays the information of Voice VLAN.

Voice Device	e List				😑 Safeguard
Port All	▼ Search]			
ID	Port	MAC Address	Priority	Туре	Delete

Figure 4.42 – VLAN > Voice VLAN > Voice Device List

Select a port or all ports and click **Search** to display the Voice Device information in the table.

Configuration > Voice VLAN > LLDE-MED Voice Device List

The Voice Device List page displays the information of voice device learned from LLDP-MED protocol. The device information is retrieved from Network Policy contained in LLDP-MED packets.

LLDP-N	IED Voice Dev	ice List			Safeguard
Port A	JI T	Search			
ID 01	Port 3	MAC Address 00-A8-59-C4-02-8C	Priority 5	Type Tagged	
•					Þ

Figure 4.69 - Configuration > Voice VLAN > LLDP-MED Voice Device List

Configuration > Auto Surveillance VLAN > Auto Surveillance Properties

The Auto Surveillance Properties page allows user to configure and display the ports surveillance VLAN settings and information.

Auto Surveillance Properties		0 Safeguard
Global Settings Surveillance VLAN Surveillance VLAN ID (2-4094) Surveillance VLAN CoS Aging Time (1-65535) ONVIF Discover Port (554,1025-65535)	 Enabled Disabled 5 720 min 554 Enabled Disabled 	Angle
Log State Note: Surveillance VLAN ID and Voice VLAN		Apply
ONVIF Global Status Surveillance Device Detected (OUI) IP-Camera Detected (ONVIF) NVR Detected (ONVIF)	0 0 0	
From Port To Port 01 • 28 •	State Disabled V	Apply
Port 1 2	State Disabled Disabled	×

Figure 4.43 – VLAN > Auto Surveillance VLAN > Auto Surveillance Properties

Global Settings: To configure the related auto surveillance VLAN global settings.

Auto Surveillance VLAN: To enable or disable the auto surveillance VLAN state.

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

Surveillance VLAN CoS: Specifies the priority of the surveillance VLAN. The range is from 0 to 7.

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

Discover Port (554, 1024-65535): Specifies the TCP/UDP port number for surveillance VLAN. The range is either 554, or between 1024 and 65535. This is used to configure the TCP/UDP port number for RTSP stream snooping. ONVIF-capable IPC and ONVIF-capable NVR utilize WS-Discovery to find other devices. Once IPCs are discovered, the Switch can further discover NVRs by snooping RTSP, HTTP, and HTTPS packets between NVRs and IPCs. These packets cannot be snooped if the TCP/UDP port is not equal to the RTSP port number.

Log State: To enable or disable the log state of surveillance VLAN.

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

Configuration > Auto Surveillance VLAN > MAC Settings and Surveillance Device

Similar as Voice VLAN, Auto Surveillance VLAN is a feature that allows you to automatically place the video traffic from D-Link IP cameras to an assigned VLAN to enhance the IP surveillance service. With a higher priority and individual VLAN, the quality and the security of surveillance traffic are guaranteed. The Auto Surveillance VLAN function will check the source MAC address / VLAN ID on the incoming packets. If it matches specified MAC address / VLAN ID, the packets will pass through switch with desired priority.

AC S	Settings and Surveilland	ce Device			😑 Safegua	
ser-de	fined MAC Settings					
		ce VLAN by user-defined configuration	on as below			
mpon	nent Type Des	cription	(XX-XX-	XX-XX-XX-XX)		
	Management Server		MAC V		Add	
ueo					Add	
махі	mum number of user-defined MAC	S is 5 entries.				
ID	Component Type	Description	MAC Address	Mask	Delete	
01	D-Link Surveillance Device	D-Link IP Surveillance Device	28-10-7B-00-00-00	FF-FF-FF-E0-00-00	Default	
02	D-Link Surveillance Device	D-Link IP Surveillance Device	28-10-7B-20-00-00	FF-FF-FF-F0-00-00	Default	
03	D-Link Surveillance Device	D-Link IP Surveillance Device	B0-C5-54-00-00-00	FF-FF-FF-80-00-00	Default	
04	D-Link Surveillance Device	D-Link IP Surveillance Device	F0-7D-68-00-00-00	FF-FF-FF-F0-00-00	Default	
ito Su	Port	Component Type		Description	Refresh	
	1	None		None		
	2	None		None		
	3	None		None		
	4	None		None		
	5	None		None		
6 None				None		
	7 8	None		None		



User-defined MAC Settings:

Component Type: Auto Surveillance VLAN will automatically detect D-Link Surveillance Devices by default. There are another five surveillance components that could be configured to be auto-detected by the Auto Surveillance VLAN. These five components are *Video Management Server (VMS), VMS Client/Remote viewer, Video Encoder, Network Storage* and Other *IP Surveillance Devices*.

Description: Here to input the description for the component type.

MAC Address: User can manually create an MAC or OUI address for the surveillance component. The maximum number of user defined MAC address is 5.

Mask: Specifies the mask address for the MAC or OUI.

Click **Add** to create a new surveillance component and **Refresh** to refresh the Auto Surveillance VLAN summary table.

Configuration > Auto Surveillance VLAN > ONVIF IPC Information

The ONVIF (Open Network Video Interface Forum) IPC Information page displays the information on each IP camera connected to the switch. Information includes the port number, IP address, MAC address, throughput and other information such as port description and model name.

ONVIF IPC Informat	ion						😑 Safeguard
ONVIF IPC Information							
Total Entries Discovered: 0							
Ports IP Address	MAC Address	Model	Manufacturer	Traffic	Description	Throughput	
Note:System probes IP-Cam	era every 30s.						

Figure 4.45 – VLAN > Auto Surveillance VLAN > ONVIF IPC Information

Configuration > Auto Surveillance VLAN > ONVIF NVR Information

The ONVIF (Open Network Video Interface Forum) NVR Information page displays the information on each NVR connected to the switch. Including the port number, IP address, MAC address, IP-Camera number, throughput and description relating to the cameras connected to the NVR, such as the group name, total number of cameras and the port and IP address of each camera.



Figure 4.46 – VLAN > Auto Surveillance VLAN > ONVIF NVR Information

Configuration > QinQ > QinQ Settings

The QinQ Settings page allows user to enable or disable the Q-in-Q function. Q-in-Q is designed for service providers to carry traffic from multiple users across a network.

Q-in-Q is used to maintain customer specific VLAN and Layer 2 protocol configurations even when the same VLAN ID is being used by different customers. This is achieved by inserting SPVLAN tags into the customer's frames when they enter the service provider's network, and then removing the tags when the frames leave the network.

Customers of a service provider may have different or specific requirements regarding their internal VLAN IDs and the number of VLANs that can be supported. Therefore customers in the same service provider network may have VLAN ranges that overlap, which might cause traffic to become mixed up. So assigning a unique range of VLAN IDs to each customer might cause restrictions on some of their configurations requiring intense processing of VLAN mapping tables which may exceed the VLAN mapping limit. Q-in-Q uses a single service provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer's VLAN IDs are segregated within the service provider's network even when they use the same customer specific VLAN ID. Q-in-Q expands the VLAN space available while preserving the customer's original tagged packets and adding SPVLAN tags to each new frame. Select *Enabled* or *Disabled* then click **Apply** to enable or disable the Q-in-Q Global Settings.

QinQ Settings				O Safeguar
QinQ Global Settings:	O Enabled	sabled		Apply
inner_tpid:	0x <mark>8100</mark>			Apply
From Port To Port	Role Outer TPID (hex : 0 NNI 0x [8100	x1-0xfff) Miss Drop Disabled	Add Inner Tag	Disabled
Port	Role	Outer TPID	Drop Status	Add Inner Tag
1	NNI	0x88a8	Disabled	Disabled
2	NNI	0x88a8	Disabled	Disabled
3	NNI	0x88a8	Disabled	Disabled
4	NNI	0x88a8	Disabled	Disabled
5	NNI	0x88a8	Disabled	Disabled
6	NNI	0x88a8	Disabled	Disabled
7	NNI	0x88a8	Disabled	Disabled
8	NNI	0x88a8	Disabled	Disabled
9	NNI	0x88a8	Disabled	Disabled
10	NNI	0x88a8	Disabled	Disabled
11	NNI	0x88a8	Disabled	Disabled
12	NNI	0x88a8	Disabled	Disabled
13	NNI	0x88a8	Disabled	Disabled
14	NNI	0x88a8	Disabled	Disabled
15	NNI	0x88a8	Disabled	Disabled
16	NNI	0x88a8	Disabled	Disabled

Figure 4.70 - Configuration > QinQ > QinQ Settings

From Port / To Port: A consecutive group of ports that are part of the VLAN configuration starting with the selected port.

Role: The user can choose between *UNI* or *NNI* role.

UNI – To select a user-network interface which specifies that communication between the specified user and a specified network will occur.

NNI – To select a network-to-network interface specifies that communication between two specified networks will occur.

Outer TPID (hex: 0x1-0xffff): The Outer TPID is used for learning and switching packets. The Outer TPID constructs and inserts the outer tag into the packet based on the VLAN ID and Inner Priority.

Miss Drop: Specifies to enable or disable the Miss Drop. If Miss Drop is enabled, the packet does not match any assignment rule in the VLAN translation and Q-in-Q profile will be dropped. If disabled, the packet will be forwarded and will be assigned to the PVID of the received port.

Add Inner Tag: Unselect the **Disable** check box and enter an entry that an Inner Tag will be added to the entry.

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

Configuration > QinQ > VLAN Translation Settings

The VLAN Translation translates the VLAN ID carried in the data packets it receives from private networks into those used in the Service Providers network.

VLAN Transla	ation Settings		_			O Safeguard
From Port 01 •	To Port 28 V	CVID (e.g.: 1,5-7)	Action Add ▼	SVID (1-4094)	Priority None ▼	Apply
Total Entries:0						Delete All
Port	CVID	SVID	Action	Priority		
			< < Table is em	pty > >		

Figure 4.71 - Configuration > QinQ > VLAN Translation Settings

From Port / To Port: A consecutive group of ports that are part of the VLAN configuration starting with the selected port.

Action: Specify for SPVID packets to be added or replaced.

CVID List (1-4094): The customer VLAN ID List to which the tagged packets will be added.

SVID (1-4094): This configures the VLAN to join the Service Providers VLAN as a tagged member.

Priority: Specifies the CVID entry priority.

Click Apply to make the configurations take effect. Click **Delete All** to remove all the CVID entries.

Q-in-Q and VLAN Translation Rules:

For Ingress untagged packets at UNI ports:

1. The Switch does not reference the VLAN translation table.

2. Check the Switch VLAN tables. The Sequence is MAC-based VLAN -> subnet-based VLAN -> protocol-based VLAN -> port-based VLAN. If matched, the matched VLAN will become this packet's SPVLAN.

For Ingress tagged packets at UNI ports:

1. The Switch looks up the VLAN translation table. If matched, the VLAN tag will be translated (replace CEVLAN with SPVLAN, or add SPVLAN).

2. Or, check the Switch VLAN tables. The sequence is the same as above. The matched VLAN becomes this packet's SPVLAN.

Configuration > Link Aggregation > Port Trunkings

The Port Trunkings function enables the combining of two or more ports together to increase bandwidth. Up to eight Trunk groups may be created, and each group consists up to eight ports. Select **Enabled** and click **Apply** to active the Link Aggregation State.

	ing	_	_			_										(9 9	afeg	uard
Link Aggregatio	on State:		O	Enabled	۱	Disabled												Appl	у
Link Aggregatio	gregation Algorithm: MAC Source								Appl	y									
Edit Trunking	Information																		
ID 01	~	Туре	Disable	~		Mas	ter Port		0	1	~							Appl	у
Port 1	2 3 4	56	7 8 9	10	11	12 1	3 14	15	16	17	18	19	20	21	22	23	24	25	26
27	28 29 30	31 32	33 34 35	36	37	38 3	9 40	41	42	43	44	45	46	47	48	49	50	51	52
Note:maximum	n 8 ports in static or	oup and 8 pc	orts in LACP aroud).															
Note:maximum Trunking list	n 8 ports in static gr	oup and 8 pc	orts in LACP group).															
Trunking list		oup and 8 pc						_	Maste	er Port	_		Activ	/e Port	s		_		
Trunking list	Туре	oup and 8 pc	orts in LACP group Member Por						Maste	er Port			Activ	ve Port	s				_
Trunking list		oup and 8 pc							Maste	er Port			Activ	ve Port	s				
Trunking list ID 01	Type Disable	oup and 8 po							Maste	er Port			Activ	ve Port	s				
Trunking list ID 01 02	Type Disable Disable	oup and 8 po							Maste	er Port			Activ	ve Port	s				
Trunking list D 01 02 03 04 05	Type Disable Disable Disable	oup and 8 pc							Maste	er Port			Activ	ve Port	S				
Trunking list D 01 02 03 04 05 06	Type Disable Disable Disable Disable Disable Disable	oup and 8 pc							Maste	er Port			Activ	ve Port	S				
Trunking list D 01 02 03 04 05	Type Disable Disable Disable Disable Disable	oup and 8 po							Maste	er Port			Activ	ve Port	S				

Figure 4.76 – Configuration > Link Aggregation > Port Trunkings

Link Aggregation Algorithm: Specify the algorithm to be *MAC Source, MAC Destination, MAC Source Destination, IP Source, IP Destination or IP Source Destination,* and then Click Apply to make the configurations take effect.

Edit Trunking Information:

Specify the **ID**, **Type** and **Master Port** then select the ports to be grouped together, and then click **Apply** to activate the selected Trunking groups. Two types of link aggregation can be selected:

Static - Static link aggregation.

LACP - LACP (Link Aggregation Control Protocol) is enabled on the device. LACP allows for the automatic detection of links in a Port Trunking Group.

Disable - Remove all members in this trunk group.

NOTE: Each combined trunk port must be connected to devices within the same VLAN group.

Configuration > Link Aggregation > LACP Port Settings

The LACP Port Settings is used to create port trunking groups on the Switch. The user may set which ports will be active and passive in processing and sending LACP control frames.

m Port	To Port	Port Pric	rity(0~65535)	Activity	Timeout	
01	▼ 28	•	128	Passive 🔻	short (3 sec) 🔻	Apply
Port	Port Priority	Activity			Timeout	
01	128	Active			Long (90 sec)	
02	128	Active			Long (90 sec)	
03	128	Active			Long (90 sec)	
04	128	Active			Long (90 sec)	
05	128	Active			Long (90 sec)	
06	128	Active			Long (90 sec)	
07	128	Active			Long (90 sec)	
08	128	Active			Long (90 sec)	
09	128	Active			Long (90 sec)	
10	128	Active			Long (90 sec)	
11	128	Active			Long (90 sec)	
12	128	Active			Long (90 sec)	
13	128	Active			Long (90 sec)	
14	128	Active			Long (90 sec)	

Figure 4.77 – Configuration > Link Aggregation > LACP Port Settings

From Port: The beginning of a consecutive group of ports may be configured starting with the selected port.
To Port: The ending of a consecutive group of ports may be configured starting with the selected port.
Port Priority (0-65535): Displays the LACP priority value for the port. Default is *128*.
Activity: There are two different roles of LACP ports:

A Colocus

Active - Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP.

Passive - LACP ports that are designated as passive cannot initially send LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, one end of the connection must have "active" LACP ports.

Timeout: Specify the administrative LACP timeout. The possible field values are:

Short (3 Sec) - Defines the LACP timeout as 3 seconds.

Long (90 Sec) - Defines the LACP timeout as 90 seconds. This is the default value.

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

Configuration > IGMP Snooping > IGMP Snooping

With Internet Group Management Protocol (IGMP) snooping, the DGS-1210/ME Metro Ethernet 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 DGS-1210/ME Metro Ethernet Switch will forward multicast traffic only to connections that have group members attached.

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

IGMP Snooping Configuration

enni eneeping eeningaraa	UII			- acrege				
IGMP Snooping	O Enabled	Disabled	Report to all ports					
IGMP Global Settings								
Host Timeout (130-153025 sec)		260	Router Timeout (60-600 se	ec) 125				
Max Learned Entry Value (1 - 1024)		1024						
IGMP Snooping Rate Limit	O Enabled	Disabled						
Rate Limit Value (1-200)		200						
Note: The Host Timeout was computed automatically in Querier Enabled by (Robustness Variable * Query Interval + Max Apply Apply								
The VLAN Settings of IGMP snooping								
VLAN ID VLAN Name	e 10	MP Parameters Settir	ngs Router Ports Settings	Multicast Entry Table				
1 default		IGSEdit	Edit	View				

Figure 4.79 – Configuration > IGMP Snooping > IGMP Snooping

By default, IGMP is disabled. If enabled, the IGMP Global Settings will need to be entered:

Parameters	Description
IGMP Snooping	Used to control IGMP snooping global state; the radios buttons enable/disable to change the state.
Host Timeout (130-153025 sec)	This is the interval after which a learned host port entry will be purged. For each host port learned, a 'Port Purge Timer' runs for 'Host Port Purge Interval'. This timer will be restarted whenever a report message from host is received over that port. If no report messages are received for 'Host Port Purge Interval' time, the learned host entry will be purged from the multicast group. The default value is 260 seconds.
Router Timeout (60-600 sec)	This is the interval after which a learned router port entry will be purged. For each router port learned, a 'Router Port Purge Timer' runs for 'Router Port Purge Interval'. This timer will be restarted whenever a Query control message is received over that port. If there were no Query control messages received for 'Router Port Purge Interval' time, the learned router port entry will be purged. Default is 260 seconds.

Max Learned Entry Value (1-1024)	The maximum IGMP group(s) allowed to be learned for entire system. The range from 1 to 1024 groups. The default value is 1024 groups.
IGMP Snooping Rate Limit	Used to control if system has the maximum process limit especially for IGMP packet (IGMP report, IGMP leave and IGMP query). Lower rate helps to lower the CPU loading. Rate Limit Value is a range from 1-200 in PPS.

Clicking **Apply** button for apply the changes.

Click IGSEdit button to enter the IGMP Parameters Settings page.

IGMP Snooping Parameters Settings			O Safeguard
VID	1	VLAN NAME	default
	, 		Geladit
Robustness Variable (2-255)	2	Last Member Query Interval (1-25 sec)	1
Query Interval (60-600 sec)	125	Max Response Time (10-25 sec)	10
Proxy Reporting Source IP	0.0.0.0 (e.g.: 10.90.90.90)	Proxy Reporting State	Disabled V
Querier State	Disabled V	Fast Leave	Disabled V
State	Disabled V	Data Driven Learning State	Disabled 🗸
Querier Version	v2 🗸	Report Suppression	Enabled V
VlanDataDrivenLearningAge	Disabled 🗸		
Querier Role	Non-Querier		
Querier IP	0.0.0.0		
Querier Expiry Time	0		
		Previous Page	Apply

Figure 4.80 – Configuration > IGMP Snooping > IGMP Snooping Parameters Settings

Parameters	Description
State	Used to control IGMP snooping state for this particular VLAN group. The state Enabled/Disabled can be selected in drop-down list.
Robustness Variable (2-255 sec)	The Robustness Variable allows adjustment for the expected packet loss on network. The larger robustness variable help to prevent packet lost occurred in network; the key types of packet for IGMP: report, leave and query. The Robustness Variable cannot be set to zero, and it SHOULD NOT be. Default is 2 seconds
Query Interval (60-600 sec)	The Query Interval is the interval between General Queries sent. By adjusting the Query Interval, the number of IGMP messages can be increased or decreased; larger values will cause IGMP Queries to be sent less often. Default value is 125 seconds.
Last Member Query Interval (1-25 sec)	The Last Member Query Interval is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages. This value may be adjusted to modify the "leave latency" of the network. A reduced value results in reduced time to detect the loss of the last member of a group. Default is 1 second.
Max Response Time (10-25 sec)	The Max Response Time specifies the maximum allowed time before sending a responding report message. Adjusting this setting effects the "leave latency", or the time between the moment the last host leaves a group and when the multicast server is notified that there are no more members. It also allows adjustments for controlling the frequency of IGMP traffic on a subnet. Default is 10 seconds.
Proxy Reporting Source IP	Enter the proxy reporting source IP address.
Proxy Reporting	Use the drop-down menu to enable and disable the proxy report state.

Querier State	Device starts sending general query packets by Query Interval when state configured to Enabled . Device stop sending general query packet when state configured to Disabled .
Querier Version	Specify the general query packet version; v1 , v2 and v3 are available to use.
Fast Leave	If enabled, the membership is immediately removed when the system receive the IGMP leave message.
Data Driven Learning State	Data Driven learning is a mechanism that helps to register the IGMP group via multicast traffic packet. The feature helps to solve some special network application that end host does not support IGMP function but only sending multicast traffic; for example, IP camera.
VLANDateDrivenLear ningAge	Specifies that the aging out of the entry will be enabled or disabled.
Report Suppression	By Enabled Report Suppression , the device forward 1 IGMP report that registered the same IGMP group in 10 seconds period.
Querier Role	Display the current information for Querier Role .
Querier IP	Display the current information of Querier IP address .
Querier Expiry Time	Display the current information for Querier Expiry Time .

Clicking **Apply** button for apply the changes.

Clicking **Previous Page** returned to IGMP Snooping Configuration page.

Click **Edit** button to enter the Router Port Settings page, and the ports to be assigned as router ports for IGMP snooping for the VLAN.

A router port configured manually is a **Static Router Port**, a **Forbidden Router Port** and a **Dynamic Router Port** is dynamically configured by the Switch when a query control message is received. Press **Apply** for changes to take effect.

4
4
4
28
4
28
4
28
Apply
1

Figure 4.81 – Configuration > IGMP Snooping > IGMP Snooping-Router Port Settings

To view the Multicast Entry Table for a given VLAN, press the View button.

R	/lulticast Entry Tabl	e			0 Safeguard
	Group ID VLAN ID	VLAN Name	Multicast Group	Multicast MAC address	Port Members

Figure 4.82– Configuration > IGMP Snooping > IGMP Snooping-Multicast Entry Table

Configuration > IGMP Snooping > IGMP Access Control Settings

The IGMP Access Control Settings page is used to enable or disable the IGMP access control of selected ports.

GMP Access Control S	ettings		O Safeguard
rom Port	To Port 28 ▼	Status Disabled ▼	Apply
MP Access Control Table Port		Status	
Pon			
1		Disabled	
2		Disabled	
3		Disabled	
4		Disabled	
5		Disabled	
6		Disabled	
7		Disabled	
8		Disabled	
9		Disabled	
10		Disabled	

Figure 4.83 – Configuration > IGMP Snooping > IGMP Access Control Settings

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

Status: Enable or disable the IGMP Access Control of specified ports.

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

Configuration > IGMP Snooping > Host Table

The Host Table page displays the information of Host Table. Including VLAN ID, Group, Port Number and Host IP.

Host Table				O Safeguard
VLAN ID	Group	Port Number	Host IP	

Figure 4.86 - Configuration > IGMP Snooping > Host Table

Configuration > IGMP Snooping > IGMP Snooping Static Group Settings

The IGMP Snooping Static Group Settings page allows the Switch to read the Multicast Group IP address and the corresponding MAC address from IGMP packets that pass through the Switch.

GMP Sn	ooping Static (Group Settings		-	Safegua
VLAN Na	ame	(Max: 32 characters)			
VID List		(e.g.: 1-3, 5)			
IPv4 Add	ress	(e.g.: 224.1.1.1)	Find	Create	Delete
					View All
					VIEW AII
otal Entries: D	: 1 VLAN Name	IP Address	Static Member Port		View All

Figure 4.90- Configuration > IGMP Snooping > IGMP Snooping Static Group Settings

VLAN Name: Specifies the VLAN name of the multicast group.

VID List: Specifies the VID list or of the multicast group.

IPv4 Address: Specifies the IPv4 address.

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

Configuration > MLD Snooping > MLD Snooping Settings

The MLD Snooping Settings page allows user to configure the max multicast group for IGMP Snooping.

