



DGS-1210 Series

MANUAL SMART MANAGED SWITCH

Ver. 6.11



Table of Contents

Table of Contents	i
About This Guide	1
Terms/Usage.....	1
Copyright and Trademarks	1
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	9
Rear Panel.....	10
DGS-1210-28MP.....	10
Front Panel	10
Rear Panel.....	11
DGS-1210-52	11
Front Panel	11
Rear Panel.....	12
DGS-1210-52MP.....	12
Front Panel	12
Rear Panel.....	13
LED Indicators.....	13
2 Hardware Installation	16
Safety Cautions.....	16
Step 1: Unpacking.....	17
Step 2: Switch Installation	17
Desktop or Shelf Installation.....	17
Rack Installation	17
Step 3: Plugging in the AC Power Cord with Power Cord Clip	18
Power Failure	21
Grounding the Switch	21
3 Getting Started	22
Management Options.....	22

Using Web-based Management	22
Supported Web Browsers	22
Connecting to the Switch.....	22
Login Web-based Management.....	22
Smart Wizard	23
Web-based Management.....	23
D-Link Network Assistant.....	23
4 Web-based Switch Configuration	24
Smart Wizard Configuration.....	24
Step 1 – Web Mode.....	24
Step 2 – IP Information.....	25
Step 3 – Password	26
Step 4 – SNMP (Only for Standard Mode).....	26
Web-based Management.....	28
Tool Bar > Save Menu	29
Save Configuration.....	29
Save Log	29
Tool Bar > Tools Menu.....	29
Reset	29
Reset System	29
Reboot Device	30
Configuration Backup and Restore	30
Firmware Backup and Upgrade.....	31
Flash Information.....	31
Tool Bar > Wizard	31
Tool Bar > Online Help.....	32
Tool Bar > Surveillance Mode.....	32
Function Tree	33
Device Information.....	33
System > System Settings	34
System > Password.....	35
System > Port Settings.....	36
System > Port Description.....	36
System > DHCP Auto Configuration	37
System > DHCP Relay > DHCP Relay Global Settings.....	37
System > DHCP Relay > DHCP Relay Interface Settings	38
System > DHCP Local Relay Settings	39
System > DHCPv6 Relay Settings	39
System > System Log Configuration > System Log Settings	40
System > System Log Configuration > SysLog Host	41
System > Time Profile	41
System > Power Saving	42
System > IEEE802.3az EEE Settings	42
System > D-Link Discover Protocol Settings.....	43
System > Firmware Information	44
System > Configuration Information.....	44
VLAN > 802.1Q VLAN	44
VLAN > 802.1Q VLAN PVID	46
VLAN > Voice VLAN > Voice VLAN Global Settings	47

VLAN > Voice VLAN > Voice VLAN Port Settings	48
VLAN > Voice VLAN > Voice Device List.....	49
VLAN > Auto Surveillance VLAN > Auto Surveillance Properties.....	49
VLAN > Auto Surveillance VLAN > MAC Settings and Surveillance Device	50
VLAN > Auto Surveillance VLAN > ONVIF IPC Information	51
VLAN > Auto Surveillance VLAN > ONVIF NVR Information.....	51
L2 Functions > Jumbo Frame.....	51
L2 Functions > Port Mirroring	51
L2 Functions > Loopback Detection.....	52
L2 Functions > MAC Address Table > Static MAC	53
L2 Functions > MAC Address Table > Dynamic Forwarding Table	54
L2 Functions > Spanning Tree > STP Bridge Global Settings	54
L2 Functions > Spanning Tree > STP Port Settings	56
L2 Functions > Spanning Tree > MST Configuration Identification	57
L2 Functions > Spanning Tree > STP Instance Settings	58
L2 Functions > Spanning Tree > MSTP Port Information	58
L2 Functions > Link Aggregation > Port Trunking.....	59
L2 Functions > Link Aggregation > LACP Port Settings	59
L2 Functions > Multicast > IGMP Snooping	60
L2 Functions > Multicast > MLD Snooping	62
L2 Functions > Multicast > Multicast Forwarding	63
L2 Functions > Multicast > Multicast Filtering Mode	64
L2 Functions > SNTP > Time Settings	64
L2 Functions > SNTP > TimeZone Settings.....	65
L2 Functions > LLDP > LLDP Global Settings	66
L2 Functions > LLDP > LLDP-MED Settings	66
L2 Functions > LLDP > LLDP Port Settings	67
L2 Functions > LLDP > 802.1 Extension TLV	68
L2 Functions > LLDP > 802.3 Extension TLV	68
L2 Functions > LLDP > LLDP Management Address Settings	69
L2 Functions > LLDP > LLDP Management Address Table	70
L2 Functions > LLDP > LLDP Local Port Table	70
L2 Functions > LLDP > LLDP Remote Port Table	72
L2 Functions > LLDP > LLDP Statistics	74
L3 Functions > IP Interface	75
L3 Functions > IPv6 Neighbor Settings.....	77
L3 Functions > IPv4 Static Route	77
L3 Functions > IPv4 Routing Table Finder.....	79
L3 Functions > IPv6 Static Route	79
L3 Functions > IPv6 Routing Table Finder.....	79
L3 Functions > ARP > ARP Table Global Settings	80
L3 Functions > ARP > Static ARP Settings.....	81
QoS > Bandwidth Control.....	81
QoS > 802.1p/DSCP/ToS.....	82
Security > Trusted Host.....	82
Security > Port Security.....	83
Security > Traffic Segmentation	84
Security > Safeguard Engine.....	84
Security > Storm Control	84

Security > ARP Spoofing Prevention	85
Security > DHCP Server Screening	86
Security > SSL/TLS	86
Security > DoS Prevention Settings	88
Security > SSH > SSH Settings	89
Security > SSH > SSH Authmode and Algorithm Settings.....	89
Security > SSH > SSH User Authentication Lists	90
Security > Smart Binding > Smart Binding Settings.....	91
Security > Smart Binding > Smart Binding	92
Security > Smart Binding > White List.....	92
Security > Smart Binding > Black List	93
AAA > RADIUS Server	93
AAA > 802.1X > 802.1X Global Settings.....	94
AAA > 802.1X > 802.1X Port Settings.....	94
AAA > 802.1X > 802.1X User.....	96
ACL > ACL Wizard	96
ACL > ACL Access List	110
ACL > ACL Access Group.....	111
ACL > ACL Hardware Resource Status	112
PoE > PoE Global Settings (only for DGS-1210-10P/10MP/28P/28MP/52MP)	112
PoE > PoE Port Settings (only for DGS-1210-10P/10MP/28P/28MP/52MP)	113
SNMP > SNMP > SNMP Global Settings	115
SNMP > SNMP > SNMP User	116
SNMP > SNMP > SNMP Group Table	116
SNMP > SNMP > SNMP View	117
SNMP > SNMP > SNMP Community.....	118
SNMP > SNMP > SNMP Host.....	118
SNMP > SNMP > SNMP Engine ID	118
SNMP > RMON > RMON Global Settings	118
SNMP > RMON > RMON Statistics	119
SNMP > RMON > RMON History.....	119
SNMP > RMON > RMON Alarm	120
SNMP > RMON > RMON Event.....	120
Monitoring > Port Statistics.....	121
Monitoring > Cable Diagnostics	122
Monitoring > System Log.....	123
5 Surveillance Mode Configuration	124
Web User Interface	124
Surveillance Overview.....	125
Surveillance Topology	126
Device Information.....	127
Port Information	128
IP-Camera Information	128
NVR Information	128
PoE Information.....	129
PoE Scheduling	129
Time > Clock Settings	130
Time > SNTP Settings.....	130
Surveillance Settings	131