MLD Paran	neters Configura	ation	_	_	O Safegua	nd
MLD Snooping		O Enabled	Disabled	🖉 Report to	all ports	
MLD Global Se	ttings					
Host Timeout (1	130-153025 sec)		260 Router T	imeout (60-600 sec	:)	125
Max Learned E	ntry Value (1 - 1024)		1024			
	: Timeout was compute ► Max Response Time)		uerier Enabled by (F	Robustness Variabl	e * Apply	
The VLAN Sett	ings of MLD snooping	I				
VLAN ID	VLAN Name	MLD Parameters	Settings Router Po	orts Settings M	Iulticast Entry Table	
1	default	MLDEdit		Edit	View	

Figure 4.92- Configuration > MLD Snooping > MLD Snooping Settings

MLD Snooping: Enable or disable the MLD Snooping.

MLD Global Settings:

Host Timeout (130-153025 sec): Specifies the time interval in seconds after which a port is removed from a Multicast Group. Ports are removed if a Multicast group MLD report was not received from a Multicast port within the defined *Host Timeout* period. The possible field range is 130 - 153025 seconds. The default timeout is 260 seconds.

Router Timeout (60-600): Specifies the time interval in seconds the Multicast router waits to receive a message before it times out. The possible field range is 60 - 600 seconds. The default timeout is 125 seconds.

Max Learned Entry Value (1-1024): Specifies the max learned entry value for MLD Snooping. The field range is 1-1024. The default is 256.

Click **Apply** to make the configurations take effect. Press the **Edit** button under **Router Port Setting**, and select the ports to be assigned for MLD snooping for the VLAN, and press **Apply** for changes to take effect.

Configuration > MLD Snooping > MLD Host Table

The MLD Host Table page displays the MLD Snooping information.



Figure 4.93- Configuration > MLD Snooping > MLD Host Table

Configuration > ISM VLAN Settings

In a switching environment, multiple VLANs may exist. Every time a multicast query passes through the Switch, the switch must forward separate different copies of the data to each VLAN on the system, which, in turn, increases data traffic and may clog up the traffic path. To lighten the traffic load, multicast VLANs may be incorporated. These multicast VLANs will allow the Switch to forward this multicast traffic as one copy to recipients of the multicast VLAN, instead of multiple copies.

Regardless of other normal VLANs that are incorporated on the Switch, users may add any ports to the multicast VLAN where they wish multicast traffic to be sent. Users are to set up a source port, where the multicast traffic is entering the switch, and then set the ports where the incoming multicast traffic is to be sent. The source port cannot be a recipient port and if configured to do so, will cause error messages to be

produced by the switch. Once properly configured, the stream of multicast data will be relayed to the receiver ports in a much more timely and reliable fashion.

The ISM VLAN Settings page allows the user to configure the ISM VLAN.

ISM VLAN Settings			O Safeguard
ISM VLAN Global State: O Enabled O D	isabled		Apply
VID State Member Ports(e.g.: 1-4,6) Tagged Member Ports UnTagged Source Ports Source Port Dynamical Learn	Disabled V Disabled V	VLAN Name IPv4 Replace Source IPv6 Replace Source IP Source Ports(e.g.: 1-4,6) Remap Priority	0.0.0.0
Replace CVID VID VLAN Name Replace Source IP	1-4094 None State MP	TMP SP USP	Clear All Add Group List

Figure 4.84 - Configuration > IGMP Snooping > ISM VLAN Settings

ISM VLAN Global State: Enable or disable the IGMP Snooping Multicast (ISM) VLAN Global State. Click **Apply** button to confirm the ISM VLAN Global State.

VID: Add the corresponding VLAN ID of the Multicast VLAN. Users may enter a value between 2 and 4094. **State:** Use the drop-down menu to enable or disable the selected Multicast VLAN.

Member Ports: Enter a port or list of ports to be added to the Multicast VLAN. Member ports shall be the untagged members of the multicast VLAN.

Tagged Member Ports: Enter a port or list of ports that will become tagged members of the Multicast VLAN. **UnTagged Source Ports:** Enter a port or list of ports that will become untagged members of the Multicast

VLAN.

Source Port Dynamical Learn: Specify the source port dynamical learning to be enabled or disabled.

VLAN Name: Enter the name of the new Multicast VLAN to be created. This name can be up to 32 characters in length.

IPv4 Replace Source: This field is used to replace the source IPv4 address of incoming packets sent by the host before being forwarded to the source port.

IPv6 Replace Source IP: This field is used to replace the source IPv6 address of incoming packets sent by the host before being forwarded to the source port.

Source Ports: Enter a port or list of ports to be added to the Multicast VLAN. Source ports shall be the tagged members of the multicast VLAN.

Replace CVID: Specify the VID to be replaced in CVID. The range is from 1-4094.

Remap Priority: Specify the remap priority (0 to 7) to be associated with the data traffic to be forwarded on the multicast VLAN. Specify **None**, the packet's original priority is used. The default setting is None.

Click **Add** to add the ISM VLAN which will appear in the table, or click **Clear All** to clear all fields. Click **Edit** button to modify the parameters and update the ISM VLAN Setting or click **Delete** to delete the ISM VLAN.

Click **View** to display the detail information of ISM VLAN.

VLAN Name rd3 Multicast Address (e.g.:235.1.1.1-235.1.1.9)	IPv4	
	O IPv6	Add Delete All
Multicast Group		

Figure 4.85 - Configuration > IGMP Snooping > ISM VLAN Settings

Configuration > Jumbo Frame

D-Link Gigabit Metro Ethernet Switches support jumbo frames (frames larger than the Ethernet frame size of 1536 bytes) of up to 10000 bytes (tagged). Default is disabled, Select **Enabled** then click **Apply** to turn on the jumbo frame support.

Jumbo Frame Se		🥚 Safeguard	
Jumbo Frame 🥕 Maximum Length is :		Disabled	Apply

Figure 4.47 – L2 Functions > Jumbo Frame

Configuration > Port Mirroring

Port Mirroring is a method of monitoring network traffic that forwards a copy of each incoming and/or outgoing packet from one port of the Switch to another port, where the packet can be studied. This enables network managers to better monitor network performances.

Port Mirroring Settings OSafeguard															
Port Mirroring O Enabled O Disabled Target Port 01															
Source Port Selection											Ap	oly			
Sniffer Mode	Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14
ТХ	All														
RX	All														
TX/RX	All														
None	All	•	0	•	0	0	•	•	•	•	0	•	•	•	•
Sniffer Mode	Select All	15	16	17	18	19	20	21	22	23	24	25	26	27	28
ТХ	All	•		•			•		•	•		•	0		
RX	All														
TX/RX	All														
None	All	•	•	•	•	•	•	•	•	•	•	•	•	•	•

Figure 4.48 – L2 Functions > Port Mirroring

Selection options for the Source Ports are as follows:

TX (transmit) mode: Duplicates the data transmitted from the source port and forwards it to the Target Port. Click "all" to include all ports into port mirroring.

RX (receive) mode: Duplicates the data that is received from the source port and forwards it to the Target Port. Click "all" to include all ports into port mirroring.

TX/RX (transmit and receive) mode: Duplicate both the data transmitted from and data sent to the source port, and forwards all the data to the assigned Target Port. Click "all" to include all ports into port mirroring. **None:** Turns off the mirroring of the port. Click "all" to remove all ports from mirroring.

Configuration > Loopback Detection

The Loopback Detection function is used to detect the loop created by ports which other prevention mechanism is not available, for example: Spanning Tree Protocol (STP). It usually happens when link partner is hub or un-management switch. Loopback Detection feature can automatically shutdown the port

and sends a log to the administrator when loop occurred. Also, Loopback Detection function offers recovery mechanism when loop condition removed.

oopback Dete	ction Settings	🥥 Safeguard
Loopback Detection	C Enabled Disabled	
Vode	Port-based VLAN List	
nterval (1-32767)	2 sec	
Recover Time (0 or 60-1000000)	60 sec	Apply
From Port	To Port State	
01 🗸	28 V Disabled	Refresh Apply
Port	State	Loop Status
01	Disabled	Normal
02	Disabled	Normal
03	Disabled	Normal
04	Disabled	Normal
05	Disabled	Normal
06	Disabled	Normal
07	Disabled	Normal
08	Disabled	Normal
09	Disabled	Normal
10	Disabled	Normal
11	Disabled	Normal

Figure 4.49 – L2 Functions > Loopback Detection

Loopback Detection: Use the drop-down menu to enable or disable loopback detection. The default is *Disabled.*

Mode: Specifies Port-based or VLAN-based mode. If port-based mode is selected, the loop happening port will be shut down and affect all member VLANs. If VLAN-based mode is selected, only the member port in the loop happening VLAN will be shut down.

VID List: Specifies the VID.

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

Recover Time (0 or 60-1000000): Time allowed (in seconds) for recovery when a Loopback is detected. The Loop Detection Recover Time can be set at 0 seconds, or 60 to 1000000 seconds. Entering 0 will disable the Loop Detection Recover Time. The default is 60 seconds.

From Port: The beginning of a consecutive group of ports may be configured starting with the selected port.

To Port: The ending of a consecutive group of ports may be configured starting with the selected port. **State:** Use the drop-down menu to toggle between *Enabled* and *Disabled*. Default is *Disabled*.

Click the Apply button to implement changes made or click Refresh to refresh the Loopback Detection table.

Configuration > SNTP Settings > Time Settings

SNTP or Simple Network Time Protocol is used by the Switch to synchronize the clock of the computer. The SNTP settings folders contain two windows: Time Settings and TimeZone Settings. Users can configure the time settings for the switch, and the following parameters can be set or are displayed in the Time Settings page.

Time Settings		O Safeguard
Clock Source Current Time	Local OSNTP 01/01/2014 01:02:07	
SNTP Server Configuration		
SNTP First Server	0.0.0.0 • IPv4	
	O IPv6	
SNTP Second Server	0.0.0.0 • IPv4	
	IPv6	
SNTP Poll Interval In Seconds (30-99999)	30	
Manually set current time		
Date (DD/MM/YYYY)	01/01/2014	
Time (HH:MM:SS)	01:02:07	
Set time from PC		
Date (DD/MM/YYYY)	16/01/2015	
Time (HH:MM:SS)	17:39:12	

Figure 4.98 – Configuration > SNTP Settings > Time Settings

Clock Source: Specify the clock source by which the system time is set. The possible options are:

Local - Indicates that the system time is set locally by the device.

SNTP - Indicates that the system time is retrieved from a SNTP server.

Current Time: Displays the current date and time for the switch.

If choosing **SNTP** for the clock source, then the following parameters will be available:

SNTP First Server: Select IPv4 or IPv6 and specify the IP address of the primary SNTP server from which the system time is retrieved.

SNTP Second Server: Select IPv4 or IPv6 and specify the IP address of the secondary SNTP server from which the system time is retrieved.

SNTP Poll Interval in Seconds (30-99999): Defines the interval (in seconds) at which the SNTP server is polled for Unicast information. The Poll Interval default is 30 seconds.

Click Apply to make the configurations take effect.

When selecting Local for the clock source, users can select from one of two options:

Manually set current time: Users input the system time manually.

Set time from PC: The system time will be synchronized from the local computer.

Configuration > SNTP Settings > TimeZone Settings

The TimeZone Setting Page is used to configure time zones and Daylight Savings time settings for SNTP.

TimeZone Settings	O Safeguard
Daylight Saving Time State	Disabled
Daylight Saving Time Offset In Minutes	60 •
Time Zone Offset.from GMT In +/-HH:MM	+ • 00 • 00 •
DST Repeating Settings	
From: Which Week of the Month	First •
From: Day of the Week	Sun 🔻
From: Month	Apr
From: Time In HH MM	00 • 00 •
To: Which Week of the Month	Last 🔻
To: Day of the Week	Sun 🔻
To: Month	Oct •
To: Time In HH MM	00 🔻 00 🔻
DST Annual Settings	
From: Month	Apr 🔹
From: Day	29 🔻
From: Time In HH MM	00 🔻 00 🔻
To: Month	Oct •
To: Day	12 🔻
To: Time In HH MM	00 • 00 •
	Apply

Figure 4.99 – Configuration > SNTP > TimeZone Settings

Daylight Saving Time State: Enable or disable the DST Settings.

Daylight Saving Time Offset: Use this drop-down menu to specify the amount of time that will constitute the local DST offset - *30*, *60*, *90*, or *120* minutes.

Time Zone Offset GMT +/- HH:MM: Use these drop-down menus to specify the local time zone's offset from Greenwich Mean Time (GMT.)

DST Repeating Settings:

From: Which Week of the Month: Enter the Week of Month will start on, each year.

From: Day of the Week: Enter the Day DST will start on, each year.

From: Month: Enter the month DST will start on, each year.

From: Time In HH:MM: Enter the time of day that DST will start on, each year.

To: Which Week of the Month: Enter the Week of Month will end on, each year.

To: Day of the Week: Enter the day of week that DST will end on, each year.

To: Month: Enter the month DST and date DST will end on, each year.

To: Time In HH:MM: Enter the time of day that DST will end on, each year.

DST Annual Settings:

From: Month / Day: Enter the month DST and date DST will start on, each year.
From: Time In HH:MM: Enter the time of day that DST will start on, each year.
To: Month / Day: Enter the month DST and date DST will end on, each year.
To: Time HH:MM: Enter the time of day that DST will end on, each year.

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

Configuration > DHCP Relay > DHCP Relay Global Settings

User can enable and configure DHCP/BOOTP Relay Global Settings on the Switch.

DHCP Relay Global Settings		O Safeguard
DHCP Relay State DHCP Relay Hops Count Limit (1-16) DHCP Relay Time Threshold (0-65535) DHCP Relay Port List (e.g.: 4-6) DHCP Relay Vlan Settings State(VLAN ID)	Disabled	
DHCP Relay Agent Information Option 82 State DHCP Relay Agent Information Option 82 Check DHCP Relay Agent Information Option 82 Policy DHCP Relay Agent Information Option 82 Remote ID	Enabled v Disabled v Replace v Default v EC-AD-E0-62-AF-A0	Apply



Parameters	Descriptions
DHCP Relay State	This field can be toggled between Enabled and Disabled using the pull-down menu. It is used to enable or disable the DHCP/BOOTP Relay service on the Switch. The default is <i>Disabled</i> .
DHCP Relay Hops Count Limit (1-16)	This field allows an entry between <i>1</i> and <i>16</i> to define the maximum number of router hops DHCP/BOOTP messages can be forwarded across. The default hop count is 4.
DHCP Relay Time Threshold (0-65535)	Allows an entry between 0 and 65535 seconds, and defines the maximum time limit for routing a DHCP/BOOTP packet. If a value of 0 is entered, the Switch will not process the value in the

	seconds field of the BOOTP or DHCP packet. If a non-zero value is entered, the Switch will use that value, along with the hop count to determine whether to forward a given BOOTP or DHCP packet.
DHCP Relay Port List	Specify the ports for BOOTP relay.
DHCP Relay VLAN Setting State	Specify the VLAN ID to monitor DHCP client activity. The range is from 1 – 4094.
DHCP Relay Agent Information Option 82 State	It is used to enable or disable the DHCP Agent Information Option 82 on the Switch. The default is Disabled.
	Enabled – When this field is toggled to Enabled the relay agent will insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients. When the relay agent receives the DHCP request, it adds the option 82 information, and the IP address of the relay agent (if the relay agent is configured), to the packet. Once the option 82 information has been added to the packet it is sent on to the DHCP server. When the DHCP server receives the packet, if the server is capable of option 82, it can implement policies like restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server unicasts reply to the back to the relay agent if the request was relayed to the server by the relay agent. The switch verifies that it originally inserted the option 82 data. Finally, the relay agent removes the option 82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request.
	insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the check and policy settings will have no effect.
DHCP Relay Agent Information Option 82 Check	It filed is used to enable or disable the ability to check DHCP option 82 information in DHCP packets:
	Enabled – When the field is configured to Enabled, the relay agent checks if DHCP packets carries option 82 information. If option 82 does not carried, the DHCP packet would be dropped. Disabled – No check would be executed when check state configured to Disabled.
DHCP Relay Agent Information Option 82 Policy	This filed is used to configure the policy for each port. It is used to set the Switches policy for handling packets when the DHCP Agent Information Option 82 Check is set to Disabled. There are 3 policies available to use:
	Replace - The option 82 field will be replaced if the option 82 field already exists in the packet received from the DHCP client. Drop - The packet will be dropped if the option 82 field already
	exists in the packet received from the DHCP client. Keep -The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client.
DHCP Relay Agent Information Option 82 Remote ID	This filed is used to configure the contents of Remote ID used in option 82. Options: Default , User Define are available to use.

Click **Apply** to apply the configurations.



NOTE: If the Switch receives a packet that contains the option-82 field from a DHCP client and the information-checking feature is enabled, the switch drops the packet because it is invalid. However, in some instances, user might configure a client with the option-82 field. In this

situation, user should disable the information-check feature so that the switch does not remove the option-82 field from the packet. User can configure the action that the switch takes when it receives a packet with existing option-82 information by configuring the **DHCP Agent Information Option 82 Policy**.

Configuration > DHCP Relay > DHCP Relay Interface Settings

This page allows the user to set up a server, by IP address, for relaying DHCP/BOOTP information the switch. The user may enter a previously configured IP interface on the Switch that will be connected directly to the DHCP/BOOTP server using the following window. Properly configured settings will be displayed in the **BOOTP Relay Table** at the bottom of the following window, once the user clicks the **Add** button under the **Apply** heading. The user may add up to four server IPs per IP interface on the Switch. Entries may be deleted by clicking Delete button.

Interface System		
Server IP		Apply
DHCP/BOOTP Relay Interface Table Interface Server1 Server2	Server3 Server4	

Figure 4.101 - Configuration > DHCP/BOOTP Relay > DHCP/BOOTP Relay Interface Settings

Interface: The IP interface on the Switch that will be connected directly to the Server.

Server IP: Enter the IP address of the DHCP/BOOTP server. Up to four server IPs can be configured per IP Interface.

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

Configuration > DHCP Local Relay Settings

The DHCP Local Relay Settings page allows the user to configure DHCP Local Relay. DHCP broadcasts are trapped by the switch CPU, and replacement broadcasts are forwarded with Option 82. Replies from the DHCP servers are trapped by the switch CPU, the Option 82 is removed and the reply is sent to the DHCP Client.

DHCP Local Relay S	HCP Local Relay Settings						
DHCP/BOOTP Local Relay Status DHCP/BOOTP Local Relay Port List (e.g.: 4-6)	Enabled Oisabled None	Apply Apply					
Config DHCP Local Relay fo Config VLAN by: VID DHCP/BOOTP Local Relay V	▼ St	ate Disabled Apply					

Figure 4.102 - Configuration > DHCP Local Relay Settings

DHCP/BOOTP Local Relay Status: Specifies whether DHCP Local Relay is enabled on the device. Enabled – Enables DHCP Local Relay on the device.

Disabled – Disables DHCP Local Relay on the device. This is the default value.

DHCP/BOOTP Local Relay Port List: Specifies the port or ports for DHCP/BOOTP local relay port.

Config VLAN by: Configure the VLAN by VID or VLAN Name of drop-down menu.

State: Specifies whether DHCP Local Relay is enabled on the VLAN.

Enabled – Enables DHCP Local Relay on the VLAN.

Disabled – Disables DHCP Local Relay on the VLAN.

DHCP Local Relay VID List: Displays the list of VLANs on which DHCP Local Relay has been defined.

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

Configuration > DHCPv6 Relay Settings

The DHCPv6 Relay Settings page allows user to configure the DHCPv6 settings.

HCPv6 Relay Settings		0 Safeguaro
DHCPv6 Relay State	Disabled	
DHCPv6 Relay Hops Count Limit (1-32)	4	
DHCPv6 Relay Option37 State	Disabled •	
DHCPv6 Relay Option37 Check	Disabled	
DHCPv6 Relay Option37 Remote ID Type	Default	
	EC-AD-E0-62-AF-A0	Apply
nterface	System	
Server IP		Apply

Figure 4.103 - Configuration > DHCPv6 Relay Settings

DHCPv6 Relay Status: Specifies whether DHCPv6 Relay is enabled on the device.

Enabled – Enables DHCPv6 Relay on the device.

Disabled – Disables DHCPv6 Relay on the device. This is the default value.

DHCPv6 Relay Hops Count Limit (1-32): The field allows and entry between 1 and 32 to define the maximum number of router hops DHCPv6 messages can be forwarded. The default hop count is 4.

DHCPv6 Relay Option37 State: Specifies the DHCPv6 Relay Option37 State to be enabled or disabled. DHCPv6 Relay Option37 Check: Specifies the DHCPv6 Relay Option37 Check to be enabled or disabled. DHCPv6 Relay Option37 Remote ID Type: Specifies the DHCPv6 Relay Option37 Remote ID type is CID with User Defined, User Defined or Default.

Interface: Enter a name of the interface. **Server IP:** Enter the server IP address.

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

Configuration > Spanning Tree > STP Bridge Global Settings

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

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

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

By default, Rapid Spanning Tree is disabled. If enabled, the Switch will listen for BPDU packets and its accompanying Hello packet. BPDU packets are sent even if a BPDU packet was not received. Therefore, each link between bridges is sensitive to the status of the link. Ultimately this difference results in faster detection of failed links, and thus faster topology adjustment.

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

After enabling STP,	setting the STP	Global Setting	includes the	following options:
Alter chabling off,	sound the off	Olobal Octaing	moluues me	following options.

ttings			O Safeguard
Enabled	Disabled		
RSTP	•	Root Bridge	00:00:00:00:00:00:00
32768	T	Root Cost	0
	6	Root Maximum Age	20
	20	Root Forward Delay	15
	2	Root Port	0
	15		
Enabled	T		
	20		
			Apply Refresh
	© Enabled RSTP 32768 	Enabled Disabled RSTP 32768 6 20 21 15 Enabled	Enabled Disabled Root Bridge 32768 Root Cost Root Maximum Age 20 Root Forward Delay 2 Root Port 15 Enabled

Figure 4.105 - Configuration > Spanning Tree > STP Bridge Global Settings

STP State: Specify the Spanning Tree Protocol to be Enabled or Disabled.

STP Version: Choose MSTP, RSTP or STP Compatible. The default setting is MSTP.

Bridge Priority: This value between 0 and 61410 specifies the priority for forwarding packets: the lower the value, the higher the priority. The default is 32768.

TX Hold Count (1-10): Used to set the maximum number of Hello packets transmitted per interval. The count can be specified from *1* to *10*. The default is *6*.

Maximum Age (6-40 sec): This value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that the Switch has the lowest Bridge Identifier, it will become the Root Bridge. A time interval may be chosen between 6 and 40 seconds. The default value is 20. (Max Age has to have a value bigger than Hello Time)

Hello Time (1-10 sec): The user may set the time interval between transmissions of configuration messages by the root device, thus stating that the Switch is still functioning. The default is 2 seconds.

Forward Delay (4-30 sec): This sets the maximum amount of time that the root device will wait before changing states. The default is 15 seconds.

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

Enabled - BPDU filtering is enabled on the port.

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

Maximum Hop (6-40 secs): Specifies the number of hops between devices in a spanning tree region before the BPDU (bridge protocol data unit) packet sent by the Switch will be discarded. Each switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BPDU packet and the information held for the port will age out. The user may set a hop count from 6 to 40. The default is 20.

Root Bridge: Displays the MAC address of the Root Bridge.

Root Cost: Defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is *0* (auto).

Root Maximum Age: Displays the Maximum Age of the Root Bridge. The default is 20.

Root Forward Delay: Displays the Forward Delay of the Root Bridge. The default is 15.

Root port: Displays the root port.

Click **Apply** for the settings to take effect. Click **Refresh** to renew the page.

Configuration > Spanning Tree > STP Port Settings

STP can be set up on a port per port basis. In addition to setting Spanning Tree parameters for use on the switch level, the Switch allows for the configuration of the groups of ports, each port-group of which will have its own spanning tree, and will require some of its own configuration settings.

An STP Group spanning tree works in the same way as the switch-level spanning tree, but the root bridge concept is replaced with a root port concept. A root port is a port of the group that is elected based on port priority and port cost, to be the connection to the network for the group. Redundant links will be blocked, just as redundant links are blocked on the switch level.

The STP on the switch level blocks redundant links between switches (and similar network devices). The port level STP will block redundant links within an STP Group.

TP P	ort Setti	ngs								O Safegua	rd
From Po	ırt	0	1 🔻	To Port		28	▼ Sta	ite	Enabled	T	
External (0-20000 D=AUTO)	00000;		2000000	Migrate		Disabled	▼ Ed	ge	Auto	¥	
Priority		128	T	P2P		Auto	▼ Re	stricted Role	False	•	
Restricte	ed TCN	False	•	Forward BP	DU	Enabled	▼ He	llo Time		2	
									Apply	Refresh	
Port	State	Priority	External Cost	Edge	P2P	Restricted Role	Restricted TCN	Forward BPDU	Hello Time	Port State	*
01	Enable	128	AUTO/20000	Auto	Auto	False	False	Enable	2	Disabled	
02	Enable	128	AUTO/20000	Auto	Auto	False	False	Enable	2	Disabled	
03	Enable	128	AUTO/20000	Auto	Auto	False	False	Enable	2	Disabled	
04	Enable	128	AUTO/20000	Auto	Auto	False	False	Enable	2	Disabled	
05	Enable	128	200000	Auto	Auto	False	False	Enable	2	Disabled	
06	Enable	128	AUTO/20000	Auto	Auto	False	False	Enable	2	Disabled	
07	Enable	128	AUTO/20000	Auto	Auto	False	False	Enable	2	Disabled	
08	Enable	128	AUTO/20000	Auto	Auto	False	False	Enable	2	Disabled	
										h	-

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

Figure 4.106 – Configuration > Spanning Tree > STP Port Settings

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

State: Use the drop-down menu to enable or disable STP by per-port based. It will be selectable after the global STP is enabled.

External Cost: This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. Thedefault value is 0 (auto).

0 (auto) - Setting 0 for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000.

Value 1-200000000 - Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.

Migrate: Setting this parameter as *Yes* will set the ports to send out BPDU packets to other bridges, requesting information on their STP setting. If the Switch is configured for RSTP, the port will be capable to migrate from 802.1d STP to 802.1w RSTP. Migration should be set as yes on ports connected to network

stations or segments that are capable of being upgraded to 802.1w RSTP on all or some portion of the segment.

Edge: Selecting the *True* parameter designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received, it automatically loses edge port status. Selecting the *False* parameter indicates that the port does not have edge port status. Selecting the *Auto* parameter indicates that the port status or not have edge port status automatically.

Priority: Specify 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.

P2P: Choosing the *True* parameter indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports, however they are restricted in that a P2P port must operate in full-duplex.

Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A p2p value of *false* indicates that the port cannot have p2p status. *Auto* allows the port to have p2p status whenever possible and operate as if the p2p status were true. If the port cannot maintain this status, (for example if the port is forced to half-duplex operation) the p2p status changes to operate as if the p2p value were *False*. The default setting for this parameter is *Auto*.

Restricted Role: Toggle between *True* and *False* to set the restricted role state of the packet. If set to *True*, the port will never be selected to be the Root port. The default value is *False*.

Restricted TCN: Toggle between *True* and *False* to set the restricted TCN of the packet. Topology Change Notification (TCN) is a BPDU that a bridge sends out to its root port to signal a topology change. If set to *True*, it stops the port from propagating received TCN and to other ports. The default value is *False*.

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

Disabled – BPDU filtering is enabled on the port.

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

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

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

Click **Refresh** to renew the page.

Configuration > Spanning Tree > MST Configuration Identification

The MST Configuration Identification page allows user to configure a MSTI instance on the switch. These settings will uniquely identify a multiple spanning tree instance set on the switch. The Switch initially possesses one CIST or Common Internal Spanning Tree of which the user may modify the parameters for but cannot change the MSTI ID for, and cannot be deleted.

MST Configuration Identification		O Safeguard
MST Configuration Identification Settings		
Configuration Name	9C-D6-43-60-4F-A4	
Revision Level (0-65535)	0	Apply
·		
Instance ID Settings		
MSTI ID (1-15)		
Туре	Add VID •	
VID List (1-4094)		Apply
· · ·		
Total Entries: 1 MSTI ID VID List		
CIST 1-4094		Edit Delete

Figure 4.107 - Configuration > Spanning Tree > MST Configuration Identification

MST Configuration Identification Settings:

Configuration Name: A previously configured name set on the Switch to uniquely identify the MSTI (Multiple Spanning Tree Instance). If a configuration name is not set, this field will show the MAC address to the device running MSTP. This field can be set in the **STP Bridge Global Set-tings** window.

Revision Level: This value, along with the Configuration Name will identify the MSTP region configured on the Switch. The user may choose a value between *0* and *65535* with a default setting of *0*.

MSTI ID (1-15): Enter a number between *1* and *15* to set a new MSTI on the Switch.

Type: This field allows the user to choose a desired method for altering the MSTI settings.

Add VID - Select this parameter to add VIDs to the MSTI ID, in conjunction with the VID List parameter.

Remote VID – Select this parameter to remove VIDs from the MSTI ID, in con-junction with the VID List parameter.

VID List (1-4094): This field displays the VLAN IDs associated with the specific MSTI.

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

Configuration > Spanning Tree > STP Instance Settings

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

STP Instance Settin	ngs			O Safe	eguard
STP Priority Settings	Priority	0			Apply
Total Entries: 1					
Instance Type Inst	ance Status	Instance Price	ority		
CIST Enable	d	32768(Bridge Prior	rity : 32768, SYS ID Ext : 0)	Edit	View
STP Instance Operational S	Status				
MSTP ID			Designated Root Bridge		
External Root Cost			Regional Root Bridge		
Internal Root Cost			Designated Bridge		
Root Port			Max Age		
Forward Delay			Remaining Hops		
Topology Changes Count			Last Topology Change		

Figure 4.108 - Configuration > Spanning Tree > STP Instance Settings

To modify an entry on the table, click the **Edit** button. To view more information about and entry on the table at the top of the window, click the **view** button.

The window above contains the following information:

MSTI ID: Enter the MSTI ID in this field. An entry of 0 denotes the CIST (default MSTI).

Priority: Enter the new priority in the Priority field. The user may set a priority value between 0-61440.

Click **Apply** to implement the new priority setting.

Configuration > Spanning Tree > MSTP Port Information

The MSTP Port Information page can be used to update the port configuration for an MSTI ID. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for interfaces to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest MAC address into the forwarding state and other interfaces will be blocked.

To View the MSTI settings for a particular port, select the Port number and click **Find** button. To modify the settings for a particular MSTI Instance, click **Edit** button, then modify the MSTP Port Setting and click **Apply**.

MSTF	Port Information					O Safeguard
Port	1 •					Find
MSTP F	Port Setting					
Instanc	e ID	Internal Path Cost (0-200000000; 0=AUTO)	Priority	0	¥	Apply
Port 1 S	Settings					
MSTI	Designated Bridge	Internal Path Cost	Priority	Status	Role	
0	N/A	AUTO/20000	128	Enabled	Disabled	Edit

Figure 4.109 - Configuration > Spanning Tree > MST Port Information

Instance ID: Displays the MSTI ID of the instance being configured. An entry of *0* in this field denotes the CIST (default MSTI).

Internal Path Cost (0=Auto): This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within a STP instance. The default setting is 0 (auto).

0 (Auto) - Selecting this parameter for the internal Cost will set quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface.

Value 0-2000000 - Selecting this parameter with a value in the range of *0* to 2000000 will set the quickest route then a loop occurs. A lower internal cost represents a quicker transmission.

Priority: Enter a value between 0 and 240 to set the priority for the port interface. A higher priority will designate the interface to forward packets first. A lower number denotes a higher priority.

Configuration > 802.3ah EthernetLink OAM > Ethernet OAM Port Settings

The Ethernet OAM Port Settings page allows user to configure the Ethernet OAM settings.

From Port To Port Mode	State	Remote Loopback	Received Remote Loopback	
01 🔻 01 🔻 🗖 Active 🔻	🔲 Disabled 🔻	Start	▼ □ Ignore	•
				Apply
Ethernet OAM Port Status Table				
Port 1				
Local Client				
OAM	Disabled			
Mode	Active			
Max OAMPDU	1518 Bytes			
Remote Loopback	Support			
Unidirection	Not Supporter	d		
Link Monitoring	Support			
Variable Request	Support			
PDU Revision	0			
Operation Status	Disabled			
Loopback Status	No Loopback			
Port 2				
Local Client				
OAM	Disabled			
Mode	Active			
Max OAMPDU	1518 Bytes			
Remote Loopback	Support			
Unidirection	Not Supported	d		
Link Monitoring	Support			
Variable Request	Support			
PDU Revision	0			
Operation Status	Disabled			
Loopback Status	No Loopback			

Figure 4.110 - Configuration > Ethernet OAM > Ethernet OAM Port Settings

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

Mode: Use the drop-down menu to select to operate in either **Active** or **Passive**. The default mode is **Active**. **State:** Use the drop-down menu to enable or disable the OAM function.

Remote Loopback: Specifies the Ethernet OAM remote loopback is None or Start.

None - Select to disable the remote loopback.

Start – Select to request the peer to change to the remote loopback mode.

Received Remote Loopback: To configure the client to process or to ignore the received Ethernet OAM remote loopback command.

Process – Select to process the received Ethernet OAM remote loopback command.

Ignore - Select to ignore the received Ethernet OAM remote loopback command.

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

Configuration > 802.3ah EthernetLink OAM > Ethernet OAM Event Configuration

The Ethernet OAM Event Configuration page allows user to configure the Ethernet OAM configuration settings.

Ethernet OAM Event Configura	ation				O Safeguard
From To Port Link Event	Link Monitor		Threshold (0-4294967295)	Window (1000-60000)	
01 • 01 • Link Monitor	 Error Symbol 	ol 🔻	1	1000	ms
Notify					
Disabled 🔻					Apply
Ethernet OAM Event Confiduration Table					
Port 1					<u> </u>
OAM		Disabled			
Mode		Active			
Dying Gasp		Enabled			
Critical Event		Enabled			
Remote Loopback OAMPDU		Not Processed			
Symbol Error					
Notify State		Enabled			
Window		1000 Milliseconds			
Threshold		1 Errored Symbol			
Frame Error					
Notify State		Enabled			
Window		1000 Milliseconds			
Threshold		1 Errored Frame			
Frame Period Error					
Notify State		Enabled			
Window		148810 Frames			
Threshold		1 Errored Frame			

Figure 4.111 - Configuration > Ethernet OAM > Ethernet OAM Event Configuration

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

Link Event: Select the link event, Link Monitor or Critical Link Event.

Link Monitor: Select the link monitor. Available options are Error Symbol, Error Frame, Error Frame Period, and Error Frame Seconds.

Threshold (0-4294967295): Enter the number of error frame or symbol in the period is required to be equal to or greater than in order for the event to be generated.

Window (1000-60000): Enter the period of error frame or symbol in milliseconds summary event.

Notify: Select the notification to be enabled or disabled.

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

Configuration > DULD > DULD Port Settings

The DULD Port Settings page allows user to configure the unidirectional link detection on ports. Unidirectional link detection provides discovery mechanism based on 802.3ah to discovery its neighbor. If the OAM discovery can complete in configured discovery time, it concludes the link is bidirectional. Otherwise, it starts detecting task to detect the link status.

ULD Setti	ings					O Safeguar
rom Port D1	To Port 28	Admin State Disabled v	Mode Normal ▼	Discovery Time (5-65535) 5 sec(s	5)	Apply
Port	Admin State	Oper Status	Mode	Link Status	Discovery Time	*
1	Disabled	Disabled	Normal	Unknown	5	
2	Disabled	Disabled	Normal	Unknown	5	
3	Disabled	Disabled	Normal	Unknown	5	
ļ.	Disabled	Disabled	Normal	Unknown	5	
5	Disabled	Disabled	Normal	Unknown	5	
ò	Disabled	Disabled	Normal	Unknown	5	
7	Disabled	Disabled	Normal	Unknown	5	
3	Disabled	Disabled	Normal	Unknown	5	
)	Disabled	Disabled	Normal	Unknown	5	
10	Disabled	Disabled	Normal	Unknown	5	
1	Disabled	Disabled	Normal	Unknown	5	
2	Disabled	Disabled	Normal	Unknown	5	
3	Disabled	Disabled	Normal	Unknown	5	
4	Disabled	Disabled	Normal	Unknown	5	
15	Disabled	Disabled	Normal	Unknown	5	
16	Disabled	Disabled	Normal	Unknown	5	
17	Disabled	Disabled	Normal	Unknown	5	
8	Disabled	Disabled	Normal	Unknown	5	*

Figure 4.121 - Configuration > DULD > DULD Port Settings

From Port / To Port: Specifies a range of ports to be configured.

Admin State: Enable or disable the port unidirectional link detection status. The default is disabled.

Mode: Specifies the mode of DULD.

Normal – Only log and event when a unidirectional link is detected.

Shutdown - If any unidirectional link is detected, disable the port and log an event.

Discovery Time (5-65535): Specifies these ports neighbor discovery time. If the discovery is timeout, the unidirectional link detection will start. The default discovery time is **5** seconds.

Configuration > Multicast Forwarding & Filtering > Multicast Forwarding

Allow user to create static multicast entry.

/ID	arding Settings																												
Multicast MAC A	ddress																							Cle	ear A	I		Apply	
Port	Select All	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Egress	All																												
None	All	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲	۲
gress Ports																													
otal Entries: 0																													

VID: Specify the VID

Multicast MAC Address: Specify the multicast address. **Egress**: Click the Port Number for multicast traffic.

Configuration > Multicast Forwarding & Filtering > Multicast Filter Mode

The Multicast Filtering Mode page allows user to set up the filtering mode.

Multicast Filter Mode	9		Safeguard
From Port To Po 01 28	ort 🔹	Multicast Filter Mode Forward Unregistered Groups	▼ Apply
Port	Multicast Filter Mode		· · · · · · · · · · · · · · · · · · ·
1	Forward Unregistere		
2	Forward Unregistere		
3	Forward Unregistere		
4	Forward Unregistere		
5	Forward Unregistere		
6	Forward Unregistere		
7	Forward Unregistere		
8	Forward Unregistere		
9	Forward Unregistere		
10	Forward Unregistere		
11	Forward Unregistere		
12	Forward Unregistere		
13	Forward Unregistere		
14	Forward Unregistere		
15	Forward Unregistere		
16	Forward Unregistere		
17	Forward Unregistere		
18	Forward Unregistere	d Groups	*

Figure 4.122 - Configuration > Multicast Forwarding & Filtering > Multicast Filtering

From Port / To Port: Specify the ports of the VLAN on which the corresponding MAC address belongs to. **Multicast Filtering Mode:** This drop-down menu allows user to select the action the Switch will take when it receives a multicast packet that is to be forwarded to one of the ports in the range specified above.

Forward Unregistered Groups - This will instruct the Switch to forward a multicast packet whose destination is an unregistered multicast group residing within the range of ports specified above.

Filter Unregistered Groups - This will instruct the Switch to filter any multicast packets whose destination is an unregistered multicast group residing within the range of ports specified above.

Configuration > Multicast Forwarding & Filtering > IP Multicast Profile Settings

The IP Multicast Profile Settings page allows user to configure the IP Multicast Profile.

IP Multecast I	Profile Settings		0 Sa	feguard
Profile Type Pr (Pv4 ▼	ofile ID Profile Na	me	Add	
Total Entries:0			Profile Type IPv4 Delete	All
Profile Type	Profile ID	Profile Name		

Figure 4.87 - Configuration > IGMP Snooping > IP Multicast Profile Settings

Profile ID: Specify the Profile ID.

Profile Name: Specify the Profile Name.

Click Add to create a new IP Multicast Profile or click Delete All to clear all the entries.

Configuration > Multicast Forwarding & Filtering > Limited Multicast Range Settings

The Limited Multicast Range Settings page allows user to configure the Limited Multicast. Specify the port range, select Access IP Type is *IPv4* or *IPv6* and select the Access is *Deny* or *Permit* then Click Apply to make the configurations take effect.

Limited Multicast	Range Settings		0	Safeguard		
From Port To Po	rt Access IP Type ▼ IPv4 ▼	Access Permit T		Apply		
From Port To Po	rt Profile Type ▼ IPv4 ▼	Profile ID 1 ▼	Add	Delete		
Port		Profile ID	Acc	ess State		
1		IPV4: IPV6:		IPV4: permit IPV6: permit		
2		IPV4: IPV6:	IPV	IPV4: permit IPV6: permit		
3		IPV4: IPV6:	IPV	IPV4: permit IPV6: permit		
4		IPV4: IPV6:	IPV	4: permit 6: permit		
5		IPV4: IPV6:	IPV	4: permit 6: permit		
6		IPV4: IPV6:	IPV	4: permit 6: permit		
7		IPV4: IPV6:	IPV	4: permit 6: permit		
8		IPV4: IPV6:	IPV	4: permit 6: permit		

Figure 4.88- Configuration > IGMP Snooping > Limited Multicast Range Settings

From Port / To Port: Specify the port ranges to be configured.

Profile Type: Specify the profile type is IPv4 or IPv6.

Profile ID: Specify the Profile ID.

Click Add to create the Profile ID with specified ports or click Delete to remove the ports

Configuration > Multicast Forwarding & Filtering > MAX Multicast Group Settings

The Max Multicast Group Settings page allows user to configure the max multicast group for IGMP Snooping.

rom Port	To Port	IP Type	Max Group (1-32)	
01 ▼	28 🔻	IPv4 ▼	32	Apply
Port		Aulticast Group	IPv6 MAX Multicast Group	*
1	32		32	
2	32		32	
2	32		32	
ļ	32		32	
i	32		32	
5	32		32	
,	32		32	
}	32		32	
)	32		32	
0	32		32	
11	32		32	
2	32		32	
3	32		32	
4	32		32	
15	32		32	
6	32		32	
17	32		32	
8	32		32	*

Figure 4.89- Configuration > IGMP Snooping > Max Multicast Group Settings

From Port / To Port: Specify the port ranges to be configured.

IP Type: Specify the IP type is IPv4 or IPv6.

Max Group (1-32): Specify the Max Group to be configured.

Action: Use the drop-down menu to select the appropriate action for this rule. The user can select **Drop** to initiate the drop action or the user can select **Replace** to initiate the replace action.

Click Apply to make the configurations take effect.

QoS > Traffic Control

The Traffic Control feature provides the ability to control the receive rate of broadcast, multicast, and unknown unicast packets. Once a packet storm has been detected, the Switch will drop packets coming into the Switch until the storm has subsided.

Traffic Control						_	O Safeguard
Traffic Control Settings From Port	01 🔻		To Port		28	•	
Drop Threshold (64Kbps * N) Action Time Interval (5-30) Storm Control Type	N = (64Kbps * 1 Drop ▼ 5 sec None	1~15625) = 64	Kbps Count Down (Shutdown Thr	0 or 5-30) eshold (0-255000)	0 1000	min pkt/s	Apply
Auto Recover Time(0-65535)	0 min						Apply
Traffic Trap Settings	None]					Apply
Port Storm Control 1 None 2 None 3 None 4 None 5 None	Type Action Drop Drop Drop Drop Drop	Threshold 0 Kbps 0 Kbps 0 Kbps 0 Kbps 0 Kbps	Count Down 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Interval 0 0 0 0 0	Port status Normal Normal Normal Normal	Shutdown Forever	

Figure 4.125 – QoS > Traffic Control

Parameter	Description				
From Port / To Port	Specify the From and To port(s) to be configured.				
Action	Dropkbps : Utilizes the hardware Traffic Control mechanism, which means the Switch's hardware will determine the Packet Storm based on the Threshold value stated and drop packets until the issue is resolved.				
	Shutdown : Utilizes the Switch's software Traffic Contr mechanism to determine the Packet Storm occurring. One detected, the port will deny all incoming traffic to the po- except STP BPDU packets, which are essential in keepir the Spanning Tree operational on the Switch. If the countdown timer has expired and yet the Packet Store continues, the port will be placed in rest mode and if r action is taken will enter auto-recovery mode after a fix minute period. Choosing this option obligates the user configure the interval setting as well, which will provide packet count samplings from the Switch's chip to determine if a Packet Storm is occurring.				
	DropbyPPS : Utilizes the hardware Traffic Control mechanism, which means the Switch's hardware will determine the Packet Storm based on the Threshold value stated and drop packets until the issue is resolved.				
Drop Threshold (64Kbps * N)	Specify the threshold from $64 \sim 1,024,000$ Kbit per second, with steps (N) of 64Kbps. N can be from 1 to 16000.				
Count Down (0 or 5-30)	The countdown timer is set to determine the amount of time, in minutes, that the Switch will wait before shutting down the port that is experiencing a traffic storm. This parameter is only useful for ports configured as Shutdown in their Action field and therefore will not operate for Hardware based Traffic Control implementations. The				

T	possible time settings for this field are 0, 5-30 minutes. 0 denotes that the port will never shutdown.
Time Interval (5-30)	The interval will set the time between Multicast and Broadcast packet counts sent from the Switch's chip to the Traffic Control function. These packet counts are the determining factor in deciding when incoming packets exceed the Threshold value. The interval may be set between 5 and 30 seconds with the default setting of 5 seconds.
Shutdown Threshold (0-255000)	Specify the shutdown threshold for traffic threshold.
Storm Control Type	User can select the different Storm type from Broadcast, Multicast, Broadcast + Multicast, Unknown Unicast, Broadcast + Unknown Unicast, Multicast + Unknown Unicast, and Broadcast + Multicast + Unknown Unicast.

Click Apply for the settings to take effect.

Auto Recover Time (0-65535): Specify the auto recover time. The value is from 0 to 65535. Click **Apply** for the settings to take effect.

Traffic Trap Settings: Specify the traffic trap is **None**, **Storm Occurred**, **Storm Cleared** or **Both**. Click **Apply** for the settings to take effect.



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

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



NOTE: Ports that are in rest mode will be seen as link down in all windows and screens until it enters the auto-recovery mode or the user recovers these ports by configuring the port state.

QoS > Bandwidth Control

The Bandwidth Control page allows network managers to define the bandwidth settings for a specified port's transmitting and receiving data rates.

andwidth Cont	rol			0 Safegua
	To Port Type 28 RX ndwidth control value need multiple of	Disabled •	(16-1000000) Kbits/Sec	Apply
Port	Tx Rate (Kbits/Sec)	Rx Rate (Kbits/Sec)	Effective RX (Kbit/Sec)	Effective TX (Kbit/Sec)
	No Limit	No Limit	No Limit	No Limit
2	No Limit	No Limit	No Limit	No Limit
	No Limit	No Limit	No Limit	No Limit
ļ	No Limit	No Limit	No Limit	No Limit
	No Limit	No Limit	No Limit	No Limit
	No Limit	No Limit	No Limit	No Limit
	No Limit	No Limit	No Limit	No Limit
	No Limit	No Limit	No Limit	No Limit
	No Limit	No Limit	No Limit	No Limit
0	No Limit	No Limit	No Limit	No Limit
1	No Limit	No Limit	No Limit	No Limit
2	No Limit	No Limit	No Limit	No Limit
3	No Limit	No Limit	No Limit	No Limit
4	No Limit	No Limit	No Limit	No Limit
5	No Limit	No Limit	No Limit	No Limit
6	No Limit	No Limit	No Limit	No Limit
	No Limit	No Limit	No Limit	No Limit

Figure 4.126 – QoS > Bandwidth Control

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

Type: This drop-down menu allows user to select between *RX* (receive), *TX* (transmit), and *Both*. This setting will determine whether the bandwidth ceiling is applied to receiving, transmitting, or both receiving and transmitting packets.