Surveillance Log	133
Health Diagnostic	133
Tool Bar > Wizard	134
Tool Bar > Tools Menu.....	134
Reset System	134
Reboot Device	135
Configuration Backup & Restore	135
Firmware Backup and Upgrade.....	136
Firmware Information.....	136
Flash Information.....	137
Tool Bar > Save	137
Tool Bar > Help	137
Tool Bar > Online Help.....	138
Tool Bar > Standard Mode.....	138
6 Command Line Interface.....	139
To connect a switch via TELNET:.....	139
Logging on to the Command Line Interface:.....	139
CLI Commands:	139
?	140
download	141
upload.....	142
config firmware	143
config configuration	143
config ipif system.....	144
config ipif system.....	144
logout.....	145
ping.....	145
ping6.....	146
reboot	146
reset config	147
show boot_file.....	147
show firmware information	147
show flash information.....	148
show ipif.....	149
show switch	149
show route	150
config account admin password	150
save	151
debug info	151
Appendix A - Ethernet Technology.....	153
Gigabit Ethernet Technology	153
Fast Ethernet Technology	153
Switching Technology	153
Appendix B - Technical Specifications	154
Hardware Specifications	154
Features	158
L2 Features	158
L3 Features	158
VLAN	158

QoS (Quality of Service).....	158
Security.....	158
OAM	159
Management.....	159
D-Link Green Technology	159
Appendix C – Rack mount Instructions	160

About This Guide

This guide provides instructions to install the D-Link Smart Managed 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.



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

Copyright and Trademarks

Information in this document is subjected to change without notice.

© 2017 D-Link Corporation. All rights reserved.

Reproduction in any manner 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 Smart Managed Switch Products.

D-Link's next generation Smart Managed 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 Smart Managed Switch series. It provides 8, 16, 24 or 48 10/100/1000Mbps Non-PoE or PoE ports plus 4 Combo GE/SFP ports. All switches of the DGS-1210 series feature embedded 4 gigabit SFP uplinks, which provides flexible network topology choices such as ring, tree, or mixed.

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 video traffic from pre-defined IP surveillance devices to an assigned VLAN with higher priority, so it can be separated from normal data traffic. Asymmetric VLAN is implemented in these switches for a more efficient use of shared resources, such as server or gateway devices.

Network Security. D-Link's innovative Safeguard Engine function protects the switches against traffic flooding caused by virus attacks. 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 Smart Managed 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 Smart Managed 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 Smart Managed 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) Smart Managed Switch.

Front Panel

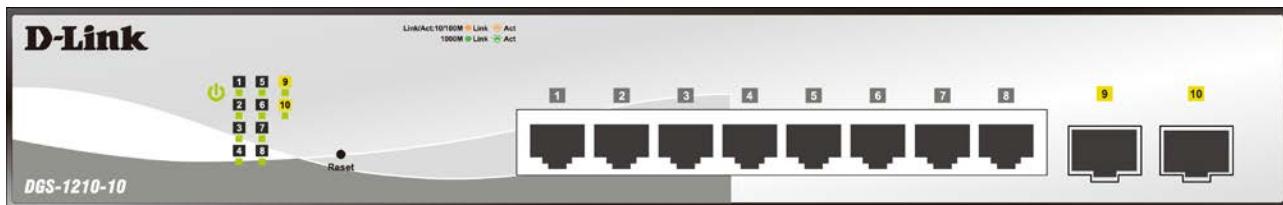


Figure 1.1 – DGS-1210-10 Front Panel

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

- **Power LED**: 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.



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 (Version 2.0.2.4 only) to download the firmware or call D-Link Technical Support for further help. (No support by DNA(Chrome) 3.0.x.x) and DNA 4.x.x.x). For DNA information, please visit below site <http://tools.dlink.com/intro/dna/>

Rear Panel



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) Smart Managed PoE Switch.

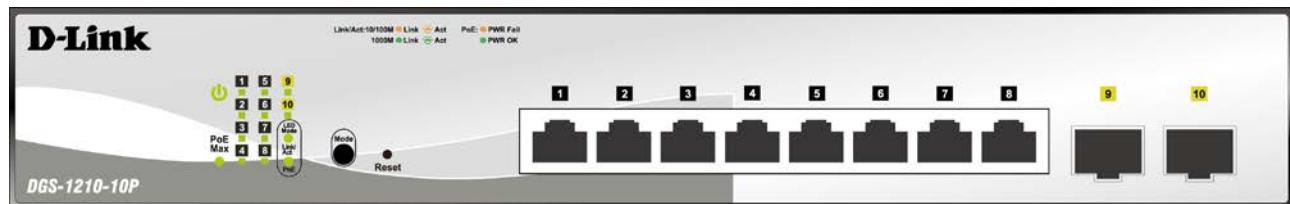
Front Panel

Figure 1.3 – DGS-1210-10P Front Panel

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

- **Power LED**: The Power LED lights up when the Switch is connected to a power source.
- **PoE Max**: The PoE Max LED lights up with solid red when 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.
- **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.
- **LED Mode**: To select the mode of port LED, the Link/Act and PoE LED under the mode button will solid green to indicate which mode is selected.
- **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.



CAUTION: 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.



NOTE: Once user enter in Loader mode, you can use DNA tool (Version 2.0.2.4 only) to download the firmware or call D-Link Technical Support for further help. (No support by DNA (Chrome) 3.0.x.x) and DNA 4.0.x.x). For DNA information, please visit below site <http://tools.dlink.com/intro/dna/>

Rear Panel

Figure 1.4 – DGS-1210-10P Rear Panel

Power: Connect the supplied DC external power 54V/1.574A cable to this port.

DGS-1210-10MP

8-Port 10/100/1000Mbps plus 2 SFP Ports (100/1000Mbps) Smart Managed PoE Switch.

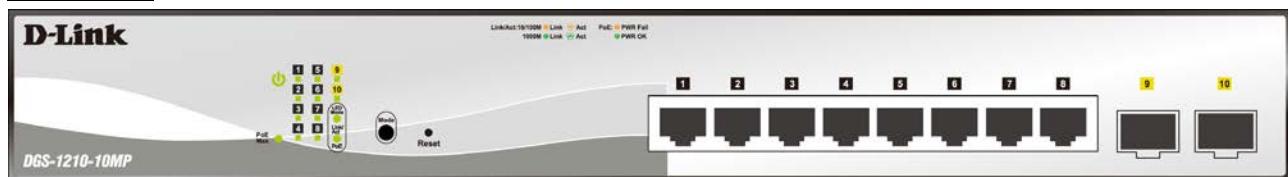
Front Panel

Figure 1.5 – DGS-1210-10MP Front Panel

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

- **Power LED**: The Power LED lights up when the Switch is connected to a power source.
- **PoE Max**: The PoE Max LED lights up with solid red when 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.
- **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.
- **LED Mode**: To select the mode of port LED, the Link/Act and PoE LED under the mode button will solid green to indicate which mode is selected.
- **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.



CAUTION: 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.