No Limit: This drop-down menu allows user to specify that the selected port will have no bandwidth limit. *Enabled* disables the limit.

Enabled disables the limit.

Rate 16-1000000): This field allows user to enter the data rate, in Kbits per second, will be the limit for the selected port. The value is between 63 and 1024000.

Click **Apply** to set the bandwidth control for the selected ports.



NOTE: The TX rate for Gigabit ports can only be configured in multiples of 1850kbps. If any other value is used, the system automatically rounds it down to the lower multiple of 1850.

QoS > QoS Settings

This page allows user to configure Qos port priority and queue mechanism.

QoS Settings								O Safeguard
Select QoS Mode Queuing mechanism	802.1P Strict Priority	T T						Apply
[WRR] 802.1P Priority Queue	0	1 0	2	3	4	5	6	7
Weight	3 w to height is 0 to 7	1	2	4	5	6	7	8
From Port 01 T	To Port 28	¥	Priority					Apply
.								A
Port 1 2 3		Priority 0 0 0			Effective Priori 0 0 0 0	цу		
Note: 1. For ingress un	tagged packets, the per gged packets, D-Link Sw	port "Default Prid	ority" settings will be a o their 802.1P inform	applied to packets ation for prioritizati	of each port to provid	e port-based traffic p	rioritization.	

Select QoS Mode: Select QoS mode from options "Port Base", "802.1P" and "DSCP" Queuing mechanism: Select options from "Strict Priority" and "WRR" From Port / To Port: Select the port that will port priority would applied Priority: Priority from 0-7

RMON > RMON Basic Settings

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

RMON Basic Settings		O Safeguard		
RMON Status: O Enabled	Disabled	Apply		
Figure 4.135 - RMON > RMON Basic Settings				

RMON > RMON Ethernet Statistics Configuration

The RMON Statistics Configuration page displays the information of RMON Ethernet Statistics and allows the user to configure the settings.

RMON Eth	ernet S	tatistics Confi	guration				O Safeguard
Index (1~65535	i)			*			
Port				*			
Owner							Apply
Index	Port	Drop Events	Octets	Packets	Broadcast Packets Multiast Packets	Owner	

Figure 4.136 - RMON > RMON Ethernet Statistics Configuration

The RMON Ethernet Statistics Configuration contains the following fields:

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

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

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

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

RMON > RMON History Control Configuration

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

RMON History Control Configuration		O Safeguard
Justice (4, 25525)		
Index (1~65535)		
Port		
Buckets Requested (1~50)	50	
Interval (1~3600 secs)	1800	
Owner		Apply
Index Port Buckets Requested	Buckets Granted Interval Owner	

Figure 4.137 - RMON > RMON History Control Configuration

The History Control Configuration contains the following fields:

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

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

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

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

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

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

RMON > RMON Alarm Configuration

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

RMON Alarm Configuration			O Safeguard
Index (1~65535)	*	Interval (1~2^31-1 secs)	300*
Variable Rising Threshold (0~2^31-1)	*	Sample type Falling Threshold (0~2^31-1)	Absolute value 🔻
Rising Event Index (1~65535)	*	Falling Event Index (1~65535)	*
Owner			Apply
Index Interval Variable	Sample Type F	Rising Threshold Falling Threshold Rising Event Index	Falling Event Owner Index

Figure 4.138 - RMON > RMON Alarm Settings

The configuration contains the following fields:

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

Variable: Specify the selected MIB variable value.

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

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

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

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

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

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

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

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

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

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

RMON > RMON Event Configuration

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

RIVION Event Configuration					U sareguaro
Index (1~65535)	*				
Description	*				
Туре	None T				
Community					
Owner					Apply
Index Description	Туре	Community	Owner	Last Time Sent	

Figure 4.139 - RMON > RMON Event Configuration

The RMON Events Page contains the following fields:

Index (1~ 65535): Displays the event.

Description: Specifies the user-defined event description.

Type: Specifies the event type. The possible values are:

None – Indicates that no event occurred.

Log - Indicates that the event is a log entry.

SNMP Trap – Indicates that the event is a trap.

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

Community: Specifies the community to which the event belongs.

Owner: Specifies the time that the event occurred.

Click **Apply** to add a new RMON event.

Security > Trusted Host

Use Trusted Host function to manage the switch from a remote station. User can specify up to ten designated management stations networks by defining the IP address/Subnet Mask as seen in the figure below.

Trusted Host			O Safeguard
Trusted Host: O Enabled	Disabled		Apply
Trusted Host Settings			
(Maximum Entries : 10)			
ID	IP Address	IP Mask	Delete
			Add Host
			Add Host
Note: Create a list of IP Addres	ses that can access the switch. Your local host IP A	ddresses must be one of the IP Addresses to avoid disco	nnection.
	Figure 4.140 - Sec	curity > Trusted Host	

To define a management station IP setting, click the **Add Host** button and type in the IP address and Subnet mask. Click the **Apply** button to save the settings. User may permit only single or a range of IP addresses by different IP mask settings, the format can either be 192.168.1.1/255.255.255.0 or 192.168.0.1/24. Please see the example below for permitting the IP range

IP Address	Subnet Mask	Permitted IP
192.168.0.1	255.255.255.0	192.168.0.1~192.168.0.255
172.17.5.215	255.0.0.0	172.0.0.1~172.255.255.255

To delete the IP address, simply click the **Delete** button. Check the unwanted address, and then click **Apply**.

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 protect the Switch from being interrupted by malicious viruses or worm attacks. This option is enabled by default.

Safeguard Engine	O Safeguard
Safeguard Engine: 💿 Enabled 🔷 Disabled	Apply
D-Link <u>Safequard Engine</u> is a robust and innovative technology developed by D-Link, which will automatically throttle the impact of packet flooding in It will keep D-Link Switches better protected from being too frequently interrupted by malicious viruses or worm attacks.	to the switch's CPU.

Figure 4.141 – Security > Safeguard Engine

Security > Port Security

Port Security is a security feature that prevents unauthorized computers (with source MAC addresses) unknown to the Switch prior to stopping auto-learning processing from gaining access to the network.

A given ports' (or a range of ports') dynamic MAC address learning can be stopped such that the current source MAC addresses entered into the MAC address forwarding table cannot be changed once the port is enabled.

Port Security	,				O Safeguard
From Port	To Port 28 ▼	Admin State Disabled	Max Learning Address (0-64) 0	Lock Address Mode Delete on Timeout 💌	Apply
Port Security					
Port	Admin State	Max Lea	arning Address	Lock Address Mode	
01	Disabled	0		Delete on Timeout	
02	Disabled	0		Delete on Timeout	
03	Disabled	0		Delete on Timeout	
04	Disabled	0		Delete on Timeout	
05	Disabled	0		Delete on Timeout	
06	Disabled	0		Delete on Timeout	
07	Disabled	0		Delete on Timeout	
08	Disabled	0		Delete on Timeout	
09	Disabled	0		Delete on Timeout	
10	Disabled	0		Delete on Timeout	

Figure 4.144 - Security > Port Security

The Port Security page contains the following fields:

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

Admin State: This pull-down menu allows users to enable or disable Port Security (locked MAC address table for the selected ports).

Max. Learning Address (0-64): The number of MAC addresses that will be in the MAC address-forwarding table for the selected switch and group of ports.

Lock Address Mode: This pull-down menu allows user to select how the MAC address table locking will be implemented on the Switch, for the selected group of ports. The options are:

Delete On Reset – The locked addresses will not age out until the Switch has been reset.

Delete On Timeout – The locked addresses will age out after the aging timer expires.

Permanent – The locked addresses will not age out after the aging timer expires.

Click Apply to make configurations make effects.

Security > Port Security FDB Entry

The page displays the MAC entries that trigger port security reaction.

Port Security FDB Entry				O Safeguar
Clear Locked Entries From Port To Port 01				Clear
VID VLAN Name	MAC Address	Port	Туре	Delete
1 default	E8-6A-64-96-83-E4	1	DeleteOnReset	Delete

By click **Delete**, the MAC entry will be released for Port Security FDB.

Security > 802.1X > 802.1X Settings

Network switches provide easy and open access to resources by simply attaching a client PC. Unfortunately this automatic configuration also allows unauthorized personnel to easily intrude and possibly gain access to sensitive data.

IEEE-802.1X provides a security standard for network access control, especially in Wi-Fi wireless networks. 802.1X holds a network port disconnected until authentication is completed. The switch uses Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol client identity (such as a user name) with the client, and forward it to another remote RADIUS authentication server to verify access rights. The EAP packet from the RADIUS server also contains the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. Depending on the authenticated results, the port is either made available to the user, or the user is denied access to the network.

The RADIUS servers make the network a lot easier to manage for the administrator by gathering and storing the user lists.

802	.1X Se	ttings											0	Safeguar
802.	1X		0 E	Inabled	Disable	d								
Auth	enticatior	Mode	Por	t Based	•			Authenti	cation Prof	tocol		Local	¥	
802.	1X Port A	ccess C	ontrol											
From	n Port			1		•		To Port				28 🔻		
Quie	tPeriod ()-65535)				50 sec		SuppTim	eout (1-65:	535)		30 sec		
Serv	erTimeou	rt (1-6553	35)			30 sec		MaxReq (2 tir	nes
TxPeriod (1-65535) 30 sec							ReAuthPe	eriod (1-65	535)			3600 se	9C	
ReA	uthenticat	tion		Disabled		•		Port Cont	rol			ForceAut	horized 🔻	
Cap	ability			None		•		Direction				Both	•	
													Refresh	Apply
Port	AdmDir	Open CrlDir	Port Control	AL	uth Status	Tx - Period	Quiet Period	Supp - Timeout	Server - Timeout	Max- Req	ReAuth Period	ReAuth	Capabi	lity 🄶
1	Both	Both	Force Authorize	d A	Authorized	30	60	30	30	2	3600	Disable	Nor	e
2	Both	Both	Force Authorize	d A	Authorized	30	60	30	30	2	3600	Disable	Nor	e
3	Both	Both	Force Authorize	d A	Authorized	30	60	30	30	2	3600	Disable	Nor	e
4	Both	Both	Force Authorize	d A	Authorized	30	60	30	30	2	3600	Disable	Nor	e
- 5	Both	Both	Force Authorize	d A	Authorized	30	60	30	30	2	3600	Disable	Nor	e

Figure 4.151 - Security > 802.1X > 802.1X Settings

By default, 802.1X is disabled. To use EAP for security, select enabled and set the **Authentication Mode** and **Authentication Protocol** then click **Apply**.

Authentication Mode: Indicates the 802.1X mode enabled on the device. The possible field values are:

Port Based – Enables 802.1X on ports. This is the default value.

MAC Based – Enables 802.1X on MAC addresses.

Authentication Protocol: Indicates the 802.1X Protocol on the device. The possible field values are *Local* and *RADIUS EAP*.

From Port/To Port: Enter the port or ports to be set.

QuietPeriod (0 – 65535 sec): Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. Default is *60* seconds.

ServerTimeout (1 – 65535 sec): Sets the amount of time the switch waits for a response from the client before resending the response to the authentication server. Default is *30* seconds.

TxPeriod (1 – 65535 sec): This sets the TxPeriod of time for the authenticator PAE state machine. This value determines the period of an EAP Request/Identity packet transmitted to the client. Default is *30* seconds.

ReAuthentication: Determines whether regular reauthentication will take place on this port. The default setting is *Disabled*.

Capability: Indicates the capability of the 802.1X. The possible field values are:

Authenticator – Specify the Authenticator settings to be applied on a per-port basis.

None – Disable 802.1X functions on the port.

SuppTimeout (1 – 65535 sec): This value determines timeout conditions in the exchanges between the Authenticator and the client. Default is *30* seconds.

MaxReq (1 – 10): This parameter specifies the maximum number of times that the switch retransmits an EAP request (md-5challnege) to the client before it times out the authentication session. Default is 2 times.

ReAuthPeriod (1 – 65535 sec): A constant that defines a nonzero number of seconds between periodic reauthentication of the client. The default setting is *3600* seconds.

Port Control: This allows user to control the port authorization state.

Select **ForceAuthorized** to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client.

If **ForceUnauthorized** is selected, the port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. The Switch cannot provide authentication services to the client through the interface.

If **Auto** is selected, it will enable 802.1X and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server.

The default setting is Auto.

Direction: Sets the administrative-controlled direction on the port. The possible field values are:

Both – Specify the control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field.

In – Disables the support in the present firmware release.

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

Security > 802.1X > 802.1X User

The **802.1X User** page allows user to set different local users on the Switch. Enter a **802.1X User** name, **Password** and **Confirm Password**. Properly configured local users will be displayed in the table.

802.1X User			O Safeguard
802.1X User Note: Password/User Name should be I	Password ess than 15 characters and more than 3 c	Confirm Password	Add
Total Entries: 0			
User Name	Password		

Figure 4.152 - Security > 802.1X > 802.1X User

Click Add to add a new 802.1X user.

Security > 802.1X > Radius Accounting Settings

The page allows user to turn of accounting state in 802.1x.

Radius Accounting	Settings	Safeguard
Accounting State	 Enabled Disabled 	Apply

Security > 802.1X > 802.1X Authentication RADIUS Server

The 802.1X Authentication RUAIUS of the Switch allows user to facilitate centralized user administration as well as providing protection against a sniffing, active hacker.

Authen	tication RADIUS Server	_	_	_	_	_	O Safeguard
Index		4	-				
Index			•				
IP Addres	c	10.48.47.11	IPv4				
II Addres	5				O IPv6		
Authentic	ation Port (1-65535)	100					
Accountin	ig Port (1-65535)	1000					
Timeout (1-255)	1	sec				
Retransm	it (1-255)	10	times				
Key							
Confirm K	(ey						
🥒 🥒 Note:	For key, the maximum number of o	character is 32.					
					Apply		
RADIUS	Server List						
Index	IP Address	Auth-Port	Acct-Port	Timeout	Retransmit	Key	Delete
1	10.48.47.11	100	1000	1	10	*****	Delete
2							
3							

Figure 4.153 - Security > 802.1X > 802.1X Authentication RUDIUS

Index: Choose the desired RADIUS server to configure: 1, 2 or 3.

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

Authentication Port (1 - 65535): Set the RADIUS authentic server(s) UDP port. The default port is 1812. Accounting Port (1 - 65535): Set the RADIUS account server(s) UDP port. The default port is 1813.

Timeout (1 – 255 sec): This field will set the time the Switch will wait for a response of authentication from the user. The user may set a time between *1* and *255* seconds. The default setting is *5* seconds.

Retransmit (1 – 255 times): This command will configure the maximum number of times the Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the Switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet and web users will be disconnected from the Switch. The user may set the number of attempts from *1* to *255*. The default setting is *2*.

Key: Set the key the same as that of the RADIUS server.

Confirm Key: Confirm the shared key is the same as that of the RADIUS server.

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

Security > 802.1X > 802.1X Guest VLAN

The 802.1X Guest VLAN page allows user to set a Guest VLAN, and the user must first configure a normal VLAN which can be enabled here for Guest VLAN status.

Enter the pre-configured VLAN name to create as a Guest 802.1X VLAN and select the port or ports. Click **Apply** to implement the settings.

LAN Nan	ne											Ap	ply	Delete
ort	01	02	03	04	05	06	07	08	09	10	11	12	13	14
'ort	15	16	17	18	19	20	21	22	23	24	25	26	27	28

Figure 4.154 - Security > 802.1X > 802.1X Guest VLAN

Security > MAC Address Table > Static MAC

Allow user to create static MAC address entry into forwarding table. This feature usually used in the port connected to certain devices that are permanent used in network, for example: DHCP servers, syslog server, network gateway location, etc.

									Select	: All	Cle	ar	A	oply
Port	01	02	03	04	05	06	07	08	09	10	11	12	13	14
earning	~	~	~	V	~	~	×	~	~	~	~	~	~	~
Port	15	16	17	18	19	20	21	22	23	24	25	26	27	28
earning	~	~	~	~	~	~	 Image: A second s	~	~	~	~	~	~	~
ort 01	Address		C Addre	ss				ID 1		~				dd ete All

Figure 4.50 – L2 Functions > MAC Address Table > Static Mac Address

The **Static MAC Address Lists** table displays the static MAC addresses connected, as well as the VID. **Add Static MAC Address:** you need to select the assigned Port number. Enter both the Mac Address and VID, and then Click **Add**. Click **Delete** to remove one entry or click **Delete all** to clear the list. By disabling MAC Address Auto Learning capability and specifying the static MAC addresses, the network is protected from potential threats like hackers, because traffic from illegal MAC addresses will not be forwarded by the Switch.

Security > MAC Address Table > Dynamic Forwarding Table

For each port, this table displays the MAC address learned by the Switch. To add a MAC address to the Static Mac Address List, click the **Add** checkbox, and then click **Apply** associated with the identified address.

Dynamic	Forwarding Ta	ble			0	Safegua
	I ▼ Search	um:0/258		Select A	All Clear	Apply
ID	Port	MAC Address	VID	Туре	Add to Static MAC	
	5	3C-97-0E-E5-76-4D	4	Dynamic		

Figure 4.51 – L2 Functions > MAC Address Table > Dynamic Forwarding Table

Security > Access Authentication Control > Authentication Policy Settings

This feature will enable an administrator-defined authentication policy for users trying to access the Switch. When enabled, the device will check the Login Method List and choose a technique for user authentication upon login.

Authentication Policy Settings		O Safeguard
Authentication Policy Response Timeout (0-255) User Attempts (1-255)	Disabled V 30 sec 3 times	
		Apply

Figure 4.161 – Security > Access Authentication control > Authentication Policy Settings

Authentication Policy: Use the pull-down menu to enable or disable the Authentication Policy on the Switch. **Response Timeout (0 - 255):** This field will set the time the Switch will wait for a response of authentication from the user. The user may set a time between *0* and *255* seconds. The default setting is *30* seconds.

User attempts (1 - 255): This command will configure the maximum number of times the Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the Switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet and web users will be disconnected from the Switch. The user may set the number of attempts from *1* to *255*. The default setting is *3*.

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

Security > Access Authentication Control > Application Authentication Settings

The Application Authentication Settings page allows user to configure switch configuration applications (Console, Telnet, SSH, HTTP) for login at the user level and at the administration level (Enable Admin) utilizing a previously configured method list.

Application Auth	nentication Settings				O Safeguard
Application	Login Method List		Enable N	lethod List	
Console	default	•	default	•	
Telnet	default	•	default	•	
SSH	default	•	default	•	
НТТР	default	•	default	•	
					Apply

Figure 4.162 – Security > Access Authentication control > Application Authentication Settings

Application: Lists the configuration applications on the Switch. The user may configure the Login Method List and Enable Method List for authentication for Console, Telnet application, SSH and the WEB (HTTP) application.

Login Method List: Using the pull-down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user.

Enable Method List: Using the pull-down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user.

Click **Apply** to implement configuration changes.

Security > Access Authentication Control > Authentication Server Group

A server group is a technique used to group TACACS+ and RADIUS server hosts into user-defined categories for authentication using method lists. The user may define the type of server group by protocol or by previously defined server group. The Switch has three built-in Authentication Server Groups that cannot be removed but can be modified.

To add a user-defined group to the list, click the Add button in the Authentication Server Group page.

Authentication Server Group	O Safeguard
Authentication Server Group Table Add Settings Group Name (Max: 15 characters)	Add
Group List (Total Entries:2)	
Group Name tacacs+	it Delete
radius	
	Delete

Figure 4.163 – Security > Access Authentication control > Authentication Server Group

Simply enter a group name of no more than 15 alphanumeric characters to define the user group to add. After clicking **Apply**, the new user-defined group will be displayed in the **Server Group** table. Here, it can be configured as the user desires.

F

The Switch has two built-in Authentication Server Groups that cannot be removed but can be modified. To modify a particular group, click **Edit** button, which will then display the following window.

Authentication Server Gro	up		Safeguard
Authentication Server Group Edit			
Group Name	tacacs+ 🔻		
Protocol	TACACS+ •		
IP address	•		
Note: Before add, the server host nee	ed to be created first.	Add	Previous pag
Host List (Total Entrine:0)			
IP Address	Protocol		

Figure 4.164 – Security > Access Authentication control > Authentication Server Group-Edit

Select Group Name, Protocol and IP address then click Add to implement the changes.

NOTE: The user must configure Authentication
Server Hosts using the Authentication Server
Hosts page before adding hosts to the list.
Authentication Server Hosts must be configured
for their specific protocol on a remote centralized
server before this function can work properly.

NOTE: The two built in server groups can only have server hosts running the same TACACS daemon. The TACACS+ and RADIUS protocols are separate entities and are not compatible with

each other.

Security > Access Authentication Control > Authentication Server

This Authentication Server page will set user-defined Authentication Server Hosts for the TACACS+ and RADIUS security protocols on the Switch. When a user attempts to access the Switch with Authentication Policy enabled, the Switch will send authentication packets to a remote TACACS+ or RADIUS server host on a remote host. The TACACS+ or RADIUS server host will then verify or deny the request and return the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS+ and RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.

Authentication Server	Authen	tication	Server	
-----------------------	--------	----------	--------	--

Authentication Server						C	Safeguard
IP Address]	IPv4				
]	IPv6				
Protocol	TACACS+ •		Port (1-65535)		49		
Key (Max: 254 characters)]	Timeout (1-255)		5	sec	
Retransmit (1-255)		times					Apply
Host List (Total Entries: 0)							
IP Address	Protocol	Authentication Port		Timeout		Retransmi	t

Figure 4.165 – Security > Access Authentication control > Authentication Server

To add an Authentication Server Host:

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

Protocol: The protocol used by the server host. The user may choose one of the following:

TACACS+ – Enter this parameter if the server host utilizes the TACACS+ protocol.

RADIUS – Enter this parameter if the server host utilizes the RADIUS protocol.

Key: Authentication key to be shared with a configured TACACS+ or RADIUS servers only. Specify an alphanumeric string up to 254 characters.

Port (1 - 65535): Enter a number between 1 and 65535 to define the virtual port number of the authentication protocol on a server host. The default port number is 49 for TACACS+ server and 1813 for RADIUS servers but the user may set a unique port number for higher security.

Timeout (1 - 255): Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is 5 seconds.

Retransmit (1 - 255): Enter the value in the retransmit field to change how many times the device will resend an authentication request when the TACACS server does not respond.

Click Apply to add a new Authentication Server Host.



NOTE: More than one authentication protocol can be run on the same physical server host.

Security > Access Authentication Control > Login Method Lists

This feature will configure a user-defined or default Login Method List of authentication techniques for users logging on to the Switch. Successful login using any of these techniques will give the user a "User" privilege only. To upgrade his or her status to the administrator level, the user must use the Enable Admin window, in which the user must enter a previously configured password, set by the administrator.

The Switch contains one Method List that is set and cannot be removed, yet can be modified. To delete a Login Method List defined by the user, click **Delete** button. To modify the Login Method List, click **Edit** button.

Login Method Lis	sts				O Safeguard
Method List Name (Ma:	x 15 characters)				
Priority 1:	none	T	Priority 2:	none 🔻	
Priority 3:	none	•	Priority 4:	none 🔻	
					Apply
Total Entries: 1					
Method List Name	Priority 1	Priority 2	Priority 3	Priority 4	
default	local				Edit Delete

Figure 4.166 – Security > Access Authentication control > Login Method Lists

To define a Login Method List, set the following parameters and click **Apply**:

Method List Name: Enter a method list name defined by the user of up to 15 characters.

Priority 1, 2, 3, 4: The user may add one, or a combination of up to four of the following authentication methods to this method list:

none - Adding this parameter will require an authentication to access the Switch.

local – Adding this parameter will require the user to be authenticated using the local user account database on the Switch.

tacacs+ – Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server.

radius – Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server.