NOTE: Once user enter in Loader mode, you can use DNA tool (Version 2.0.2.4 only) to download the firmware or call D-Link Technical Support for further help. (No support by DNA (Chrome) 3.0.x.x) and DNA 4.x.x.x). For DNA information, please visit below site <http://tools.dlink.com/intro/dna/>

Rear Panel

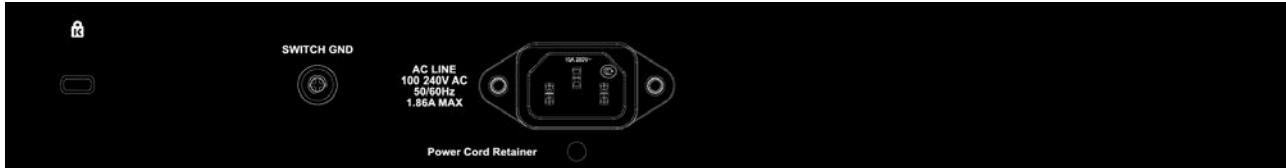


Figure 1.6 – DGS-1210-10MP Rear Panel

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

DGS-1210-20

16-Port 10/100/1000Mbps plus 4 Combo GE/SFP Slot Smart Managed Switch.

Front Panel

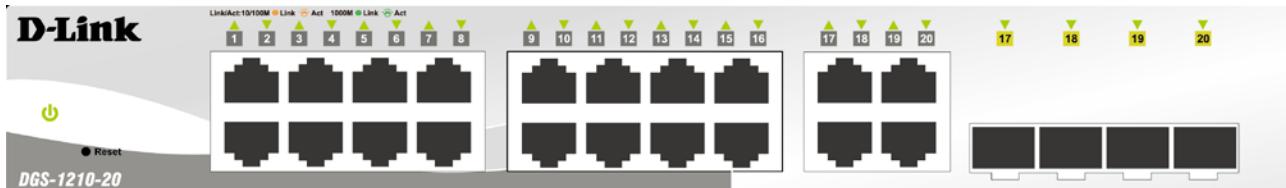


Figure 1.7 – DGS-1210-20 Front Panel

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

- **Power LED**: The Power LED lights up when the Switch is connected to a power source.
- **Port Link/Act/Speed LED (1-16):** The Link/Act/Speed LED flashes, which indicates a network link through the corresponding port. Blinking indicates that the Switch is either sending or receiving data to the port. When a port has an amber light, this indicates that the port is running on 10M or 100M. When it has a green light it is running on 1000M.
- **Port Link/Act/Speed LED (17F, 18F, 19F, 20F, 17T, 18T, 19T, 20T):** 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.



NOTE: On the DGS-1210-20, the MiniGBIC ports are shared with normal RJ-45 ports 17T, 18T, 19T and 20T. When the MiniGBIC port is used, the RJ-45 port cannot be used.



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 (Version 2.0.2.4 only) to download the firmware or call D-Link Technical Support for further help. (No support by DNA (Chrome) 3.0.x.x) and DNA 4.x.x). For DNA information, please visit below site <http://tools.dlink.com/intro/dna/>

Rear Panel

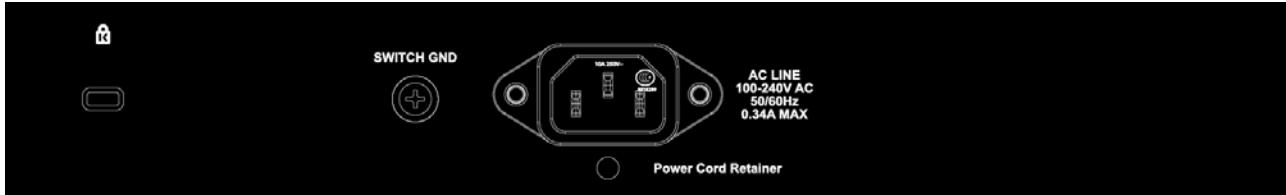


Figure 1.8 – DGS-1210-20 Rear Panel

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

DGS-1210-26

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

Front Panel



Figure 1.9 – DGS-1210-26 Front Panel

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

- Power LED**: 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 (Version 2.0.2.4 only) to download the firmware or call D-Link

Technical Support for further help. (No support by DNA (Chrome) 3.0.x.x) and DNA 4.x.x.x). For DNA information, please visit below site <http://tools.dlink.com/intro/dna/>

Rear Panel



Figure 1.10 – DGS-1210-26 Rear Panel

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

DGS-1210-28

24-Port 10/100/1000Mbps plus 4 Combo GE/SFP Slot Smart Managed Switch.

Front Panel

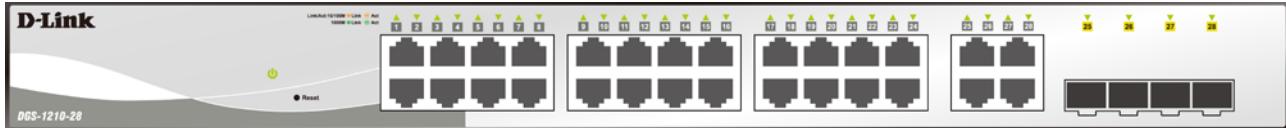


Figure 1.11 – DGS-1210-28 Front Panel

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

- **Power LED** : 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, 27F, 28F, 25T, 26T, 27T, 28T):** 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.



NOTE: On the DGS-1210-28, the MiniGBIC ports are shared with normal RJ-45 ports 25T, 26T, 27T and 28T. When the MiniGBIC port is used, the RJ-45 port cannot be used.



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 (Version 2.0.2.4 only) to download the firmware or call D-Link Technical Support for further help. (No support by DNA (Chrome) 3.0.x.x) and DNA 4.x.x.x) . For DNA information, please visit below site <http://tools.dlink.com/intro/dna/>

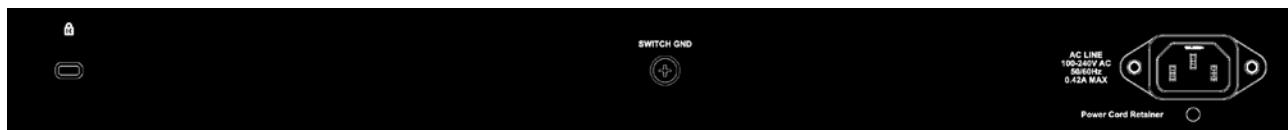
Rear Panel

Figure 1.12 – DGS-1210-28 Rear Panel

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

DGS-1210-28P

24-Port 10/100/1000Mbps plus 4 Combo GE/SFP Smart Managed PoE Switch.

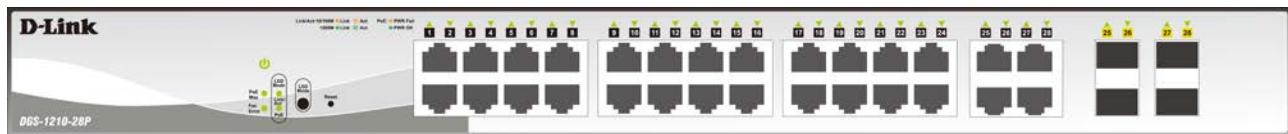
Front Panel

Figure 1.13 – DGS-1210-28P Front Panel

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

- **Power LED**: 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 PoE Max LED lights up with solid red when 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 193 Watts.
- **LED Mode**: To select the mode of port LED, the Link/Act and PoE LED under the mode button will solid green to indicate which mode is selected.
- **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, 27F, 28F, 25T, 26T, 27T, 28T)**: 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.
- **LED Mode**: By pressing the Mode button, the Port LED will switch between Link/Act and PoE modes.



NOTE: On the DGS-1210-28P, the MiniGBIC ports are shared with normal RJ-45 ports 25T, 26T, 27T and 28T. When the MiniGBIC port is used, the RJ-45 port cannot be used.