Security > Access Authentication Control > Enable Method Lists

The Enable Method Lists page is used to set up Method Lists to promote users with user level privileges to Administrator (Admin) level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight Enable Method Lists can be implemented on the Switch, one of which is a default Enable Method List. This default Enable Method List cannot be deleted but can be configured.

To delete an Enable Method List defined by the use, click Delete button to the entry desired to be deleted. To modify and Enable Method List, click **Edit** button to make the changes and click **Apply**.

Enable Method Li	sts				C	Safeguard
Method List Name (Max:	15 characters)					
Priority 1:	none 🔻		Priority 2:	none 💌		
Priority 3:	none 🔻		Priority 4:	none 🔻		
						Apply
Total Entries: 1						
Method List Name	Priority 1	Priority 2	Priority 3	Priority 4		
default					Edit	Delete

Figure 4.167 – Security > Access Authentication control > Enable Method Lists

To define an Enable Login Method List, set the following parameter and click Apply:

Method List Name: Enter a method list name defined by the user of up to 15 characters.

Priority 1, 2, 3, 4: The user may add one, or a combination of up to four of the following authentication methods to this method list:

none - Adding this parameter will require an authentication to access the Switch.

local – Adding this parameter will require the user to be authenticated using the local user account database on the Switch.

tacacs+ – Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server.

radius – Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server.

Security > Access Authentication Control > Local Enable Password Settings

The Local Enable Password Settings page allows user to configure the locally enabled password. When a user chooses the "local_enable" method to promote user level privileges to administrator privileges, he or she will be prompted to enter the password configured here that is locally set on the Switch.

Local Enable Password Settings	0	Safeguard
Old Local Enable Password (Max: 15 characters) New Local Enable Password Confirm Local Enable Password		
	(Apply
Figure 4 169 - Security > Access	Authoritication control > Local Enable Deseword Set	tinge

Figure 4.168 – Security > Access Authentication control > Local Enable Password Settings

To set the Local Enable Password, set the following parameters and click **Apply**:

Old Local Enable Password: If a password was previously configured for this entry, enter it here in order to change it to a new password.

New Local Enable Password: Enter the new password that user specified for the Switch to authenticate users attempting to access Administrator Level privileges on the Switch. The user may set a password of up to 15 characters.

Confirm Local Enable Password: Confirm the new password entered above. Entering a different password here from the one set in the New Local Enabled field will result in a fail message.

Security > Traffic Segmentation

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.

	entation												
up Forwarding) ports												
t 1	•								Selec	t All	Clear		Apply
tMap 1	2	3	4	5	6	7	8	9	10	11	12	13	14
	Image: A start and a start	e		e		e	e	e					✓
15	16	17	18	19	20	21	22	23	24	25	26	27	28
v	v	v				~		V	Image: A start and a start				
. C	•	٢	٢						•				•
				·		v		ort Map	V	•	V		٣
t Map list						•					V	¥	•
rt Map list	rt					•		ort Map		•	•		•
r t Map list Po 1	rt					•		ort Map 1-28				<u>v</u>	
rt Map list Po 1 2	rt			•				ort Map 1-28 1-28		•		V	
rt Map list Po 1 2 3	rt			•		•		ort Map 1-28 1-28 1-28 1-28		•	•	<u>v</u>	

Figure 4.169 – Security > Traffic Segmentation

To configure traffic segmentation specify a port or All ports from the switch, using the **Port** pull-down menu and select **Port Map** then click **Apply** to enter the settings into the Switch's **Traffic Segmentation** table. Click **Select All** to select all port maps or click **Clear** button to uncheck port maps.

Security > DoS Prevention Settings

The DoS is a malicious attack against a network. This attack is designed to stop a network from functioning by flooding it with useless traffic. Symptoms of a malicious attack include the inability to access any web site or a particular web site being unavailable and network performance slowing down.

DoS Prevention Setting	IS			O Safegua
Dos Prevention Trap Log State	O Enable	ed		Apply
Prevention Settings				
Type 🗌 Land Attack	Blat Attack	TCP Tiny Frag Attack	TCP Null Scan	
TCP Xmascan	TCP SYNFIN	TCP SYN SrcPort less 1024	Ping Death Attack	
_		TCP STN SICPOILless 1024	Ping Death Attack	
All				
State Enabled 🗸				Apply
DoS Attack Prevention List				
Dos Type		State	Action	
and Attack		Disabled	Drop	
Blat Attack		Disabled	Drop	
Top Null Scan		Disabled	Drop	
Tcp Xmascan		Disabled	Drop	
Tcp Synfin		Disabled	Drop	
Fcp Syn Srcport less 1024		Disabled	Drop	
Ping Death Attack		Disabled	Drop	
Ccp Tiny Fragment		Disabled	Drop	

Figure 4.170 – Security > DoS Prevention Settings

Prevention Settings:

Type: Select the attack types to be prevented. The types are *Land Attack, TCP Tine Frag Attack, TCP Null Scan, TCP Xmascan, TCP SYNFIN, TCP SYN SrcPortless 1024, Ping Death Attack* or *All.* **State:** Specify the state to be enabled or disabled.

Click Apply to make the configurations take effect

Security > Smart Binding > Smart Binding Settings

The primary purpose of Smart Binding is to restrict client access to a switch by enabling administrators to configure pairs of client MAC and IP addresses that are allowed to access networks through a switch.

The Smart Binding function is port-based, meaning that a user can enable or disable the function on any individual port. Once Smart Binding is enabled on a switch port, the switch will restrict or allow client access by checking the pair of IP-MAC addresses with the pre-configured database, also known as the "IMPB white list".

Users can enable or disable the **Packet Inspection** and **DHCP Snooping** on the Switch.

mar	rt Binding	Settings		_		_				Safeguar
From I	Port	1	o Port		Admin State		ARP Inspecti	on	IP Inspection	
C	01 •		28	•	Disabled	•	Disabled	T	Disabled	•
Allow :	Zero IP	F	orward DHCP P	acket	DHCP Snoopin	g	Max Entry		Max Entry (IPv8	5)
Disat	bled 🔹	-	Enabled	•	Disabled	•	No Limit	T	No Limit	•
онср	9v4 Vlan List		DHCPv6 Vlan Lis	t						
										Apply
MPB 9	Setting									
MPB 9	Setting Admin State	ARP Inspection	IP Inspection	Allow Zero IP	Forward DHCP Packet	DHCP Snooping	Max Entry	Max Entry (IPv6)	DHCPv4 Vlan List	DHCPv6 Vlan ⊿ List
	-		IP Inspection Disabled	Allow Zero IP Disabled			Max Entry No Limit	Max Entry (IPv6) No Limit		
Port 1	Admin State	Inspection			Packet	Snooping				
Port 1 2	Admin State Disabled	Inspection Disabled	Disabled	Disabled	Packet Enabled	Snooping Disabled	No Limit	No Limit		
'ort 1 2	Admin State Disabled Disabled	Inspection Disabled Disabled	Disabled Disabled	Disabled Disabled	Packet Enabled Enabled	Snooping Disabled Disabled	No Limit No Limit	No Limit No Limit		
ort 1 2 3	Admin State Disabled Disabled Disabled	Inspection Disabled Disabled Disabled	Disabled Disabled Disabled	Disabled Disabled Disabled	Packet Enabled Enabled Enabled	Snooping Disabled Disabled Disabled	No Limit No Limit No Limit	No Limit No Limit No Limit		
ort 2 3 4 5	Admin State Disabled Disabled Disabled Disabled	Inspection Disabled Disabled Disabled Disabled	Disabled Disabled Disabled Disabled	Disabled Disabled Disabled Disabled	Packet Enabled Enabled Enabled Enabled	Snooping Disabled Disabled Disabled Disabled	No Limit No Limit No Limit No Limit	No Limit No Limit No Limit No Limit		
Port 1 2 3 4 5	Admin State Disabled Disabled Disabled Disabled Disabled	Inspection Disabled Disabled Disabled Disabled Disabled	Disabled Disabled Disabled Disabled Disabled Disabled	Disabled Disabled Disabled Disabled Disabled	Packet Enabled Enabled Enabled Enabled Enabled	Snooping Disabled Disabled Disabled Disabled Disabled	No Limit No Limit No Limit No Limit No Limit	No Limit No Limit No Limit No Limit No Limit No Limit		
	Admin State Disabled Disabled Disabled Disabled Disabled Disabled	Inspection Disabled Disabled Disabled Disabled Disabled Disabled	Disabled Disabled Disabled Disabled Disabled Disabled	Disabled Disabled Disabled Disabled Disabled Disabled	Packet Enabled Enabled Enabled Enabled Enabled Enabled	Snooping Disabled Disabled Disabled Disabled Disabled Disabled	No Limit No Limit No Limit No Limit No Limit No Limit	No Limit No Limit No Limit No Limit No Limit No Limit		

Figure 4.146 – Security > Smart Binding > Smart Binding Settings

The Smart Binding Settings page contains the following fields:

From Port/ To Port: Select a range of ports to set for IP-MAC-port binding.

Admin State: Use the drop-down menu to enable or disable these ports for Smart Binding.

Enabled – Enable Smart Binding with related configurations to the ports

Disabled –Disable Smart Binding.

ARP Inspection: If ARP inspection is enabled, the Switch will inspect incoming ARP packets and compare them with the Switch's Smart Binding white list entries. If the IP-MAC pair of an ARP packet is not found in the white list, the Switch will block the MAC address. A major benefit of Loose state is that it uses less CPU resources. However, it cannot block malicious users who send only unicast IP packets. An example of this is that a malicious user can perform DoS attacks by statically configuring the ARP table on their PC. In this case, the Switch cannot block such attacks because the PC will not send out ARP packets.

IP Inspection: When IP Inspection is enabled, and ARP Inspection is disabled, all non-IP packets are forwarded by default. If **ARP Inspection** and **IP Inspection** mode are enabled, the Switch will inspect all incoming ARP and IP packets and compare them to the IMPB white list. If the IP-MAC pair find a match in the white list, the packets from that MAC address are unblocked. If not, the MAC address will stay blocked. While the mode examines every ingress ARP and IP packet, it enforces better security.

Allow Zero IP: Enable or disable to allow zero IP to configure the state which allows ARP packets with 0.0.0.0 source IP to bypass.

Forward DHCP Packet: Enable or disable to forward DHCP packet.

DHCP Snooping: By enable DHCP Snooping, the switch will snoop the packets sent from DHCP Server and clients, and update information to the White List.

Max Entry: Specifies the max entries of Smart Binding. The range is between 1 and 10, or No Limit.

Max Entry (IPv6): Specifies the IPv6 max entries of Smart Binding. The range is between 1 and 10, or No Limit.

Click **Apply** to make configurations make effects.

Security > Smart Binding > Smart Binding

The Smart Binding page allows the user to create Static IP-MAC-Port Binding entries on the Switch.

Smart Binding	O Safeguard
Manual Binding From Port To Port IP Address MAC Address 01 01	Add
Auto Scan Enter a range of IP address to scan all devices in the network. IP Address From To	Scan
Select All Clear All VLAN IP Address Port	Apply Binding

Figure 4.147 – Security > Smart Binding > Smart Binding

The Manual Binding Settings contains the following fields:

From Port / To Port: Specifies the port ranges for MAC address to bind to the IP address of Binding list. **IP Address:** Specifies the IP address to bind to the MAC address set below.

MAC Address: Specifies the MAC address to bind to the IP address set above.

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

Auto Scan: Specifies to scan connected devices in a range of IP address. **IP Address From/To:** Specifies the range of IP Address to scan all devices in the network.

Click **Scan** and the search results will be listed in below table. **Binding:** check the box to select desired binding devices. **Apply:** click **Apply** to set IP-MAC-Port Binding entries." **Select All:** to check the boxes of Binding for all found devices.

Clear All: to cancel the box of Binding.

Security > Smart Binding > White List

When IP+ARP Inspection Mode were selected, the White List page displays finished IP-MAC-Port Binding entries from page Smart Binding. Only IP packets or ARP packets carrying matched IP-MAC-Port information can access to the switch. User can cancel a device's authorization by deleting it from the table.

White List				O Saf	eguard
		Delete	Select All		lean
Total Entries: 0		Delete	Select All		lean
IP Address		MAC Address		Port	Delete
	=:				

Figure 4.148 – Security > Smart Binding > White List

Click **Select All** to select all entries of the table or click **Clean** to select none entries. Please keep at least one management host in the White List.

Security > Smart Binding > Black List

The Black List page shows unauthorized accesses. When ARP Inspection is selected and a device sends out an ARP packet containing unmatched IP-MAC-Port information, the device will be forbidden and listed here.

Black List				O Safeguard
	IP Address	MAC Address	Port	Find
			Delete	Select All Clean
Total Entries: 0				
VID IP Addre	ess		MAC Address	Port Delete

Figure 4.149 – Security > Smart Binding > Black List

By giving conditions, desired devices information can be screened out below then click **Find** to search for a list of the entry:

VID: Enter the VLAN ID number of the device.

IP Address: Enter the IP Address of the device.

MAC Address: Enter the MAC Address of the device.

Port: Enter the port number which the device connects.

Check a box of **Delete** column to release an entry from the forbidden list then click **Apply** to delete an entry from the list.

Click **Select All** to select all entries, or click **Clean** to select none of the entries.

Security > Smart Binding > DHCP Snooping List

The DHCP Snooping List page shows the DHCP Snooping list.

DHCP Snooping List					O Safegu	land
Total Entries: 0						
IP Address	MAC Address	Port	Lease Time	Remaining Time	Status	

Figure 4.150 – Security > Smart Binding > DHCP Snooping List

Security > Smart Binding > Smart Binding Settings

The primary purpose of Smart Binding is to restrict client access to a switch by enabling administrators to configure pairs of client MAC and IP addresses that are allowed to access networks through a switch.

The Smart Binding function is port-based, meaning that a user can enable or disable the function on any individual port. Once Smart Binding is enabled on a switch port, the switch will restrict or allow client access by checking the pair of IP-MAC addresses with the pre-configured database, also known as the "IMPB white list".

Users can enable or disable the **Packet Inspection** and **DHCP Snooping** on the Switch.

Sma	rt Binding S	Settings		_		_				Safeguar
From	Port	r	o Port		Admin State		ARP Inspecti	on	IP Inspection	
- 1	01 🔹	1	28	•	Disabled	•	Disabled	T	Disabled	•
Allow	Zero IP	F	orward DHCP P	acket	DHCP Snoopin	3	Max Entry		Max Entry (IPv8	6)
Disa	bled 🔻	-	Enabled	•	Disabled	•	No Limit	•	No Limit	•
энсг	Pv4 Vlan List)HCPv6 Vlan Lis	t						Apply
MPB Port	Setting Admin State	ARP								
			IP Inspection	Allow Zero IP	Forward DHCP	DHCP	Max Entry	Max Entry (IPv6)	DHCPv4 Vlan	DHCPv6 Vian
	Disabled	Inspection			Packet	Snooping			DHCPv4 Vlan List	DHCPv6 Vlan List
1 2	Disabled Disabled	Inspection Disabled	Disabled	Disabled	Packet Enabled	Snooping Disabled	No Limit	No Limit		
	Disabled Disabled Disabled	Inspection			Packet	Snooping				
3	Disabled	Inspection Disabled Disabled	Disabled Disabled	Disabled Disabled	Packet Enabled Enabled	Snooping Disabled Disabled	No Limit No Limit	No Limit No Limit		
3 4	Disabled Disabled	Inspection Disabled Disabled Disabled	Disabled Disabled Disabled	Disabled Disabled Disabled	Packet Enabled Enabled Enabled	Snooping Disabled Disabled Disabled	No Limit No Limit No Limit	No Limit No Limit No Limit		
3 4 5	Disabled Disabled Disabled	Inspection Disabled Disabled Disabled Disabled	Disabled Disabled Disabled Disabled	Disabled Disabled Disabled Disabled	Packet Enabled Enabled Enabled Enabled	Snooping Disabled Disabled Disabled Disabled	No Limit No Limit No Limit No Limit	No Limit No Limit No Limit No Limit		
3 4 5	Disabled Disabled Disabled Disabled	Inspection Disabled Disabled Disabled Disabled Disabled	Disabled Disabled Disabled Disabled Disabled	Disabled Disabled Disabled Disabled Disabled	Packet Enabled Enabled Enabled Enabled Enabled	Snooping Disabled Disabled Disabled Disabled Disabled	No Limit No Limit No Limit No Limit No Limit	No Limit No Limit No Limit No Limit No Limit No Limit		
1 2 3 4 5 6 7 8	Disabled Disabled Disabled Disabled Disabled	Inspection Disabled Disabled Disabled Disabled Disabled Disabled	Disabled Disabled Disabled Disabled Disabled Disabled	Disabled Disabled Disabled Disabled Disabled Disabled	Packet Enabled Enabled Enabled Enabled Enabled Enabled	Snooping Disabled Disabled Disabled Disabled Disabled Disabled	No Limit No Limit No Limit No Limit No Limit No Limit	No Limit No Limit No Limit No Limit No Limit No Limit		

Figure 4.146 – Security > Smart Binding > Smart Binding Settings

The Smart Binding Settings page contains the following fields:

From Port/ To Port: Select a range of ports to set for IP-MAC-port binding.

Admin State: Use the drop-down menu to enable or disable these ports for Smart Binding.

Enabled – Enable Smart Binding with related configurations to the ports

Disabled – Disable Smart Binding.

ARP Inspection: If ARP inspection is enabled, the Switch will inspect incoming ARP packets and compare them with the Switch's Smart Binding white list entries. If the IP-MAC pair of an ARP packet is not found in the white list, the Switch will block the MAC address. A major benefit of Loose state is that it uses less CPU resources. However, it cannot block malicious users who send only unicast IP packets. An example of this is that a malicious user can perform DoS attacks by statically configuring the ARP table on their PC. In this case, the Switch cannot block such attacks because the PC will not send out ARP packets.

IP Inspection: When IP Inspection is enabled, and ARP Inspection is disabled, all non-IP packets are forwarded by default. If **ARP Inspection** and **IP Inspection** mode are enabled, the Switch will inspect all incoming ARP and IP packets and compare them to the IMPB white list. If the IP-MAC pair find a match in the white list, the packets from that MAC address are unblocked. If not, the MAC address will stay blocked. While the mode examines every ingress ARP and IP packet, it enforces better security.

Allow Zero IP: Enable or disable to allow zero IP to configure the state which allows ARP packets with 0.0.0.0 source IP to bypass.

Forward DHCP Packet: Enable or disable to forward DHCP packet.

DHCP Snooping: By enable DHCP Snooping, the switch will snoop the packets sent from DHCP Server and clients, and update information to the White List.

Max Entry: Specifies the max entries of Smart Binding. The range is between 1 and 10, or No Limit.

Max Entry (IPv6): Specifies the IPv6 max entries of Smart Binding. The range is between 1 and 10, or No Limit.

Click **Apply** to make configurations make effects.

Security > Smart Binding > Smart Binding

The Smart Binding page allows the user to create Static IP-MAC-Port Binding entries on the Switch.

Smart Binding	O Safeguard
Manual Binding From Port To Port IP Address MAC Address 01 01 IP IP IP Auto Scan Inter a range of IP address to scan all devices in the network. IP Address IP Address	Add
IP Address From To	Scan
Select All Clear All VLAN IP Address Port	Apply Binding

Figure 4.147 – Security > Smart Binding > Smart Binding

The Manual Binding Settings contains the following fields:

From Port / To Port: Specifies the port ranges for MAC address to bind to the IP address of Binding list.

IP Address: Specifies the IP address to bind to the MAC address set below.

MAC Address: Specifies the MAC address to bind to the IP address set above.

Click Add to add a new entry.

Auto Scan: Specifies to scan connected devices in a range of IP address.

IP Address From/To: Specifies the range of IP Address to scan all devices in the network.

Click Scan and the search results will be listed in below table.

Binding: check the box to select desired binding devices.

Apply: click Apply to set IP-MAC-Port Binding entries."

Select All: to check the boxes of Binding for all found devices.

Clear All: to cancel the box of Binding.

Security > Smart Binding > White List

When IP+ARP Inspection Mode were selected, the White List page displays finished IP-MAC-Port Binding entries from page Smart Binding. Only IP packets or ARP packets carrying matched IP-MAC-Port information can access to the switch. User can cancel a device's authorization by deleting it from the table.

0) Saf	eguard
Select All	Cl	lean
_	Port	Delete
	_	Port

Figure 4.148 – Security > Smart Binding > White List

Click **Select All** to select all entries of the table or click **Clean** to select none entries. Please keep at least one management host in the White List.

Security > Smart Binding > Black List

The Black List page shows unauthorized accesses. When ARP Inspection is selected and a device sends out an ARP packet containing unmatched IP-MAC-Port information, the device will be forbidden and listed here.

Black List				O Safeguard
	IP Address	MAC Address	Port	Find
·			Delete Select	: All Clean
Total Entries: 0				
VID IP Address	_		MAC Address	Port Delete

Figure 4.149 – Security > Smart Binding > Black List

By giving conditions, desired devices information can be screened out below then click **Find** to search for a list of the entry:

VID: Enter the VLAN ID number of the device.

IP Address: Enter the IP Address of the device.

MAC Address: Enter the MAC Address of the device.

Port: Enter the port number which the device connects.

Check a box of **Delete** column to release an entry from the forbidden list then click **Apply** to delete an entry from the list.

Click Select All to select all entries, or click Clean to select none of the entries.

Security > Smart Binding > DHCP Snooping List

The DHCP Snooping List page shows the DHCP Snooping list.

			O Safeguard
Address Port	Lease Time	Remaining Time	Status
	Address Port	Address Port Lease Time	Address Port Lease Time Remaining Time

Figure 4.150 – Security > Smart Binding > DHCP Snooping List

Monitoring > Statistics

The Statistics screen displays the status of each port packet count.

tistics				0 Safegu
				Refresh All Clear All Cour
Port	TxOK	RxOK	TxError	RxError
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
Z	0	0	0	0
8	0	0	0	0
9	0	0	0	0
<u>10</u>	0	0	0	0
11	69434	43107	0	0
12	0	0	0	0
13	0	0	0	0

Figure 4.182 – Monitoring > Statistics

Refresh All: Renews the details collected and displayed.

Clear All: To reset the details displayed.

TxOK: Number of packets transmitted successfully.

RxOK: Number of packets received successfully.

TxError: Number of transmitted packets resulting in error.

RxError: Number of received packets resulting in error.

To view the statistics of individual ports, click one of the linked port numbers for details.

ort Statistics				O Safeguard
		F	Previous Pac Refres	h Clear Counte
тх		RX		
OutOctets	53797423	InOctets	4327100	
OutUcastPkts	70485	InUcastPkts	43966	
OutNUcastPkts	571	InNUcastPkts	152	
OutErrors	0	InDiscards	0	
LateCollisions	0	InErrors	0	
ExcessiveCollisions	0	FCSErrors	0	
InternalMacTransmitErrors	0	FrameTooLongs	0	
		InternalMacReceiveErrors	з О	

Figure 4.183 – Monitoring > Port Statistics

Previous Page: Go back to the Statistics main page.

Refresh: To renew the details collected and displayed.

Clear Counter: To reset the details displayed.

Monitoring > Session Table

The Session Table allows the user to view detailed information on the current configuration session of the Switch. Information such as the Session ID of the user, initial Login Time, Live Time, configuration connection From the Switch, Level and Name of the user are displayed. Click Reload to refresh this window.

Session Table				O Safeguard
Reload				
Total Entries : 0				
ID Login Time	Live Time	From	Level	Name

Figure 4.184 – Monitoring > Session Table

Monitoring > CPU Utilization

The **CPU Utilization** displays the percentage of the CPU being used, expressed as an integer percentage and calculated as a simple average by time interval. The window will automatically refresh with new updated statistics.

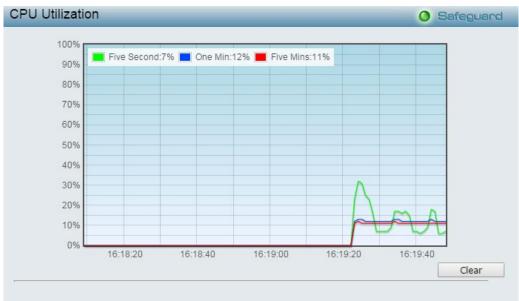


Figure 4.185 – Monitoring > CPU Utilization

Clear: Clicking this button clears all statistics counters on this window.

Monitoring > Memory Utilization

The Memory Utilization displays the percentage of the memory being used, expressed as an integer percentage and calculated as a simple average by time interval. Click **Apply** to implement the configured settings. The window will automatically refresh with new updated statistics.



Figure 4.186 – Monitoring > Memory Utilization

The information is described as follows:

Time Interval: Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is *one* second.

Record Number: Select number of times the Switch will be polled between 20 and 200. The default value is 200.

Show/Hide: Check whether to display Five Secs, One Min, and/or Five Mins.

Clear: Clicking this button clears all statistics counters on this window.

Monitoring > Port Utilization

The Port Utilization page displays the percentage of the total available bandwidth being used on the port.



Figure 4.187 – Monitoring > Port Utilization

The user may use the real-time graphic of the Switch at the top of the web page to view utilization statistics per port by clicking on a port. Click Apply to make the configurations take effect. The following field can be set:

Time Interval: Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is *one* second.

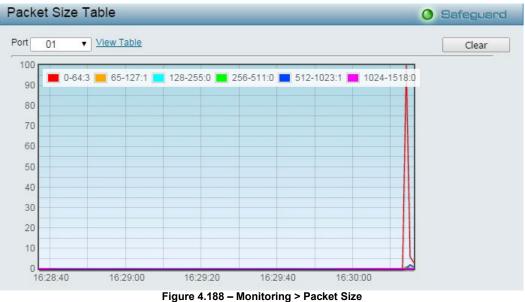
Record Number: Select number of times the Switch will be polled between 20 and 200. The default value is 200.

Show/Hide: Check whether to display Utilization.

Clear: Clicking this button clears all statistics counters on this window.

Monitoring > Packet Size

The Web Manager allows packets received by the Switch, arranged in six groups and classed by size, to be viewed as either a line graph or a table. Two windows are offered. To select a port to view these statistics for, select the port by using the **Port** pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.



To view the **Packet Size Analysis Table**, click the link <u>View Table</u>, which will show the following table:

/iew LineChart		0 Safeguari
64	Frames	Frame/Sec
64	13083	190
65-127	2099	10
128-255	9	0
256-511	292	2
512-1023	503	7
1024-1518	0	0

Figure 4.189 – Monitoring > Packet Size Table

The following fields can be set or viewed:

Time Interval: Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is *one* second.

Record Number: Select number of times the Switch will be polled between 20 and 200. The default value is 200.

64: The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).

65-127: The total number of packets (including bad packets) received that were between *65* and *127* octets in length inclusive (excluding framing bits but including FCS octets).

128-255: The total number of packets (including bad packets) received that were between *128* and *255* octets in length inclusive (excluding framing bits but including FCS octets).

256-511: The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

512-1023: The total number of packets (including bad packets) received that were between *512* and *1023* octets in length inclusive (excluding framing bits but including FCS octets).

1024-1518: The total number of packets (including bad packets) received that were between *1024* and *1518* octets in length inclusive (excluding framing bits but including FCS octets).

Show/Hide: Check whether or not to display *64*, *65-127*, *128-255*, *256-511*, *512-1023*, and *1024-1518* packets received.

Clear: Clicking this button clears all statistics counters on this window.

View Table: Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart: Clicking this button instructs the Switch to display a line graph rather than a table.

Monitoring > Packets > Transmitted (TX)

The Transmitted (TX) page displays the following graph of packets transmitted from the Switch. To select a port to view these statistics for, use the **Port** pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.



Figure 4.190 - Monitoring > Packets > Transmitted (TX) (line graph for Bytes and Packets)

To view the **Transmitted (TX) Table**, click the link <u>View Table</u>, which will show the following table:

Packet Analysis Ta	O Safeguard	
View LineChart		
Rx Packets	Total	Rate/sec
Bytes	1920369	7837
Packets	20995	84
Rx Packets	Total	Rate/sec
Bytes	19442	81
Packets	598	0
Packets	955	3
Rx Packets	Total	Rate/sec
Bytes	27747797	116464
Packets	33553	143

Figure 4.191 - Monitoring > Packet s > Transmitted (TX) (table for Bytes and Packets)

Time Interval: Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is *one* second.

Record Number: Select number of times the Switch will be polled between 20 and 200. The default value is 200.

Bytes: Counts the number of bytes successfully sent from the port.

Packets: Counts the number of packets successfully sent on the port.

Unicast: Counts the total number of good packets that were transmitted by a unicast address.

Multicast: Counts the total number of good packets that were transmitted by a multicast address.

Broadcast: Counts the total number of good packets that were transmitted by a broadcast address.

Show/Hide: Check whether or not to display Bytes and Packets.

Clear: Clicking this button clears all statistics counters on this window.

View Table: Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart: Clicking this button instructs the Switch to display a line graph rather than a table.

Monitoring > Packets > Received (RX)

The Received (RX) page displays the following graph of packets received on the Switch. To select a port to view these statistics for, use the **Port** pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.



Figure 4.192 - Monitoring > Packets > Received (RX) (line graph for Bytes and Packets)

To view the Received Packets Table, click the link View Table, which will show the following table:

Packet Analysis Ta	O Safeguard	
View LineChart		
Rx Packets	Total	Rate/sec
Bytes	2445927	33032
Packets	26304	391
Rx Packets	Total	Rate/sec
Bytes	24746	391
Packets	598	0
Packets	960	0
Rx Packets	Total	Rate/sec
Bytes	34850825	615653
Packets	42458	706

Figure 4.193 - Monitoring > Packet s > Received (RX) (table for Bytes and Packets)

Time Interval: Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is *one* second.

Record Number: Select number of times the Switch will be polled between 20 and 200. The default value is 200.

Bytes: Counts the number of bytes received on the port.

Packets: Counts the number of packets received on the port.

Unicast: Counts the total number of good packets that were received by a unicast address.

Multicast: Counts the total number of good packets that were received by a multicast address.

Broadcast: Counts the total number of good packets that were received by a broadcast address.

Show/Hide: Check whether or not to display Bytes and Packets.

Clear: Clicking this button clears all statistics counters on this window.

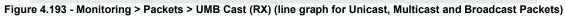
View Table: Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart: Clicking this button instructs the Switch to display a line graph rather than a table.

Monitoring > Packets > UMB Cast (RX)

The **UMB Cast (RX)** page displays the following graph of UMB cast packets received on the Switch. To select a port to view these statistics for, use the **Port** pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.





To view the **UMB Cast Table**, click the <u>View Table</u> link, which will show the following table:

Packet Analysis Ta	O Safeguard	
View LineChart		
Rx Packets	Total	Rate/sec
Bytes	2966821	2882
Packets	31419	15
Rx Packets	Total	Rate/sec
Bytes	29861	15
Packets	598	0
Packets	960	0
Rx Packets	Total	Rate/sec
Bytes	41491737	1315
Packets	50935	15

Figure 4.194 - Monitoring > Packets > UMB Cast (RX) (table for Unicast, Multicast and Broadcast Packets)

Time Interval: Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is *one* second.

Record Number: Select number of times the Switch will be polled between 20 and 200. The default value is 200.

Unicast: Counts the total number of good packets that were received by a unicast address.

Multicast: Counts the total number of good packets that were received by a multicast address.

Broadcast: Counts the total number of good packets that were received by a broadcast address.

Show/Hide: Check whether or not to display Multicast, Broadcast and Unicast packets.

Clear: Clicking this button clears all statistics counters on this window.

View Table: Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart: Clicking this button instructs the Switch to display a line graph rather than a table.

Monitoring > Errors > Received (RX)

This page displays the following graph of error packets received on the Switch. To select a port to view these statistics for, select the port by using the **Port** pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.

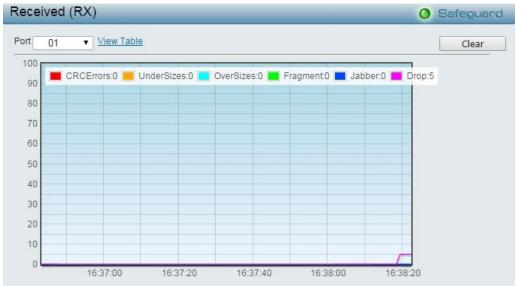


Figure 4.195 - Monitoring > Errors > Received (RX) (line graph)

To view the Received Error Packets Table, click the link View Table, which will show the following table:

X Error Packet Analysis Table		O Safeguaro
Tx Packets	Frames	
CRCError	0	
UnderSize	0	
OverSize	0	
Fragment	0	
Jabber	0	
Drop	40045	

Figure 4.196 - Monitoring > Errors > Received (RX) (table)

The following fields can be set or viewed:

Time Interval: Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is *one* second.

Record Number: Select number of times the Switch will be polled between 20 and 200. The default value is 200.

CRC Error: Counts otherwise valid packets that did not end on a byte (octet) boundary.

UnderSize: The number of packets detected that are less that the minimum permitted packets size of 64 bytes and have a good CRC. Undersize packets usually indicate collision fragments, a normal network occurrence.

OverSize: Counts packets received that were longer that *1518* octets, or if a VLAN frame is *1522* octets, and less that the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to *1522*.

Fragment: The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.

Jabber: The number of packets with lengths more than the MAX_PKT_LEN bytes. Internally, MAX_PKT_LEN is equal to *1522*.

Drop: The number of packets that are dropped by this port since the last Switch reboot.

Show/Hide: Check whether or not to display CRC Error, Under Size, Over Size, Fragment, Jabber, and Drop errors.

Clear: Clicking this button clears all statistics counters on this window.

View Table: Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart: Clicking this button instructs the Switch to display a line graph rather than a table.

Monitoring > Errors > Transmitted (TX)

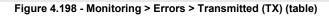
This page displays the following graph of error packets transmitted on the Switch. To select a port to view these statistics for, select the port by using the **Port** pull-down menu. The user may also use the real-time graphic of the Switch at the top of the web page by simply clicking on a port.



Figure 4.197 - Monitoring > Errors > Transmitted (TX) (line graph)

To view the **Transmitted Error Packets Table**, click the link <u>View Table</u>, which will show the following table:

IX Error Packet Analysis Table		0 Safeguari
/iew LineChart		
Tx Packets	Frames	
ExDefer	0	
CRCError	0	
LateColl	0	
ExColl	0	
SingColl	0	
Collision	0	



Time Interval: Select the desired setting between *1s* and *60s*, where "s" stands for seconds. The default value is *one* second.

Record Number: Select number of times the Switch will be polled between 20 and 200. The default value is 200.

ExDefet: Counts the number of packets for which the first transmission attempt on a particular interface was delayed because the medium was busy.

CRC Error: Counts otherwise valid packets that did not end on a byte (octet) boundary.

LateColl: Counts the number of times that a collision is detected later than *512* bit-times into the transmission of a packet.

ExColl: Excessive Collisions. The number of packets for which transmission failed due to excessive collisions.

SingColl: Single Collision Frames. The number of successfully transmitted packets for which transmission is inhibited by more than one collision.

Coll: An estimate of the total number of collisions on this network segment.

Show/Hide: Check whether or not to display ExDefer, LateColl, ExColl, SingColl, and Coll errors.

Clear: Clicking this button clears all statistics counters on this window.

View Table: Clicking this button instructs the Switch to display a table rather than a line graph.

View Line Chart: Clicking this button instructs the Switch to display a line graph rather than a table.

Monitoring > Cable Diagnostics

The Cable Diagnostics is designed primarily for administrators and customer service representatives to examine of the copper cable quality. It rapidly determines the type of cable errors occurred in the cable.

Select a port and then click the **Test Now** button to start the diagnosis.

Cable Diagnostics	O Safeguard
Port 01 V	Test Now
Port Type Test Result	Cable Length(M)
The cable diagnostics feature is designed primarily for administrators or customer copper cables; it can rapidly determine the quality of the cables and the types of e	
Note: 1. If cable length is displayed as "N/A" it means the cable length is "Not Available" This is due to the port being unable to obtain cable length/either because its lin used are broken and/or bad in quality.	ik speed is 10M or 100M, or the cables
The deviation of "Cable Fault Distance" is +/-10 meters, therefore No cable may cable used is less than 2 m in length.	y be displayed under Test Result, when the
3. It also measures cable fault and identifies the fault in length according to the dis	
 Before enabling Cable Diagnostics function, please be sure to disable Power S of Web GUI. 	saving via the Fower Saving conlightation
Figure 4.199 - Monitoring > Cable Diag	inostics

Test Result: The description of the cable diagnostic results.

•OK means the cable is good for the connection.

•Short in Cable means the wires of the RJ45 cable may be in contact somewhere.

•Open in Cable means the wires of RJ45 cable may be broken or the other end of the cable is simply disconnected.

•Test Failed means some other errors occurred during cable diagnostics. Please select the same port and test again.

Cable Fault Distance (meters): Indicates the distance of the cable fault from the Switch port, if the cable is less than 2 meters, it will show "No Cable", whether the fiber is connected to the port or not.

Cable Length (meter): If the test result shows OK, then cable length will be indicated for the total length of the cable. The cable lengths are categorized into four types: <50 meters, 50~80 meters, 80~100 meters and

>100 meters. Deviation is +/-2 meters, therefore "No Cable" may be displayed under "Test Result," when the cable used is less than 2 m in length. This test can only be performed when the port is up and operating at 1 Gbps.



NOTE: Cable length detection is effective on Gigabit ports only. The definition of cable pair is listed below: Pair1: PIN4, PIN5 Pair2: PIN1, PIN2 Pair3: PIN3, PIN6

Monitoring > System Log

The System Log page provides information about system logs, including information when the device was booted, how the ports are operating, when users logged in, when sessions timed out, as well as other system information.

Switc	0 Safeguard		
			Refresh Clear
' Maxin	ium Entries : 500)		
·	-		
ID	Time	Log Description	Severity
ID 4	Jan 1 04:01:11	Successful login through Web (IP: 10.90.90.99)	info
ID 4			
·	Jan 1 04:01:11	Successful login through Web (IP: 10.90.90.99)	info

Figure 4.200 - Monitoring > System Log

ID: Displays an incremented counter of the System Log entry. The Maximum entries are 500.

Pair4: PIN7, PIN8

Time: Displays the time in days, hours, and minutes the log was entered.

Log Description: Displays the description of event recorded.

Severity: Displays a severity level of the event recorded.

Click **Refresh** to renew the page, and click **Clear** to clean out all log entries.

Monitoring > Browse ARP Table

The Browse ARP Table page provides information regarding ARP VLANs, including which IP address was mapped to what MAC address. To clear the ARP Table, click **Clear All.**

Browse ARP Ta	able			O Safeguard
Interface Name	System	IP Address		Find
				Clear All
Interface Name	IP Address	MAC Address	Туре	

Figure 4.201 - Monitoring > Browse ARP Table

Click Find, The table updates and displays the values required.

Interface Name: Defines the name of ARP mappings.

IP Address: Defines the station IP address, which is associated with the MAC address.

MAC Address: Displays the MAC address associated with the IP address.

Type: Indicates how the MAC was assigned. The possible values are:

Dynamic – Indicates that the MAC address is dynamically created.

Static – Indicates the MAC address is a static IP address.

Port: Defines the ARP mapping ports.

Monitoring > Ethernet OAM > Browse Ethernet OAM Event Log

The Browse Ethernet OAM Event Log page displays the ports Ethernet OAM event log information.

Browse Ethernet OAM Event Log				
Port	01 🔻	Find		
Port List (e.g.:1,4-6)	All Ports	Clear		
Local Event Statistics				
	Error Symbol Event	0		
	Error Frame Event	0		
	Error Frame Period Event	0		
	Errored Frame Seconds Event	0		
	Dying Gasp	U		
Remote Event Statistics	Critical Event	0		
Remote Event Statistics	Error Symbol Event	0		
	Error Frame Event	0		
	Error Frame Period Event	0		
	Errored Frame Seconds Event	ů		
	Dying Gasp	ŭ		
	Critical Event	õ		
Ethernet OAM Event Log Table				
Index	Type Location	Time Stamp		

Figure 4.202 - Monitoring > Ethernet OAM > Browse Ethernet OAM Event Log

Port: Select the port to be viewed.

Port List: Enter a list of ports. Tick the All Ports check box to select all ports.

Click **Find** to locate a specific entry based on the information entered. Click **Clear** to clear all the information entered in the fields.

Monitoring > Ethernet OAM > Browse Ethernet OAM Statistics

The Browse Ethernet OAM Statistics page displays the ports Ethernet OAM statistics information.

Browse Ethernet OAM Statistics			O Safeguard
Port List (e.g.:1,4-6)		All Ports	Clear
Ethernet OAM Statistics			
Port 1			▲
Information OAMPDU Tx	0	Information OAMPDU Rx	0
Unique Event Notification OAMPDU Tx	0	Unique Event Notification OAMPDU Rx	0
Duplicate Event Notification OAMPDU Tx	0	Duplicate Event Notification OAMPDU Rx	0
Loopback Control OAMPDU Tx	0	Loopback Control OAMPDU Rx	0
Variable Request OAMPDU Tx	0	Variable Request OAMPDU Rx	0
Variable Response OAMPDU Tx	0	Variable Response OAMPDU Rx	0
Organization Specific OAMPDUs Tx	0	Organization Specific OAMPDUs Rx	0
Unsupported OAMPDU Tx	0	Unsupported OAMPDU Rx	0
Frames Lost Due To OAM	0		
Port 2			
Information OAMPDU Tx	0	Information OAMPDU Rx	0
Unique Event Notification OAMPDU Tx	0	Unique Event Notification OAMPDU Rx	0
Duplicate Event Notification OAMPDU Tx	0	Duplicate Event Notification OAMPDU Rx	0
Loopback Control OAMPDU Tx	0	Loopback Control OAMPDU Rx	0

Figure 4.203 - Monitoring > Ethernet OAM > Browse Ethernet OAM Statistics

Port List: Enter a list of ports. Tick the **All Ports** check box to select all ports.

Click Clear to clear all the information entered in the fields.

Monitoring > IGMP Snooping > IGMP Snooping Group

The IGMP Snooping Group page is used to display the current IGMP snooping static group information on the Switch.

IGMP Snooping C	Group				(Safeguard
VLAN Name						
Group IP Address					Find Vlan CI	ear Data Driven
IGMP Snooping Group Ta	ble Total Entries	: 0		View All View	All Data Driven Clear	All Data Driven
VID Vlan Name	Source	Group	Member Port Router Port	Reports Up T	- Expire	Filter Mode
MD Maintaine		Cloup	Member For Roder For	ricpono opr	Time(sec)	Thick Mode

Figure 4.204 - Monitoring > IGMP Snooping > IGMP Snooping Group

VLAN Name: Specify the name of the VLAN for which to be displayed the IGMP Snooping Group information.

VID: Specify the list of the VLAN IDs for which to be displayed the IGMP Snooping Group information.

Group IP Address: Specify the static group address for which to be displayed the IGMP Snooping static group information.

Click **Find VLAN** to display the IGMP group information or click **Clear Data Driven** to clear the IGMP group information.

Monitoring > IGMP Snooping > IGMP Snooping Host

The IGMP Snooping Host page allows user to display the information of IGMP Snooping Host.

IGMP Snooping Host			O Safeguard
 VLAN Name VID(1-4094) 			
Port			
O Group			Find
IGMP Snooping Host Table Total Entries : 0			
VLAN ID Group	Port No	IGMP Host	

Figure 4.205 - Monitoring > IGMP Snooping > IGMP Snooping Host

VLAN Name: Specify the name of the VLAN for which to be displayed the IGMP Snooping Host information. VID (1-4094): Specify the list of the VLAN IDs for which to be displayed the IGMP Snooping Host information. Port: Specify the ports of IGMP Snooping Host information to be displayed.

Group: Specify the group of IGMP Snooping Host information to be displayed.

Click **Find** to display the information.

Monitoring > MLD Snooping > MLD Snooping Group

The MLD Snooping Group page allows user to configure the MLD Snooping group settings.

MLD Snooping Group	O Safeguard
VLAN Name Group IP Address	O VID Find Vlan Clear Data Driven
·	View All View All Data Driven Clear All Data Driven
MLD Snooping Group Table Total Entries : 0	
VID Vlan Name Source Group	Member Router Reports Up Time Expire Filter Port Port Rode Time(sec) Mode

Figure 4.206 - Monitoring > MLD Snooping > MLD Snooping Group

VLAN Name: Specify the VLAN name for MLD Snooping group.

VID: Specify the VID for MLD Snooping group.

Group IP Address: Specify the IP address for the specified VLAN.

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

Click View All to display all the existing entries.

Click View All Data Driven to display all existing entire entries.

Click **Clear All Data Driven** to clear data driven information for all entries.

Monitoring > Port Access Control > RADIUS Authentication

This table contains information concerning the activity of the RADIUS authentication client on the client side of the RADIUS authentication protocol. It has one row for each RADIUS authentication server that the client shares a secret with.

ServerInde	ex InvalidSe	erver Identifier	ServerIPAd	ldr UDP_P	ort Timeou	uts Reque	sts Challer	iges Accep	ots Rejec	ts RoundT
2	0		0.0.0.0	0	0	0	0	0	0	0
3	0	D-Link		0	0	0	0	0	0	0

Figure 4.207 - Monitoring > Port Access Control > RADIUS Authentication

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is one second. To clear the current statistics shown, click the **Clear** button in the top left hand corner.

The following fields can be viewed:

Server Index: The identification number assigned to each RADIUS Authentication server that the client shares a secret with.

UDP Port: The UDP port the client is using to send requests to this server.

Timeouts: The number of authentication timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

Requests: The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.

Challenges: The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.

Accepts: The number of RADIUS Access-Accept packets (valid or invalid) received from this server.

Rejects: The number of RADIUS Access-Reject packets (valid or invalid) received from this server.

RoundTripTime: The time interval (in hundredths of a second) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.

AccessRetrans: The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.

PendingRequests: The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject or Access-Challenge, a timeout or retransmission.

AccessResponses: The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or Signature attributes or known types are not included as malformed access responses.

BadAuthenticators: The number of RADIUS Access-Response packets containing invalid authenticators or Signature attributes received from this server.

UnknownTypes: The number of RADIUS packets of unknown type which were received from this server on the authentication port.

PacketsDropped: The number of RADIUS packets of which were received from this server on the authentication port and dropped for some other reason.

Monitoring > Port Access Control > RADIUS Account Client

This RADIUS Account Client page shows managed objects used for managing RADIUS accounting clients, and the current statistics associated with them. It has one row for each RADIUS authentication server that the client shares a secret with.

Cle	ar								
Serverl	ndex InvalidServerA	ddr Identifier	D Addr	Server Port Number		Requests	Responses	RoundTripTime	AccessRetra
1	0	D-Link	0.0.0.0	0	0	0	0	0	0
2	0	D-Link	0.0.0.0	0	0	0	0	0	0
3	0	D-Link	0.0.0.0	0	0	0	0	0	0

Figure 4.208 - Monitoring > Port Access Control > RADIUS Account Client

The user may also select the desired time interval to update the statistics, between *1s* and *60s*, where "s" stands for seconds. The default value is *one* second. To clear the current statistics shown, click the Clear button in the top left hand corner.

The following fields can be viewed:

Server IP Addr: The IP address assigned to each RADIUS Accounting server that the client shares a secret with.

Server Port Number: The UDP port the client is using to send requests to this server.

Timeouts: The number of accounting timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.

Requests: The number of RADIUS Accounting-Request packets sent. This does not include retransmissions. **Responses:** The number of RADIUS packets received on the accounting port from this server.

RoundTripTime: The time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.

AccessRetrans: The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.

PendindRequests: The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an Accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.

MalformedResponses: The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.