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



CAUTION: The port 1 ~ port 24 are PoE ports. When user press the **Mode** button to PoE mode, only port 1 ~ port 24 will light up.



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



NOTE: Once user enter in Loader mode, you can use DNA tool (Version 2.0.2.4 only) to download the firmware or call D-Link Technical Support for further help. (No support by DNA (Chrome) 3.0.x.x) and DNA 4.x.x). For DNA information, please visit below site <http://tools.dlink.com/intro/dna/>

Rear Panel

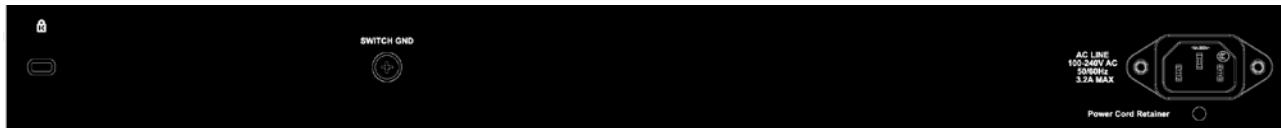


Figure 1.14 – DGS-1210-28P Rear Panel

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

DGS-1210-28MP

24-Port 10/100/1000Mbps plus 4 combo GE/SFP Slot Smart Managed PoE Switch.

Front Panel

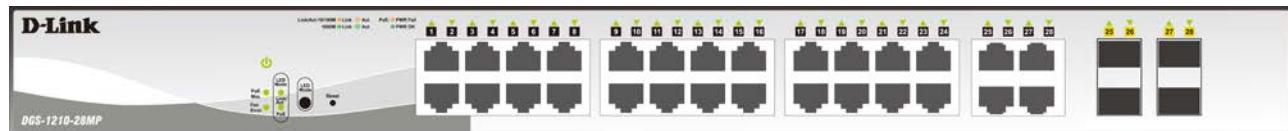


Figure 1.15 – DGS-1210-28MP Front Panel

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

- **Power LED**: 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 PoE Max LED lights up with solid red when 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.
- **LED Mode**: To select the mode of port LED, the Link/Act and PoE LED under the mode button will solid green to indicate which mode is selected.
- **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, 27F, 28F, 25T, 26T, 27T, 28T)**: 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.

- **LED Mode:** By pressing the Mode button, the Port LED will switch between Link/Act and PoE modes.



NOTE: On the DGS-1210-28MP, the MiniGBIC ports are shared with normal RJ-45 ports 25T, 26T, 27T and 28T. When the MiniGBIC port is used, the RJ-45 port cannot be used.



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



CAUTION: The port 1 ~ port 24 are PoE ports. When user press the **Mode** button to PoE mode, only port 1 ~ port 24 will light up.



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



NOTE: Once user enter in Loader mode, you can use DNA tool (Version 2.0.2.4 only) to download the firmware or call D-Link Technical Support for further help. (No support by DNA (Chrome) 3.0.x.x) and DNA 4.x.x.x). For DNA information, please visit below site <http://tools.dlink.com/intro/dna/>

Rear Panel

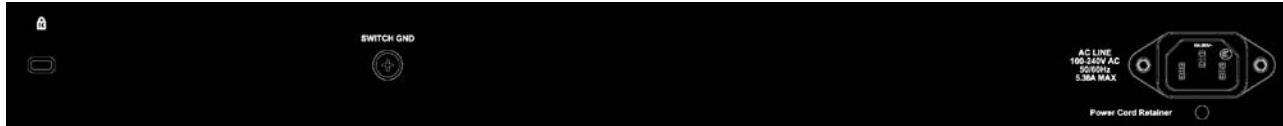


Figure 1.16 – DGS-1210-28MP Rear Panel

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

DGS-1210-52

48-Port 10/100/1000Mbps plus 4 Combo GE/SFP Slot Smart Managed Switch.

Front Panel

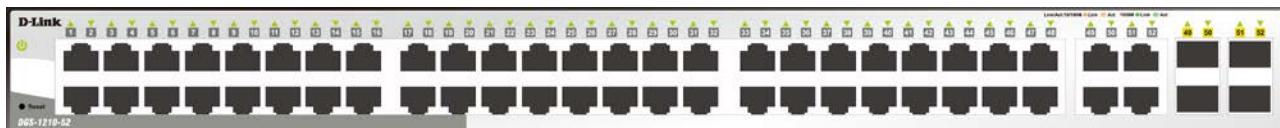


Figure 1.17 – DGS-1210-52 Front Panel

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

- **Power LED** : The Power LED lights up when the Switch is connected to a power source.
- **Port Link/Act/Speed LED (1-48):** 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, 50F, 51F, 52F, 49T, 50T, 51T, 52T):** 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.



NOTE: On the DGS-1210-52, the MiniGBIC ports are shared with normal RJ-45 ports 49T, 50T, 51T and 52T. When the MiniGBIC port is used, the RJ-45 port cannot be used.



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 (Version 2.0.2.4 only) to download the firmware or call D-Link Technical Support for further help. (No support by DNA (Chrome) 3.0.x.x) and DNA 4.x.x.x). For DNA information, please visit below site <http://tools.dlink.com/intro/dna/>.

Rear Panel



Figure 1.18 – DGS-1210-52 Rear Panel

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

DGS-1210-52MP

48-Port 10/100/1000Mbps plus 4 Combo GE/SFP Smart Managed PoE Switch.

Front Panel

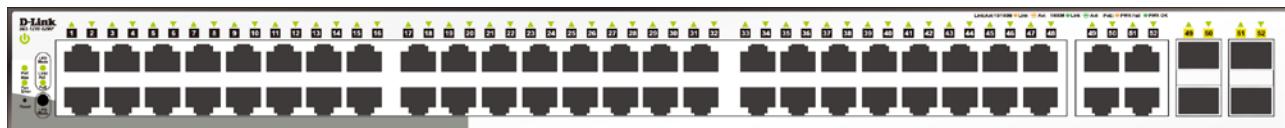


Figure 1.19 – DGS-1210-52MP Front Panel

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

- **Power LED**: 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 PoE Max LED lights up with solid red when 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.
- **LED Mode**: To select the mode of port LED, the Link/Act and PoE LED under the mode button will solid green to indicate which mode is selected.
- **Port Link/Act/Speed LED (1-48)**: 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, 50F, 51F, 52F, 49T, 50T, 51T, 52T):** 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.
- LED Mode:** By pressing the Mode button, the Port LED will switch between Link/Act and PoE modes.



NOTE: On the DGS-1210-52MP, the MiniGBIC ports are shared with normal RJ-45 ports 49T, 50T, 51T and 52T. When the MiniGBIC port is used, the RJ-45 port cannot be used.



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



CAUTION: The port 1 ~ port 48 are PoE ports. When user press the **Mode** button to PoE mode, only port 1 ~ port 48 will light up.



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



NOTE: Once user enter in Loader mode, you can use DNA tool (Version 2.0.2.4 only) to download the firmware or call D-Link Technical Support for further help. (No support by DNA (Chrome) 3.0.x.x) and DNA 4.x.x.x). For DNA information, please visit below site <http://tools.dlink.com/intro/dna/>.

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 Smart Managed Switch along with an explanation of each indicator.