BadAuthenticators: The number of RADIUS Accounting-Response packets, which contained invalid authenticators, received from this server.

UnknownTypes: The number of RADIUS packets of unknown type which were received from this server on the accounting port.

PacketsDropped: The number of RADIUS packets, which were received from this server on the accounting port and dropped for some other reason.

ACL > ACL Configuration Wizard

Access Control List (ACL) allows user to establish criteria to determine whether or not the Switch will forward packets based on the information contained in each packet's header. These criteria can be specified on a basis of MAC address, or IP address.

The **ACL Configuration Wizard** will aid with the creation of access profiles and ACL Rules. The ACL Wizard will create the access rule and profile automatically. The maximum usable profiles are 50 and with 240 Rules in total for the switch.

ACL Configuration Wizard	O Safeguard
General ACL Rules	
From	
Any	
То	
Any	
Service Type	
Any T (P(0x0800)	
Action	
Permit	
Ports	
Ex(1,2,4-6)	
	Apply
Note: ACL Wizard will create the access profile and rule automatically.	
ACL with and win create the access profile and rule adjornatically. For advanced access profile/rule setting, you can manually configure it in Access Profile List.	

Figure 4.229 - ACL > ACL Configuration Wizard

From: Specify the origin of accessible packets. The possible values are:

Any - Indicates ACL action will be on packets from any source.

MAC Address - Indicates ACL action will be on packets from this MAC address.

IPv4 Addresses - Indicates ACL action will be on packets from this IPv4 source address.

IPv6 Addresses - Indicates ACL action will be on packets from this IPv6 source address

To: Specify the destination of accessible packets. The possible values are:

Any - Indicates ACL action will be on packets from any source.

MAC Address - Indicates ACL action will be on packets from this MAC address. The field of format is xx-xx-xx-xx-xx.

IPv4 Addresses - Indicates ACL action will be on packets from this IPv4 source address.

IPv6 Addresses - Indicates ACL action will be on packets from this IPv6 source address.

Service Type: Specify the type of service. The possible values are:

Any - Indicates ACL action will be on packets from any service type.

Ether type - Specifies an Ethernet type for filtering packets.

ICMP All - Indicates ACL action will be on packets from ICMP packets.

IGMP - IGMP packets can be filtered by IGMP message type.

TCP All - Indicates ACL action will be on packets from TCP Packets.

TCP Source Port - Matches the packet to the TCP Source Port.

TCP Destination Port - Matches the packet to the TCP Destination Port.

UDP All - Indicates ACL action will be on packets from UDP Packets.

UDP Source Port - Matches the packet to the UDP Source Port.

UDP Destination Port - Matches the packet to the UDP Destination Port.

Action: Specify the ACL forwarding action matching the rule criteria.

Permit - Forwards packets if all other ACL criteria are met.

Deny - Drops packets if all other ACL criteria is met.

Mirror - Mirrors packets if all other ACL criteria is met.

Rate Limit - Rate limiting is activated if all other ACL criteria is met.

Replace DSCP - Reassigns a new DSCP value to the packet if all other ACL criteria are met.

Ports: Enter a range of ports to be configured.

Press Apply for the settings to take effect.

NOTE: Once the ACL rules conflict, rules with

smaller rule ID will take higher priority.



NOTE: Be careful when configuring ACL rules, an inappropriate may cause management access failed.

ACL > Access Profile List

The Access Profile List provides information for configuring ACL Profiles manually. ACL profiles are attached to interfaces, and define how packets are forwarded if they match the ACL criteria.

Access Profile List	lafeguard
Add ACL Profile Delete All	
Profile ID Owner Type Profile Summary Action Action	Action
Current/Max. Profile: 0/6, Current/Max. Rule: 0/768	

Figure 4.230 - ACL > Access Profile List

The contents of Access Profile List table include:

Profile ID: Indicates the profile Identification number. The possible configured profile IDs are 1~50, and profile ID 51~55 are reserved for the pre-defined features.

Owner Type: The owner type of ACL profile; it can be normal ACL, Voice VLAN or Surveillance VLAN.

Profile Summary: Displays the profile summary.

Show Details: To display an ACL's profile details. The ACL profile details are displayed below the ACL table. **Show Rules:** To show the access rule in this profile.

To add a new rule, please see **Access Rule List** in the next section.

Delete: To delete an access profile.

To manually add a profile, click Add ACL Profile:

Add ACL Profile			O Safeguard
Select Profile ID	1 •		
Select Frame Type	O MAC ACL		
	IPv4 ACL ICMF	•	
	IPv6 ACL		
	Packet content ACL		Select
You can select the fi	eld in the packet to create filtering mask		
	L2 Header	IPv4 DSCP/TOS	ICMP
IPv4 Address			
🔲 Source IP Mask 📃	Mask Generate		
Destination IP Mask	Mask Generate		

Figure 4.231 - Add ACL Profile

The steps of adding an access profile is like below:

1) After selecting the **Profile ID** and **Frame Type** (MAC, IPv4, IPv6 or Packet content ACL), specify attributes like Untagged/Tagged (for MAC), ICMP/IGMP/TCP/UDP/Protocol ID (for IPv4), or ICMPv6/TCP/UDP (for IPv6), then click **Select** and a simplified frame diagram will be displayed.

2) Select the field of interest and related columns will be displayed in lower part of the page. Enter the filtering mask and click **Create** when done. A filtering mask is to specify the digit that user wants to check. For example, if user wants to check a network of 192.168.1.0/24, then it should enter the IP mask as 255.255.255.0.

NOTE: Unable to select Payload in a MAC ACL, or L2 Header in IP ACL.

3) After the **Profile ID** has been created, it will go back to the main Access Profile List page.

ACL > ACL Finder

The ACL Finder page is used to help user to find a previously configured ACL entry. To search for an entry, enter the Profile ID from the drop-down menu, select a port that user would like to view and click **Find.** The table on the lower half of the screen will display the entries. To delete an entry click the corresponding **Delete** button.

ACL Finder	O Safeguard
ACL rule finder helps you identify any rule has been assigned to a specific port Profile ID Any Ports	Find
Profile ID Access ID Profile Type Summary Action	

Figure 4.232 - ACL > ACL Finder

ACL > CPU Filter Configuration Wizard

The CPU Filter Configuration Wizard will aid with the creation of CPU Filter Rules.

CPU Filter Configuration Wizard			O Safeguard
CPU Filter Global Settings:	Enabled	O Disabled	Apply
General CPU Filter Rules			
From			
Any 🔻]	
То			
Any 🔻]	
Service Type			
Any 🔻]	
Action			
Permit 🔹]	
Ports			
		ex:(1,2,4-6)	
			Apply
Note: CPU Filter Wizard will create the access profile For advanced access profile/rule setting. you c			st.

Figure 4.233 - ACL > CPU Filter Configuration Wizard

CPU Filter Global Settings: To enable or disable the CPU filter feature. Press **Apply** for the settings to take effect.

From: Specify the origin of accessible packets. The possible values are:

Any - Indicates CPU Filter action will be on packets from any source.

MAC Address - Indicates CPU Filter action will be on packets from this MAC address.

IPv4 Addresses - Indicates CPU Filter action will be on packets from this IPv4 source address.

IPv6 - Indicates CPU Filter action will be on packets from this IPv6 source address.

To: Specify the destination of accessible packets. The possible values are:

Any - Indicates CPU Filter action will be on packets to any source.

MAC Address - Indicates CPU Filter action will be on packets to this MAC address. The field of format is xx-xx-xx-xx-xx.

IPv4 Addresses - Indicates CPU Filter action will be on packets to this IPv4 source address.

IPv6 - Indicates CPU Filter action will be on packets to this IPv6 source address.

Service Type: Specify the type of service. The possible values are:

Any - Indicates CPU Filter action will be on packets of any service type.

Ether type - Specifies an Ethernet type for filtering packets.

ICMP AII - Indicates CPU Filter action will be on all ICMP packets.

IGMP - IGMP packets can be filtered by IGMP message type.

TCP All - Indicates CPU Filter action will be on all TCP Packets.

TCP Source Port - Take effect if TCP Source Port matches.

TCP Destination Port - Take effect if TCP Destination Port matches.

UDP All - Indicates CPU Filter action will be on all UDP Packets.

UDP Source Port - Take effect if UDP Source Port matches.

UDP Destination Port - Take effect if UDP Destination Port matches.

Action: Specify the CPU Filter forwarding action matching the rule criteria.

Permit - Forwards packets if all other CPU Filter criteria are met.

Deny - Drops packets if all other CPU Filter criteria is met.

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

ACL > CPU Filter Access Profile List

The CPU Filter Access Profile List provides information for configuring CPU Profiles manually. CPU Filter Access profiles are attached to interfaces, and define how packets are forwarded if they match the CPU Filter criteria.

CPU Filter Access Profile List		O Safeguard
Add CPU Filter Profile Delete All		
Profile ID Owner Type	Profile Summary	
Current/Max. Profile: 0/3, Current/Max. Rule: 0/0		

Figure 4.234 - ACL > CPU Filter Access Profile List

The contents of CPU Filter Access Profile List table include:

Profile ID: Indicates the profile Identification number. The possible configured profile IDs are 1~50, and profile ID 51 is reserved for Voice VLAN.

Owner Type: The owner type of CPU Filter profile, it can be normal CPU Filter, Voice VLAN or Surveillance VLAN.

Profile Summary: Displays the profile summary.

Show Details: To display a CPU Filter's profile details. The CPU Filter profile details are displayed below the CPU Filter table.

Edit/New Rules: To configure or add the CPU access rule in this profile.

To add a new rule, please see Add CPU Filter Profile in the next section.

Delete All: To delete all access profile.

To manually add a profile, click Add CPU Filter Profile.

Add CPU Filter P	rofile			Safeguard		
Select Profile ID Select Frame Type	1 MAC Filter Pv4 Filter Pv6 Filter Traffic Clas			Select		
You can callect the fi		5 *		Select		
You can select the field in the packet to create filtering mask						
	L2 Header	IPv6 Class	IPv6 Address			
IPv6 Address	L2 Header	IPv6 Class	IPv6 Address			
IP v6 Address	L2 Header Mask Generate	IPv6 Class	IPv6 Address			
	Mask Generate	IPv6 Class	IPv6 Address			

Figure 4.235 - ACL > CPU Filter Access Profile List -Add CPU Filter Profile

The steps of adding a CPU Filter profile is like below:

1) After selecting the **Profile ID** and **Frame Type** (MAC, IPv4 or IPv6), specify attributes like Untagged/Tagged (for MAC), or ICMP/IGMP/TCP/UDP/Protocol ID (for IPv4), or Traffic Class (for IPv6), then click **Select** and a simplified frame diagram will be displayed.

2) Select the field of interest and related columns will be displayed in lower part of the page. Enter the filtering mask and click **Create** when done. A filtering mask is to specify the digit that user wants to check. For example, if user wants to check a network of 192.168.1.0/24, then it should enter the IP mask as 255.255.255.0.

3) After the **Profile ID** has been created, it will go back to the main **CPU Filter Access Profile** List page.

ACL > CPU Filter Finder

The CPU Filter Finder page is used to help user to find a previously configured CPU entry. To search for an entry, enter the Profile ID from the drop-down menu, select a port that user would like to view and click **Find**. The table on the lower half of the screen will display the entries. To delete an entry click the corresponding **Delete** button.

CPU Filter Finder				O Safeguard
CPU filter rule finder helps	you identify any rul	e has been assigned to a specific port		
Profile ID Any 🔻	Ports			Find
Durfle ID Arrest ID	Duefie True		0 stient	
Profile ID Access ID	Profile Type	Summary	Action	
		Figure 4.236 - ACL > CPU Filter Finder		

PoE > PoE Port Settings (DGS-1210-10P/10MP/28P/28MP/52MP only)

DGS-1210-10P/10MP/28P/28MP/52MP supports Power over Ethernet (PoE) as defined by the IEEE specification.

DGS-1210-10P/10MP/28P/28MP/52MP works with all D-Link 802.3af or 802.3at capable devices. The Switch also works in PoE mode with all non-802.3af capable D-Link AP, IP Cam and IP phone equipment via the PoE splitter DWL-P50.

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

Class	Usage	Output power limit by PSE
0	Default	15.4W
1	Optional	4.0W
2	Optional	7.0W

3	Optional	15.4W
4	Reserved	30W

The PoE port table will display the PoE status including, Port Enable, Power Limit, Power (W), Voltage (V), Current (mA), Classification, Port Status. User can select **From Port** / **To Port** to control the PoE functions of a port. DGS-1210-10P/28P/28MP/52P/52MP/52MPP/ME will auto disable the ports if port current is over 375mA in 802.3af mode or 625mA in pre-802.3at mode.

Note: The PoE Status information of Power current, Power Voltage, and Current is the power usage information of the connected PD; please "Refresh" to renew the information.

Note: The following table listed PoE hardware specifications for each model of DGS-1210/ME series:

Model	802.3at compliance port	System Budget
DGS-1210-10P	1-8	65 Watts
DGS-1210-10MP	1-8	130 Watts
DGS-1210-28P	1-24	193 Watts
DGS-1210-28MP	1-24	370 Watts
DGS-1210-52MP	1-8	370 Watts

oE P	ort Settin	gs		_		_	_	_	0	Safegu	ar
rom Po 1 Delay Po Disable	V ower Detect	To Port 48 Power Limit Auto	>	State Enabled User Define			Time Range N/A Apply	✓ Refres	Priority Normal V		
Port	State	Time Range	Priority	Delay Power Detect	Power Limit	Power(W)	Voltage(V)	Current(mA)	Classification	Status	1
1	Enabled	N/A	Normal	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF	1
2	Enabled	N/A	Normal	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF	1
3	Enabled	N/A	Normal	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF	1
4	Enabled	N/A	Normal	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF	1
5	Enabled	N/A	Normal	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF	1
6	Enabled	N/A	Normal	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF	1
7	Enabled	N/A	Normal	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF	1
8	Enabled	N/A	Normal	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF	1
9	Enabled	N/A	Normal	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF	1
10	Enabled	N/A	Normal	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF	1
11	Enabled	N/A	Normal	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF	1

Figure 4.239 – PoE > PoE Port Settings

Parameter	Description
From Port/To Port	Specifies the PoE function of a port or ports
State	Select "Enabled" or "Disabled" to configure PoE function for designated port(s). Default is Enabled
Time Range	Select the PoE time profile configured from Time-Based PoE > Time Range Settings to enable the time-based PoE function on designated port(s). Default setting is N/A

⁰

Priority	Configure the power supply priority as " Low ", " Normal ", or " High " on designated port(s). Default is Normal .
Delay Power Detect	Configure the delay power detection. Default is Disabled. This switch conforms to IEEE 802.3af and 802.3at standards. The IEEE PoE standard requires a switch to shut off power to a port if the power draw is less than 10mA within a 400ms time interval. To support some non- standard devices that may take longer, user may enable this feature to extend the time interval to 500ms. If the PD is still not powering on, please contact the vendor of the device for support.
Power Limit	This feature allows user to specify the power limit for each ports. If a port requested the power exceeds its power limit, it will shut down. There are options as the following list: Auto: Automatic classification the PD's power consumption. Class 1: Specifies that the power limit will be set to 4W Class 2: Specifies that the power limit will be set to 7W Class 3: Specifies that the power limit will be set to 15.4W Class 4: For 802.3at compliance PD devices. Supports up to 30W in this class. User Define: Maximum supports to 30W

Click **Apply** to make the configurations take effect or click **Refresh** to redisplay the table.



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.



Note: The ports 1-4 are capable of feeding power up to 30 watts to devices with the LLDP-Med function is enabled of the connected PD. Or the ports can only feeding power up to 15.4 watts.

PoE > PoE System Settings (DGS-1210-10P/10MP/28P/28MP/52MP only)

This PoE System Settings page will display the PoE status including **System Budget Power**, **Support Total Power**, **Remainder Power**, and **The ratio of system power supply**.

PoE System settings		O Safeguard
System Power Threshold	370.0W (7.1-370.0)	
PoE LegcyPd Detection	Disabled V	
System Setting Disconnect Method	Deny low priority port 🗸	Apply
System Power Status		
System Budget Power	370 W	
Support Total Power	0 W	
Remainder Power	370 W	
The ratio of system power supply	0 %	
Note : If power disconnection method is set to	deny next port, then the system can not utilize out of its maximum power cap	pacity.
	Figure 4.240 – PoE > PoE System Settings	

System Power Threshold: Manually configure the system power budget 7.1 ~ 193.0 watts for DGS-1210-28P/ME.

PoE LeacyPD Detection: Specifies the legacy PDs detection status.

System Setting Disconnect Method: Defines the method used to deny power to a port once the threshold is reached. The possible fields are:

Deny next port: When the power budget is exceeded, the next port attempting to power up is denied, regardless of the port priority.

Deny low priority port: The port with the lower priority will be shut down to allow the higher priority port to power up.

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

LLDP > LLDP Global Settings

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

LLDP Global Settings			O Safeguard
LLDP LLDP Forward Message	 Enabled Enabled 	Disabled Disabled	Apply Apply
Message TX Hold Multiplier (2 - 10)		4	
Message TX Interval (5 - 32768)		30 sec	
LLDP Reinit Delay (1 - 10)		2 sec	
LLDP TX Delay (1 - 8192)		2 sec	Apply
LLDP System Information			
Chassis ID Subtype		macAddress	
Chassis ID		80-26-89-3D-D0-60	
System Name			
System Description		DGS-1210-52MP/ME/B1	

Figure 4.242 – LLDP > LLDP Global Settings

LLDP: When this function is *Enabled*, the switch can start to transmit, receive and process the LLDP packets. For the advertisement of LLDP packets, the switch announces the information to its neighbor through ports. For the receiving of LLDP packets, the switch will learn the information from the LLDP packets advertised from the neighbor in the neighbor table. Click **Apply** to make the change effective.

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**.

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.

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

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

LLDP > Basic LLDP Port Settings

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

Basic LLDF	Port Settings					O Safeguard
From Port	To Port 28 ▼		n Status Port Desci Only T Disabled	<u> </u>	System Description Disabled ▼ Ap	System Capabilities Disabled V ply Refresh
Port	Notification State	Admin Status	Port Description	System Name	System Description	System Capabilities
1	Disable	TX_and_RX	Disable	Disable	Disable	Disable
2	Disable	TX_and_RX	Disable	Disable	Disable	Disable
3	Disable	TX_and_RX	Disable	Disable	Disable	Disable
4	Disable	TX_and_RX	Disable	Disable	Disable	Disable
5	Disable	TX_and_RX	Disable	Disable	Disable	Disable
6	Disable	TX_and_RX	Disable	Disable	Disable	Disable
7	Disable	TX_and_RX	Disable	Disable	Disable	Disable
8	Disable	TX_and_RX	Disable	Disable	Disable	Disable
9	Disable	TX and RX	Disable	Disable	Disable	Disable

Figure 4.243– LLDP > Basic LLDP Port Settings

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

Notification State: Specifies whether notification is sent when an LLDP topology change occurs on the port. The possible field values are:

Enabled – Enables LLDP notification on the port.

Disabled – Disables LLDP notification on the port. This is the default value.

Admin Status: Specifies the LLDP transmission mode on the port. The possible field values are:

TX_Only – Enables transmitting LLDP packets only.

RX_Only – Enables receiving LLDP packets only.

TX_and_RX - Enables transmitting and receiving LLDP packets. This is the default.

Disabled - Disables LLDP on the port.

Port Description: Specifies whether the Port Description TLV is enabled on the port. The possible field values are:

Enabled – Enables the Port Description TLV on the port.

Disabled - Disables the Port Description TLV on the port.

System Name: Specifies whether the System Name TLV is enabled on the port. The possible field values are:

Enabled – Enables the System Name TLV on the port.

Disabled – Disables the System Name TLV on the port.

System Description: Specifies whether the System Description TLV is enabled on the port. The possible field values are:

Enabled – Enables the System Description TLV on the port.

Disabled – Disables the System Description TLV on the port.

System Capabilities: Specifies whether the System Capabilities TLV is enabled on the port. The possible field values are:

Enabled – Enables the System Capabilities TLV on the port.

Disabled – Disables the System Capabilities TLV on the port.

Define these parameter fields. Click **Apply** to implement changes made and click **Refresh** to refresh the table information.

LLDP > 802.1 Extension LLDP Port Settings

This 802.1 Extension LLDP Port Settings page is used to configure the LLDP Port settings.

802.1 Exte	nsion LLDP Port Settings			O Safeguard
From Port To Port Port VLAN ID Protocol VLAN VLAN Name Protocol Identity	Disabled VLAN ID	 ✓ ✓ 		Apply Refresh
Port	Port VLAN ID	Protocol VLAN ID	Enabled VLAN Name	Enabled Protocol Identity
1	Disable		(None)	(None)
2	Disable		(None)	(None)
3	Disable		(None)	(None)
4	Disable		(None)	(None)
5	Disable		(None)	(None)
6	Disable		(None)	(None)
7	Disable		(None)	(None)
8	Disable		(None)	(None)
9	Disable		(None)	(None)
10	Disable		(None)	(None)
11	Disable		(None)	(None)
12	Disable		(None)	(None)
13	Disable		(None)	(None)
14	Disable		(None)	(None)
15	Disable		(None)	(None)
16	Disable		(None)	(None)

Figure 4.244 – LLDP > 802.1 Extension LLDP Port Settings

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

Port VLAN ID : Specifies the Port VLAN ID to be enabled or disabled.

Protocol VLAN ID : Specifies the VLAN ID to be enabled or disabled in the LLDP port. If select Enabled, users can specifies the content of VLAN ID.

VLAN Name : Specifies the VLAN name to be enabled or disabled in the LLDP port. If select Enabled, users can specifies the content of VLAN Name.

Protocol Identity : Specifies the Protocol Identity to be enabled or disabled in the LLDP port. If select Enabled, users can specifies the EAPOL, LACP, GVRP, STP or ALL.

Click **Apply** to implement changes made and click **Refresh** to refresh the table information.

LLDP > 802.3 Extension LLDP Port Settings

The 802.3 Extension LLDP Port Settings page displays 802.3 Extension LLDP port information and contains parameters for configuring 802.3 Extension LLDP port settings.

802.3 Exter	802.3 Extension LLDP Port Settings O Safeguard					
From Port		PHY juration/Status Power Via MDI bled V Disabled V	Link Aggregation Maximum F Disabled V Disabled			
Port	MAC/PHY Configuration/Status	Power Via MDI	Link Aggregation	Maximum Frame Size		
1	Disable	Enable	Disable	Disable	$^{\sim}$	
2	Disable	Enable	Disable	Disable		
3	Disable	Enable	Disable	Disable		
4	Disable	Enable	Disable	Disable		
5	Disable	Enable	Disable	Disable		
6	Disable	Enable	Disable	Disable		
7	Disable	Enable	Disable	Disable		
8	Disable	Enable	Disable	Disable		
9	Disable	Disable	Disable	Disable		
10	Disable	Disable	Disable	Disable		
11	Disable	Disable	Disable	Disable		
12	Disable	Disable	Disable	Disable		
13	Disable	Disable	Disable	Disable		
14	Disable	Disable	Disable	Disable		
15	Disable	Disable	Disable	Disable		
16	Disable	Disable	Disable	Disable		
17	Disable	Disable	Disable	Disable		
18	Disable	Disable	Disable	Disable		

Figure 4.245 – LLDP > 802.3 Extension LLDP Port Settings

From Port/To Port: A consecutive group of ports may be configured starting with the selected port. **MAC/PHY Configuration/Status:** Specifies whether the MAC/PHY Configuration Status is enabled on the

port. The possible field values are:

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

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

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

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

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

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

Enabled – Enables the link aggregation configured on the port.

Disabled – Disables the link aggregation configured on the port.

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

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

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

Define these parameter fields. Click **Apply** to implement changes made and click **Refresh** to refresh the table information.