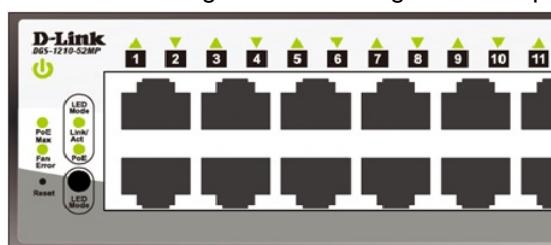


Figure 1.21 –LED Indicators on DGS-1210 series

Location	LED Indicative	Color	Status	Description
Per Device	Power	Green	Solid Light	Power on.
			Light off	Power off.
	Fan Error (For DGS-1210-28P/28MP/52MP)	Red	Solid light	The fan has runtime failure and is brought offline.
	PoE Max. (For DGS-1210-10P/10MP/28P/28MP/52MP)	Amber	Solid light	The PoE Max LED lights up when the total PoE output of Switch reached or exceeded 65 Watts for DGS-1210-10P, 130 Watts for DGS-1210-10MP, 193 Watts for DGS-1210-28P, and 370 Watts for DGS-1210-28MP/52MP. 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.
	Link/Act	Green/Amber	Solid Green	When there is a secure 1000Mbps Ethernet connection (or link) at any of the ports.
			Blinking Green	When there is reception or transmission (i.e. Activity—Act) of data occurring at a 1000Mbps Ethernet connected port.
			Solid Amber	When there is a secure 10/100Mbps 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 10/100Mbps Ethernet connected port.
			Light off	No link.
LED Per 10/100/1000Mbps Copper Port	PoE Mode	Green	Solid Light	Power feeding.
		Amber	Solid Light	Error Condition.
		Off	Solid Off	No Power feeding.
	Link/Act	Green/Amber	Solid Green	When there is a secure 1000Mbps Ethernet connection (or link) at any of the ports.
			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	Link/Act	Green/Amber	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 Smart Managed 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 Smart Managed Switch
- One Multilingual Getting Started Guide
- User Guide CD
- Power cord and Power Cord Retainer or external power adapter(DGS-1210-10P only)
- 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.

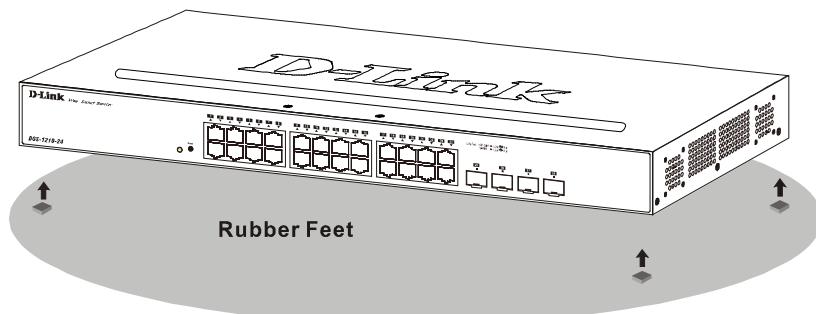


Figure 2.1 – Attach the adhesive rubber pads to the bottom

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).

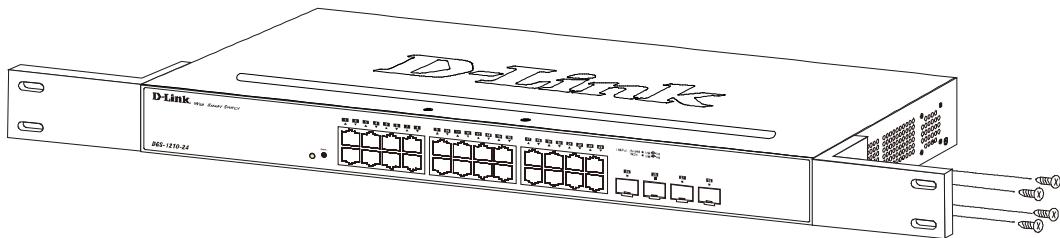


Figure 2.2 – Attach the mounting brackets to the Switch

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

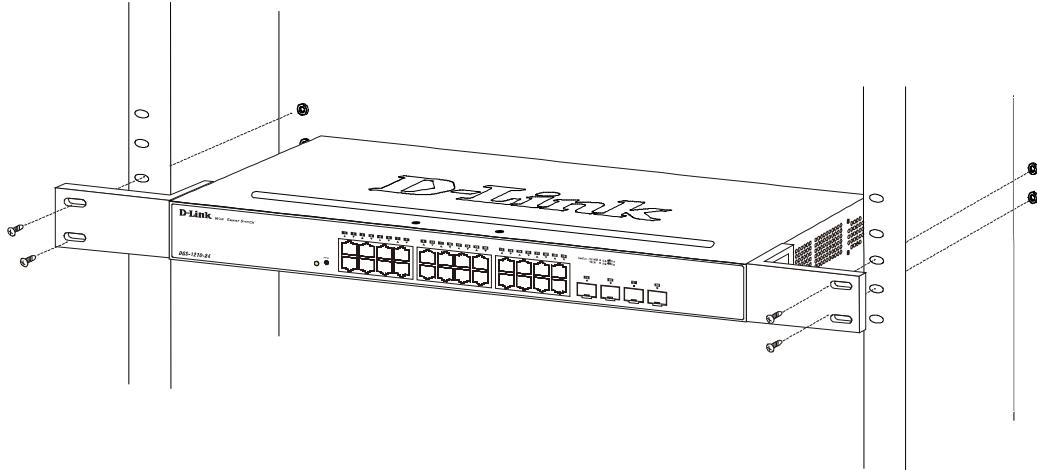


Figure 2.3 – Mount the Switch in the rack or chassis

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 (T_{ma}) specified by the manufacturer.
- B) Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
- C) Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- D) Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit, and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- E) Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips)."