LLDP > LLDP Management Address Settings

The LLDP Management Address Settings allows the user to set management address which is included in LLDP information transmitted.

LLDP Manag	gement Address	Settings			O Safeguard
From Port	To Port	Address Type	Address	Port State Disabled 🔻	Apply
Enabled Manage	ment Address Table				
Port ID	Enabled Manag	ement Address			
1	(NONE)				
2	(NONE)				
3	(NONE)				
4	(NONE)				
5	(NONE)				
6	(NONE)				
7	(NONE)				
8	(NONE)				
9	(NONE)				
10	(NONE)				
11	(NONE)				
12	(NONE)				

Figure 4.246 – LLDP > LLDP Management Address Settings

From Port/To Port: A consecutive group of ports may be configured starting with the selected port. **Address Type:** Specify the LLDP address type on the port. The value is always IPv4.

Address: Specify the address.

Port State: Specify whether the Port State is enabled n the port. The possible field values are:

Enabled – Enables the port state configured on the port.

Disabled – Disables the port state configured on the port.

Click Apply to make the configurations take effect.

LLDP > LLDP Statistics Table

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

LDP	Statistics Table						O Safegua
LLDP St	atistics System						
Last Ch	ange Time		0				
Number	r of Table Insert		0				
Number	of Table Delete		0				
Number	r of Table Drop		0				
Number	of Table Age Out		0				
LLDP St	atistics Ports						
	atistics Ports TxPort FramesTotal	RxPortFrames DiscardedTotal	RxPort FramesErrors	RxPort FramesTotal	RxPortTLVs DiscardedTotal	RxPortTLVs UnrecognizedTotal	RxPort AgeoutsTotal
			RxPort FramesErrors 0	RxPort FramesTotal			RxPort AgeoutsTotal 0
LLDP St No. 1 2	TxPort FramesTotal				DiscardedTotal		-
	TxPort FramesTotal		0		DiscardedTotal		
No. 1 2	TxPort FramesTotal 0 0	DiscardedTotal 0 0	0	0 0	DiscardedTotal 0 0	UnrecognizedTotal 0 0	0
No. 1 2	TxPort FramesTotal 0 0	DiscardedTotal 0 0	0	0 0	DiscardedTotal 0 0	UnrecognizedTotal 0 0	0
No. 1 2 3 4	TxPort FramesTotal 0 0 0 0	DiscardedTotal 0 0 0 0	0 0 0 0	0 0 0 0	DiscardedTotal 0 0 0 0	UnrecognizedTotal 0 0 0 0	0
No. 1 2 3 4	TxPort FramesTotal 0 0 0 0	DiscardedTotal 0 0 0 0	0 0 0 0	0 0 0 0	DiscardedTotal 0 0 0 0	UnrecognizedTotal 0 0 0 0	0
No. 1 2 3 4	TxPort FramesTotal 0 0 0 0 0 0 0	DiscardedTotal 0 0 0 0	0 0 0 0 0	0 0 0 0 0	DiscardedTotal 0 0 0 0 0 0 0	UnrecognizedTotal 0 0 0 0 0 0 0	0

Figure 4.247 – LLDP > LLDP Statistics Table

The following information can be viewed:

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

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

Number of Table Insert – Displays the number of new entries inserted since switch reboot.

Number of Table Delete - Displays the number of new entries deleted since switch reboot.

Number of Table Drop – Displays the number of LLDP frames dropped due to that the table was full.

Number of Table Age Out - Displays the number of entries deleted due to Time-To-Live expiring.

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

TxPort FramesTotal – Displays the total number of LLDP frames transmitted on the port.

RxPort FramesDiscarded – Displays the total discarded frame number of LLDP frames received on the port.

RxPort FramesErrors – Displays the Error frame number of LLDP frames received on the port.

RxPort Frames – Displays the total number of LLDP frames received on the port.

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

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

RxPort 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.

LLDP > LLDP Management Address Table

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

LLD	LDP Management Address Table O Safeguard					
Mana	agement Ado	dress IPv4 Address 🔻		Find		
Total	Entries: 2					
No.	Subtype	Address	IF Type	OID	Advertising Ports	
1	IPv4	10.90.90.90	ifIndex	1.3.6.1.2.1.2.2.1.1	(NONE)	
2	IPv6	fe80::212:10ff:fe28:3395	ifIndex	1.3.6.1.2.1.2.2.1.1	(NONE)	

Figure 4.248 – LLDP > LLDP Management Address Table

Management Address: Specifies IPv4 or IPv6 address then enter the address. Click **Search** and the table will update and display the values required.

Subtype: Displays the managed address subtype. For example, MAC or IPv4.

Management Address: Displays the IP address.

IF Type: Displays the IF Type.

OID: Displays the SNMP OID.

Advertising Ports: Displays the advertising ports.

LLDP > LLDP Local Port Table

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

No.	Port ID Subtype	Port ID	Port Description	Normal	Detailed
1	Local	Slot0/1	D-Link DGS-1210-52MP/ME Rev.B1/7.03.006 Port 1	View	View
2	Local	Slot0/2	D-Link DGS-1210-52MP/ME Rev.B1/7.03.006 Port 2	View	View
3	Local	Slot0/3	D-Link DGS-1210-52MP/ME Rev.B1/7.03.006 Port 3	View	View
4	Local	Slot0/4	D-Link DGS-1210-52MP/ME Rev.B1/7.03.006 Port 4	View	View
5	Local	Slot0/5	D-Link DGS-1210-52MP/ME Rev.B1/7.03.006 Port 5	View	View
6	Local	Slot0/6	D-Link DGS-1210-52MP/ME Rev.B1/7.03.006 Port 6	View	View
7	Local	Slot0/7	D-Link DGS-1210-52MP/ME Rev.B1/7.03.006 Port 7	View	View
8	Local	Slot0/8	D-Link DGS-1210-52MP/ME Rev.B1/7.03.006 Port 8	View	View
9	Local	Slot0/9	D-Link DGS-1210-52MP/ME Rev.B1/7.03.006 Port 9	View	View
10	Local	Slot0/10	D-Link DGS-1210-52MP/ME Rev.B1/7.03.006 Port 10	View	View
11	Local	Slot0/11	D-Link DGS-1210-52MP/ME Rev.B1/7.03.006 Port 11	View	View
12	Local	Slot0/12	D-Link DGS-1210-52MP/ME Rev.B1/7.03.006 Port 12	View	View
13	Local	Slot0/13	D-Link DGS-1210-52MP/ME Rev.B1/7.03.006 Port 13	View	View
14	Local	Slot0/14	D-Link DGS-1210-52MP/ME Rev.B1/7.03.006 Port 14	View	View
15	Local	Slot0/15	D-Link DGS-1210-52MP/ME Rev.B1/7.03.006 Port 15	View	View
16	Local	Slot0/16	D-Link DGS-1210-52MP/ME Rev.B1/7.03.006 Port 16	View	View
17	Local	Slot0/17	D-Link DGS-1210-52MP/ME Rev.B1/7.03.006 Port 17	View	View
18	Local	Slot0/18	D-Link DGS-1210-52MP/ME Rev.B1/7.03.006 Port 18	View	View
19	Local	Slot0/19	D-Link DGS-1210-52MP/ME Rev.B1/7.03.006 Port 19	View	View

Figure 4.249 –LLDP > LLDP Local Port Table

No: Displays the port number.

Port ID Subtype: Displays the port ID subtype.

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

Port Description: Displays the port description.

Click View of Normal column to display more information.

LLDP Local Port Normal Table	0 5	afeguard
No.	1	
Port Id Subtype	Interface Alias	
Port Id	Slot0/1	
Port Description	Ethernet Interface	
Port VID	1	
Management Address Count	1	
PPVID Entries Count	0	
VLAN Name Entries Count	1	
Protocol Identity Entries Count	0	
MAC/PHY Configuration/Status	See detail	
Power Via MDI	See detail	
Link Aggregation	See detail	
Maximum Frame Size	1522	
Show LLDP Local Port Brief Table		
Show LLDP Local Port Detailed Table		

Figure 4.250 – LLDP > LLDP Local Port Normal Table

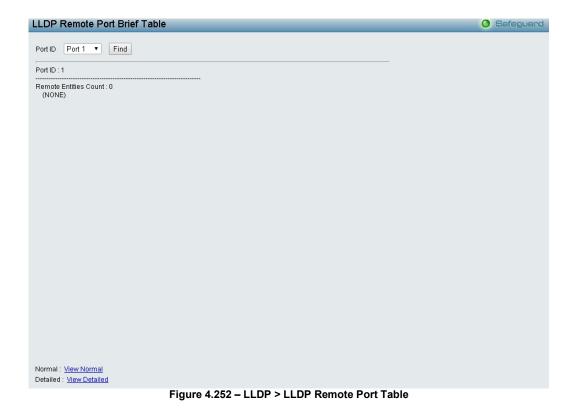
Click View of Detailed column to display detail information.



Figure 4.251 – LLDP > LLDP Local Port Detailed Table

LLDP > LLDP Remote Port Table

This LLDP Remote Port Table page is used to display the LLDP Remote Port Brief Table. Select port number and click **Search** to display additional information.



To view the settings for a remote port, click **View Normal** and the following page displays.

LLDP Remote Port Normal Table	O Safeguard
Port ID : 1	
Remote Entities Count : 0 (NONE)	
Show LLDP Remote Port Brief Table Show LLDP Remote Port Detailed Table	

Figure 4.253 – LLDP > LLDP Remote Port Normal Table

To view the detail settings for a remote port, click **View Detailed** and the following page displays.

LLDP Remote Port Detailed Table	O Safeguard
Port ID : 1	
Remote Entities Count : 0	
(NONE)	
Show LLDP Remote Port Brief Table Show LLDP Remote Port Normal Table	
Eigure 4 254 – 11 DP > 11 DP Remote Port Detailed Table	

LLDP > LLDP-MED Settings

By selecting a range of ports (**From Port** and **To Port**), the power PSE TLV type can be enabled for all selected ports to indicate the power source equipment (PSE) switch to transmit high power (15.4 to 30 Watts) to the pre-standard of 802.3at power devices via LLDP MDI TLV. Through this feature, the PSE can provide precise output power to the pre-standard of 802.3at power devices and achieve optimal power management.

LDP MED Settings O Safeguard						
LLDP-MED Power PSE	TLV Setting					
From Port	To Port	Power PSE TLV				
1 •	24 🔻	Disable v	Apply Refresh			
Port		Power PSE TLV	/			
1		Enable				
2		Enable				
3		Enable				
4		Enable				
5		Enable				

Figure 4.255 – LLDP > LLDP –MED Settings

Appendix A - Ethernet Technology

This chapter will describe the features of the D-Link Metro Ethernet Switch and provide some background information about Ethernet/Fast Ethernet/Gigabit Ethernet switching technology.

Gigabit Ethernet Technology

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

The increased speed and extra bandwidth offered by Gigabit Ethernet is essential in solving network bottlenecks, which frequently develops as more advanced computer users and newer applications continue to demand greater network resources. Upgrading key components, such as backbone connections and servers to Gigabit Ethernet technology, can greatly improve network response times as well as significantly speed up the traffic between subnets.

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

In addition, the phenomenal bandwidth delivered by Gigabit Ethernet is the most cost-effective method to take advantage of today and tomorrow's rapidly improving switching and routing internetworking technologies. With expected advances in the coming years in silicon technology and digital signal processing, which will enable Gigabit Ethernet to eventually operate over unshielded twisted-pair (UTP) cabling, a flexible foundation for the next generation of network technology products will be created. This will outfit your network with a powerful 1000-Mbps-capable backbone/server connection.

Fast Ethernet Technology

The growing importance of LANs, and the increasing complexity of desktop computing applications are fueling the need for high performance networks. A number of high-speed LAN technologies have been proposed to provide greater bandwidth and improve client/server response times. Among them, 100BASE-T (Fast Ethernet) provides a non-disruptive, smooth evolution from the current 10BASE-T technology. The non-disruptive and smooth evolution nature, and the dominating potential market base, virtually guarantees cost-effective and high performance Fast Ethernet solutions.

100Mbps Fast Ethernet is a standard specified by the IEEE 802.3 LAN committee. It is an extension of the 10Mbps Ethernet standard with the ability to transmit and receive data at 100Mbps, while maintaining the CSMA/CD Ethernet protocol. Since the 100Mbps Fast Ethernet is compatible with all other 10Mbps Ethernet environments, it provides a straightforward upgrade and utilizes existing investments in hardware, software, and personnel training.

Switching Technology

Another approach to push beyond the limits of Ethernet technology is the development of switching technology. A switch bridges Ethernet packets at the MAC address level of the Ethernet protocol transmitting among connected Ethernet or Fast Ethernet LAN segments.

Switching is a cost-effective way of increasing the total network capacity available to users on a local area network. A switch increases capacity and decreases network loading by dividing a local area network into different segments, which won't compete with each other for network transmission capacity.

The switch acts as a high-speed selective bridge between the individual segments. The switch, without interfering with any other segments, automatically forwards traffic that needs to go from one segment to another. By doing this the total network capacity is multiplied, while still maintaining the same network cabling and adapter cards.

Appendix B - Technical Specifications

This appendix contains the device specifications, and contains the topics:

- Hardware Specifications
- Features

Hardware Specifications

Key Components / Performance				
Switching Capacity	DGS-1210-10: 20Gbps DGS-1210-10P: 20Gbps DGS-1210-10MP: 20Gbps DGS-1210-20: 40Gbps DGS-1210-26: 52Gbps DGS-1210-28: 56Gbps DGS-1210-28P: 56Gbps DGS-1210-28MP: 56Gbps DGS-1210-52: 104Gbps DGS-1210-52MP: 104Gbps			
Max. Forwarding Rate	DGS-1210-10: 14.88 Mpps DGS-1210-10P: 14.88 Mpps DGS-1210-10MP: 14.88 Mpps DGS-1210-20: 29.8 Mpps DGS-1210-26: 38.7 Mpps DGS-1210-28: 41.7 Mpps DGS-1210-28P: 41.7 Mpps DGS-1210-28MP: 41.7 Mpps DGS-1210-52: 77.4 Mpps DGS-1210-52MP: 77.4 Mpps			
Forwarding Mode	Store and Forward			
Packet Buffer memory	DDGS-1210-10: 4.1 Mbits DGS-1210-10P: 4.1 Mbits DGS-1210-10MP: 4.1 Mbits DGS-1210-20: 4.1 Mbits DGS-1210-26: 4.1 Mbits DGS-1210-28: 4.1 Mbits DGS-1210-28P: 4.1 Mbits DGS-1210-28MP: 4.1 Mbits DGS-1210-52: 12 Mbits DGS-1210-52MP: 12 Mbits			
DDRIII for CPU	256M bytes			
Flash Memory	32M bytes			
Priority Queues	8			
Port Functions				
10/100/1000BASE-TX	8 x 10/100/1000BaseT ports for DGS-1210-10, DGS-1210-10P and DGS-			

Ethernet ports	1210-10MP
Ethemet ports	20 x 10/100/1000BaseT ports for DGS-1210-20
	24 x 10/100/1000BaseT ports for DGS-1210-26
	28 x 10/100/1000BaseT ports for DGS-1210-28, DGS-1210-28P, DGS-1210- 28MP
	52 x 10/100/1000BaseT ports for DGS-1210-52, DGS-1210-52MP
	 1000Base-T ports compliant to following standards: IEEE 802.3 compliance IEEE 802.3u compliance IEEE 802.3ab compliance Support Half/Full-Duplex operations IEEE 802.3x Flow Control support for Full-Duplex mode Back Pressure for Half-Duplex mode
	- Head-of-line blocking prevention
	Support manual/auto MDI/MDIX configuration Support Auto-Negotiation for each port
	Port 9 ~ 10 for DGS-1210-10, DGS-1210-10P and DGS-1210-10MP
	Port 17 ~ 20 for DGS-1210-20
	Port 25 ~ 26 for DGS-1210-26
	Port 25 ~ 28 for DGS-1210-28, DGS-1210-28P, DGS-1210-28MP
	Port 49 ~ 52 for DGS-1210-52 and DGS-1210-52MP
	SFP ports comply with following standards:
	- IEEE 802.3u compliance (Support 100M transceivers)
	- IEEE 802.3z compliance
	- IEEE 802.3ah compliance
SED porto	Support Transceivers:
SFP ports	- 100M/1000M SFP Transceivers
	- WDM SFP Transceivers
	- 1000BASE-T Transceivers
	SFP Transceivers Supported:
	- DGS-712 (1000Base-T)
	- DEM-210 (100BASE-FX, 15km)
	- DEM-211 (100BASE-FX, 2km)
	- DEM-310GT (1000BASE-LX, 10km) - DEM-311GT (1000BASE-SX, 550m)
	- DEM-314GT (1000BASE-SA, 550m) - DEM-314GT (1000BASE-LH, 50km)
	- DEM-314GT (1000BASE-EI), 30km) - DEM-315GT (1000BASE-ZX, 80km)
	- DEM-312GT2 (1000BASE-SX, 2km)

Physical & Environment	WDM Transceivers Supported: - DEM-220T (100Base-BX,TX-1550/RX-1310nm, 20km) - DEM-220R (100Base-BX,TX-1310/RX-1550nm, 20km) - DEM-330T (1000Base-BX,TX-1550/RX-1310nm, 10km) - DEM-330R (1000Base-BX,TX-1310/RX-1550nm, 10km) - DEM-331T (1000Base-BX,TX-1550/RX-1310nm, 40km) - DEM-331R (1000Base-BX,TX-1310/RX-1550nm, 40km)
	DGS-1210-10: Standby power consumption: 2.03 Watts DGS-1210-10P: Maximum power consumption: 81.9 Watts (PoE On),7.6 Watts (PoE Off)
	Standby power consumption: 2.5 Watts DGS-1210-10MP: Maximum power consumption: 152.3 Watts (PoE On), 9.4 Watts (PoE Off) Standby power consumption: 5.2 Watts
	DGS-1210-20: Standby power consumption: 5.47 Watts
	DGS-1210-26: Standby power consumption: 5.01 Watts
Power Consumption	DGS-1210-28: Standby power consumption: 6.49 Watts
	DGS-1210-28P: Maximum power consumption: 263.9 Watts (PoE On), 30.6 Watts (PoE Off) Standby power consumption: 19.6 Watts
	DGS-1210-28MP: Maximum power consumption: 446.1 Watts (PoE On), 29.8 Watts (PoE Off) Standby power consumption: 18.5 Watts
	DGS-1210-52: Standby power consumption: 13.7 Watts
	DGS-1210-52MP: Maximum power consumption: 478.9 Watts (PoE On), 54.4 Watts (PoE Off) Standby power consumption: 32 Watts
Power Supply	DGS-1210-10P: DC:54V / 1.574A DGS-1210-10/10MP/20/26/28/28P/28MP/52/52MP: AC:100~240V, 50/60Hz
Fans	DGS-1210-28P: 2pcs Smart Fan DGS-1210-28MP: 2pcs Smart Fan DGS-1210-52: 2pcs Smart Fan DGS-1210-52MP: 2pcs Smart Fan
Operating Temperature	-5~50°C
Storage Temperature	-20~70°C
Humidity	Storage: 0%~90% non-condensing

Dimensions	$\begin{array}{l} DGS-1220-10:\ 280 \ x\ 126 \ x\ 44 \ mm \\ DGS-1220-10P:\ 280 \ x\ 126 \ x\ 44 \ mm \\ DGS-1220-10MP:\ 330 \ x\ 180 \ x\ 44 \ mm \\ DGS-1220-20:\ 280 \ x\ 180 \ x\ 44 \ mm \\ DGS-1220-26:\ 440 \ x\ 140 \ x\ 44 \ mm \\ DGS-1220-28:\ 440 \ x\ 140 \ x\ 44 \ mm \\ DGS-1220-28P:\ 440 \ x\ 250 \ x\ 44 \ mm \\ DGS-1220-28MP:\ 440 \ x\ 250 \ x\ 44 \ mm \\ DGS-1220-28MP:\ 440 \ x\ 250 \ x\ 44 \ mm \\ DGS-1220-52:\ 440 \ x\ 210 \ x\ 44 \ mm \\ DGS-1220-52MP:\ 440 \ x\ 430 \ x\ 44 \ mm \\ \end{array}$
Weight	DGS-1210-10: 0.98 kg DGS-1210-10P: 0.95 kg DGS-1210-10MP: 1.77 kg DGS-1210-20: 1.75 kg DGS-1210-26: 2.06 kg DGS-1210-28: 2.15 kg DGS-1210-28P: 3.75 kg DGS-1210-28MP: 3.94 kg DGS-1210-52: 3.46 kg DGS-1210-52MP: 6.26 kg
EMI	CE, FCC/IC, VCCI, BSMI, C-Tick
Safety	UL, CB, BSMI

Features

L2 Features

- Supports up to 8K MAC address for DGS-121010MP/28MP.
- Supports 256 static MAC
- Jumbo frame: Supports up to 10,000 bytes.
 - IGMP Snooping v1/v2/v3 awareness:
 - Supports 256 multicast groups
 - Supports at least 32 static multicast groups
- MLD Snooping:
 - Supports max. 32 MLD Snooping groups - Supports 32 static MLD groups per device
- 802.1D Spanning Tree
- 802.1w Rapid Spanning Tree
- 802.1s MSTP
- Loopback Detection
- 802.3ad Link Aggregation:
- Port mirroring
- SNTP
- LLDP/LLDP-MED
- IPv6 neighbor Discovery (ND): Supports 128 dynamic + static ND entries
- L2 Multicast Filtering

L3 Features

- ARP:
- Max 4K ARP entries
 - Support 384 static ARP entries
- Support 4 IPv4 and 4 IPv6 interfaces
- Support IPv6 Neighbor Discovery:
 - Max 128 ND entries
 - Support up to 128 static ND entries
- Max. 124 IPv4 and 50 IPv6 static route entries
- Supports default route backup entry
- Max. 384 IPv4 and 128 IPv6 host route

<u>VLAN</u>

- 802.1Q VLAN standard (VLAN Tagging)
- Up to 256 static VLAN groups
- Asymmetric VLAN
- Management VLAN
- Auto Voice VLAN
- Auto Surveillance VLAN 2.0

QoS (Quality of Service)

- Priority queue mapping by :
 - 802.1p
 - DSCP
 - ToS
 - TCP/UDP port number
 - IPv6 traffic class
- Up to 8 queues per port
- Supports Strict in queue handling

Bandwidth Control

<u>AAA</u>

- 802.1X port-based access control
- Support RADIUS server

<u>ACL</u>

- Max 50 ingress ACL access-list
- Ingress ACL rules: 768 rules (each rule can be associated to a single port or multiple ports)
- Support different ACL policy packet contents:
 - 802.1p priority
 - VLAN
 - MAC address
 - Ethernet Type
 - IPv4/IPv6 address
 - DSCP
 - Protocol type
 - TCP/UDP port number
 - IPv6 Traffic class

Security

- Trusted Host
- Port Security: Support 64 MAC addresses per port
- Traffic Segmentation
- D-Link Safeguard Engine
- Broadcast Storm Control
- ARP Spoofing Prevention: Supports max 127 entries
- DHCP Server Screening: Able to configure 4 IP addresses for DHCP server.
- SSL/TLS: Support v1/v2/v3, TLS1.2
- Smart Binding
 - Support manual configuration and scanning for binding.
 - Supports ARP packet inspection as default, ARP and IP packet inspection as an option.
 - Supports DHCP Snooping

<u>OAM</u>

- Cable Diagnostics
- Reset button (reset to factory default)

<u>Management</u>

- Web-based GUI or D-Link Network Assistant (DNA)
- D-Link CLI style
- SNMP support
- DHCP client

- Trap setting for destination IP, system events, fiber port events, twisted-pair port events
- Password access control
- Web-based configuration backup / restoration
- Web-based firmware backup/restore
- Firmware upgrade using D-Link Network Assistant (DNA) & Web-based management
- Reset, Reboot
- Surveillance Mode

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 C – 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).