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

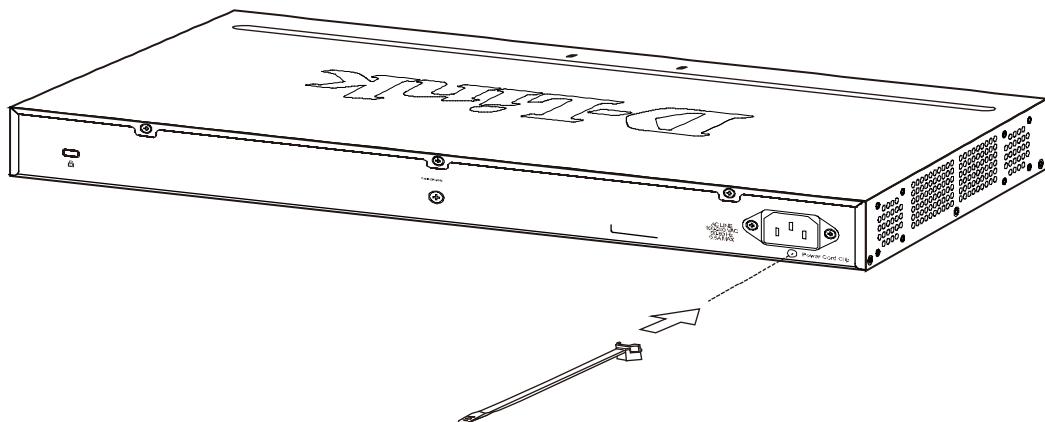


Figure 2.4 – Insert Tie Wrap to the Switch

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

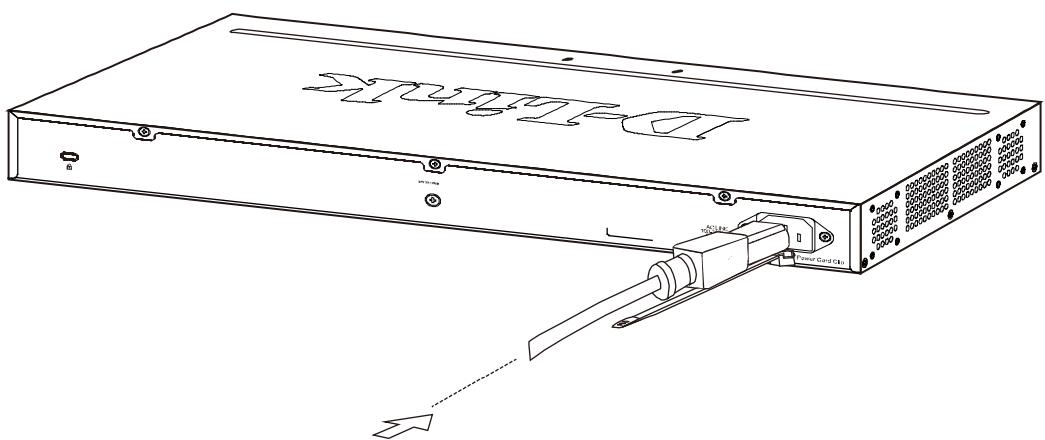


Figure 2.5 – Connect the power cord to the Switch

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

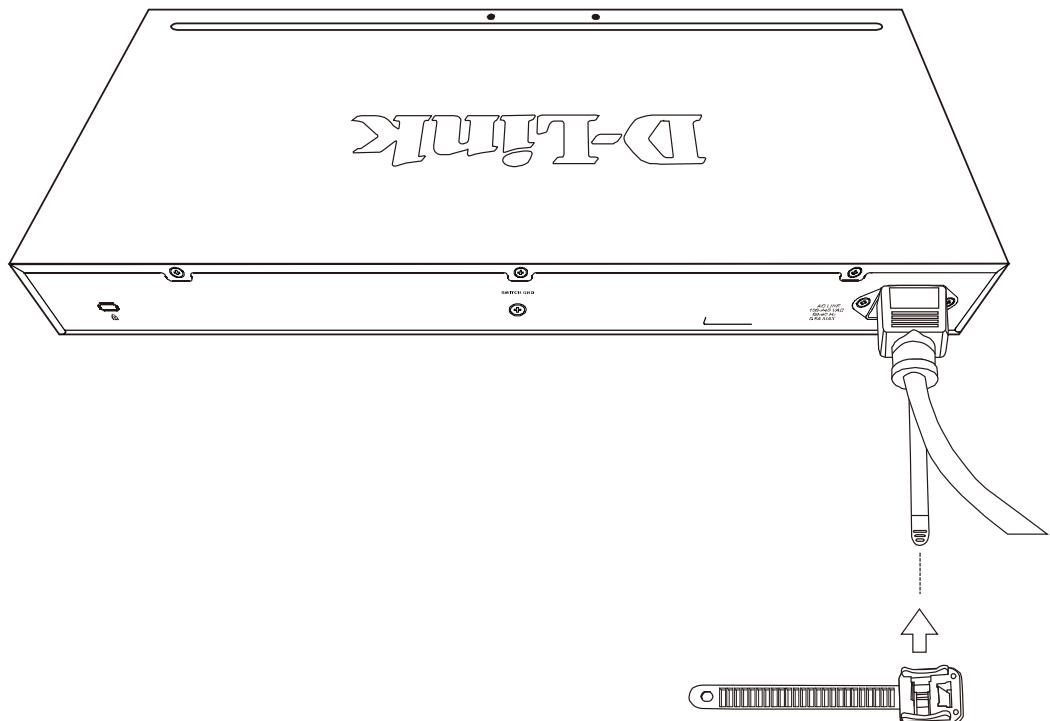


Figure 2.6 – Slide the Retainer through the Tie Wrap

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

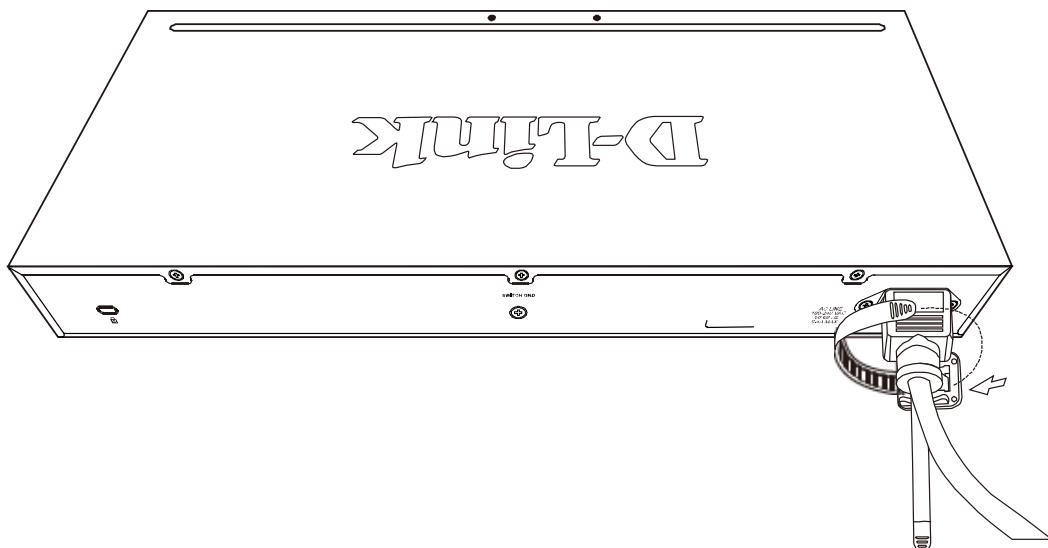


Figure 2.7 – Circle around the power cord

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

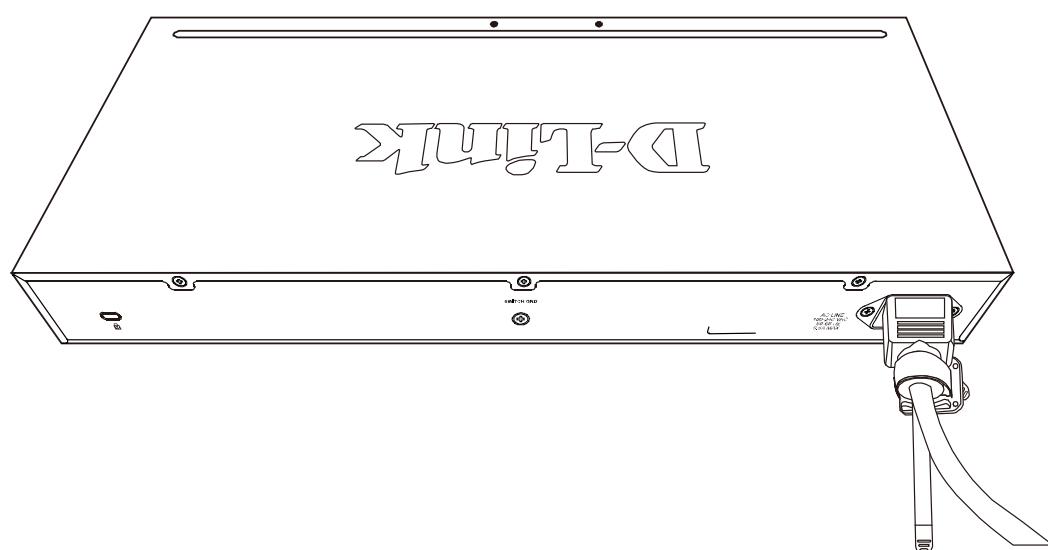


Figure 2.8 – Secure the power cord

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

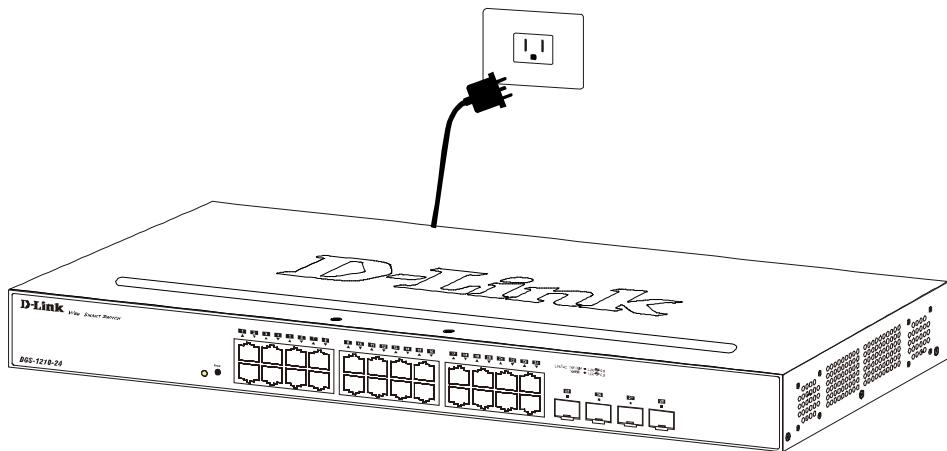


Figure 2.9 – Plugging the switch into an outlet

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.

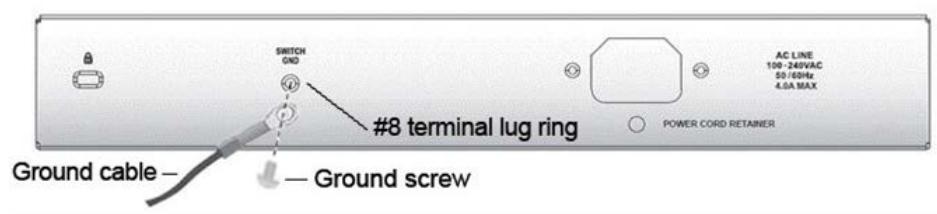


Figure 2.10 – Connect a Grounding Cable

3 Getting Started

This chapter introduces the management interface of D-Link Smart Managed Switch.

Management Options

The D-Link Smart Managed 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.

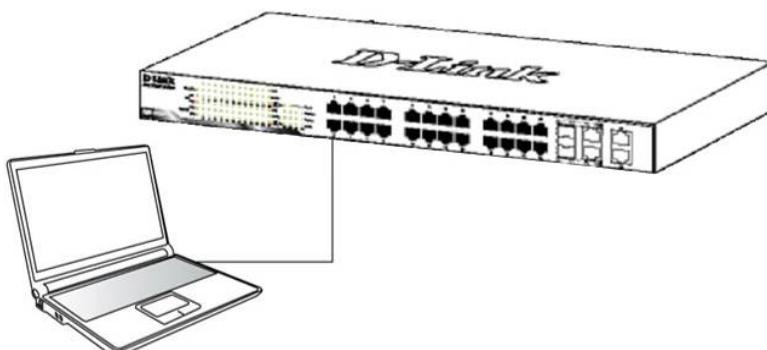


Figure 3.1 – Connected Ethernet cable

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 ~ 254 and z is a number between 1 ~ 254), and a subnet mask of **255.0.0.0**. There are two ways to launch the Web-based Management, 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>.



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 Web-based Management interface then click **OK**.

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



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 Smart Managed 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 [Web-based Switch Configuration](#) 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 <http://tools.dlink.com/intro/dna/>. Please go to above link for details.

4 Web-based Switch Configuration

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

Smart Wizard Configuration

The Smart Wizard is a configuration utility that is launched the first time the Web UI is accessed. It allows users to configure basic settings such as the switch mode, management IP, password and SNMP. It can also be used to switch between **Standard Mode** and **Surveillance Mode** Web UI types.

Standard Mode is used to manage the network and system elements of the switch. Surveillance Mode is a dedicated user interface designed for monitoring and managing the surveillance and IP security device on your network.

To switch between the two types of interfaces, you can re-run the Smart Wizard that is presented when you access the web interface of the device.

Step 1 – Web Mode

After a successful login, the Smart Wizard will guide you through essential settings of the D-Link Smart Managed Switch. The initial page allows the user to choose between **Standard Mode** and **Surveillance Mode** on the switch. This can be changed at any time by returning to the Smart Wizard.

If you do not plan to change anything, click **Exit** to leave the Wizard and enter the Web Interface. You can also skip it by clicking **Ignore the Wizard next time** for the next time you logon to the Web-based Management.

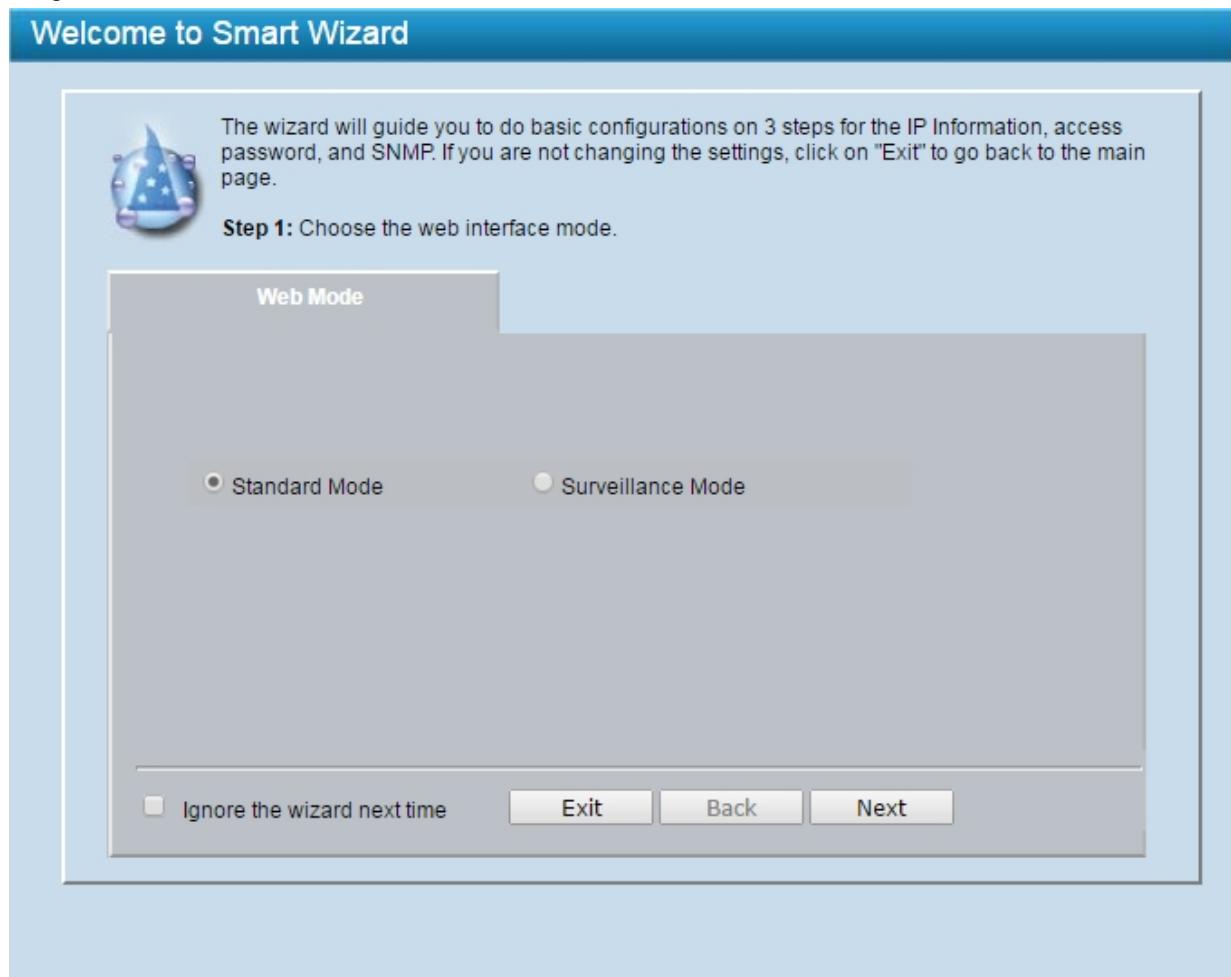


Figure 4.1 – Web Mode in Smart Wizard

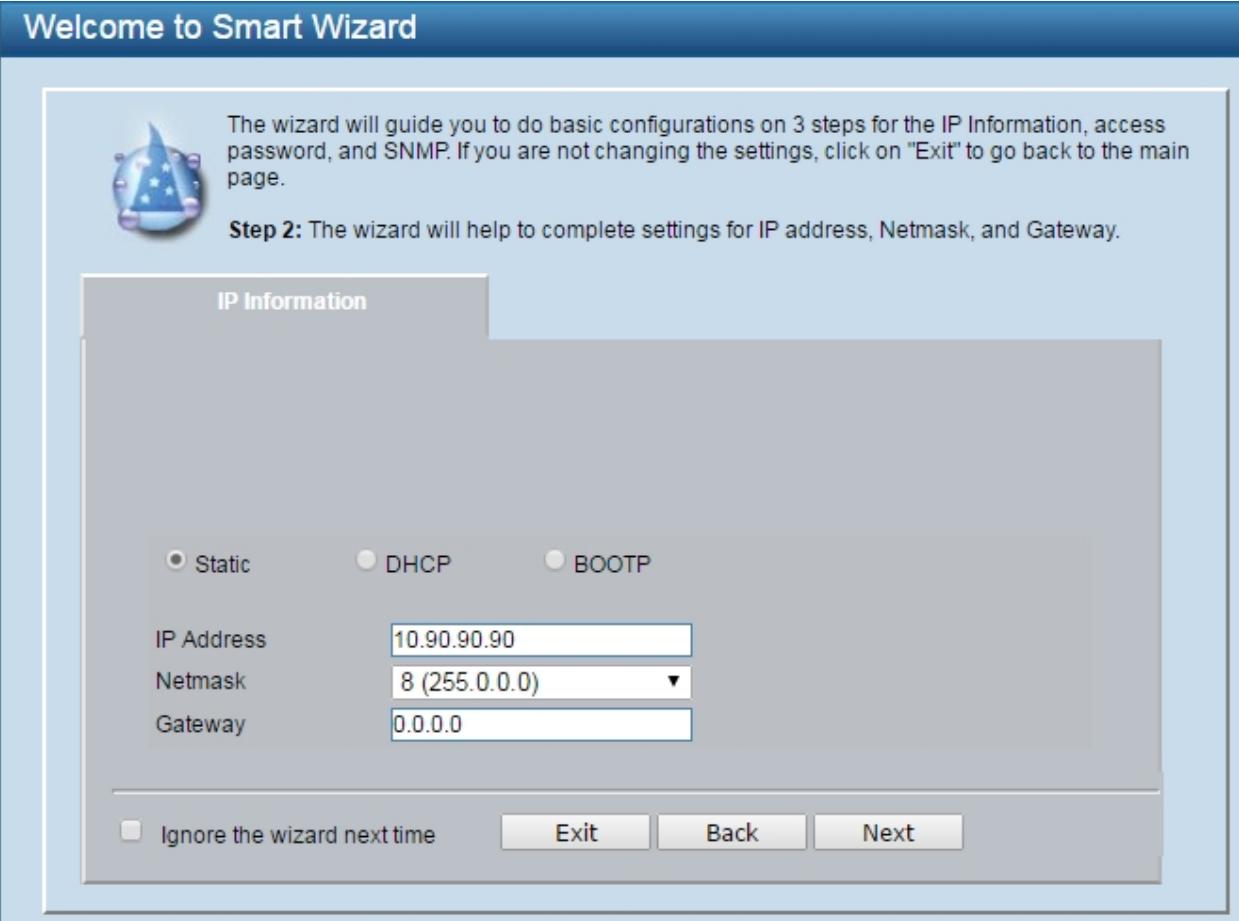
The fields that can be configured are described below:

Item	Description
Web Mode	Select the Standard Mode to continue the following settings or select the Surveillance Mode to continue the Smart Wizard in Surveillance Mode.

Click **Next** to enter the next configuration page.

Step 2 – IP Information

The IP Information page allows the user to configure IP address assignment method, the static IP address, netmask and gateway address.



The screenshot shows the "Welcome to Smart Wizard" interface. A blue header bar at the top has the title "Welcome to Smart Wizard". Below it is a main content area with a light blue background. On the left, there's a small icon of a blue star with a face. To its right, a text box contains the following message: "The wizard will guide you to do basic configurations on 3 steps for the IP Information, access password, and SNMP. If you are not changing the settings, click on "Exit" to go back to the main page." Below this message, another text box says "Step 2: The wizard will help to complete settings for IP address, Netmask, and Gateway." A large rectangular input field is labeled "IP Information". Inside this field, there are three radio buttons for IP address assignment: "Static" (selected), "DHCP", and "BOOTP". Below these are three input boxes: "IP Address" containing "10.90.90.90", "Netmask" containing "8 (255.0.0.0)", and "Gateway" containing "0.0.0.0". At the bottom of the "IP Information" field, there is a checkbox labeled "Ignore the wizard next time" followed by three buttons: "Exit", "Back", and "Next".

Figure 4.2 – IP Information in Smart Wizard

The fields that can be configured are described below:

Item	Description
Static	Select Static option to manually configure and use IP address settings on this switch.
DHCP	Select DHCP option to obtain IP address settings from a DHCP server.
IP Address	Specifies the IP address to be configured.
Netmask	Specifies the Netmask to be configured.
Gateway	Specifies the default Gateway IP address to be configured.
BOOTP	Select BOOTP option to be used on the switch.

Click **Next** to enter the next Password setting page.

Tick the **Ignore the wizard next time** option to skip the Smart Wizard on the next login.

-  **NOTE:** The Smart Wizard supports quick settings for IPv4 network.
-  **NOTE:** The switch will probe IP-Cameras every 30 seconds. If an IP-Camera is not in the same subnet as the switch, the IP-Camera will not be automatically discovered. Place the switch management IP in the same subnet as the IP-Cameras for the cameras to be automatically added to the Surveillance Mode Web UI.

Step 3 – Password

Type the desired new password in the **Password** box and again in the **Confirm Password**, then click the **Apply&Save** button to accept the changes made and enter the next **SNMP** setting page. Tick the **Ignore the wizard next time** option to skip the Smart Wizard on the next login.

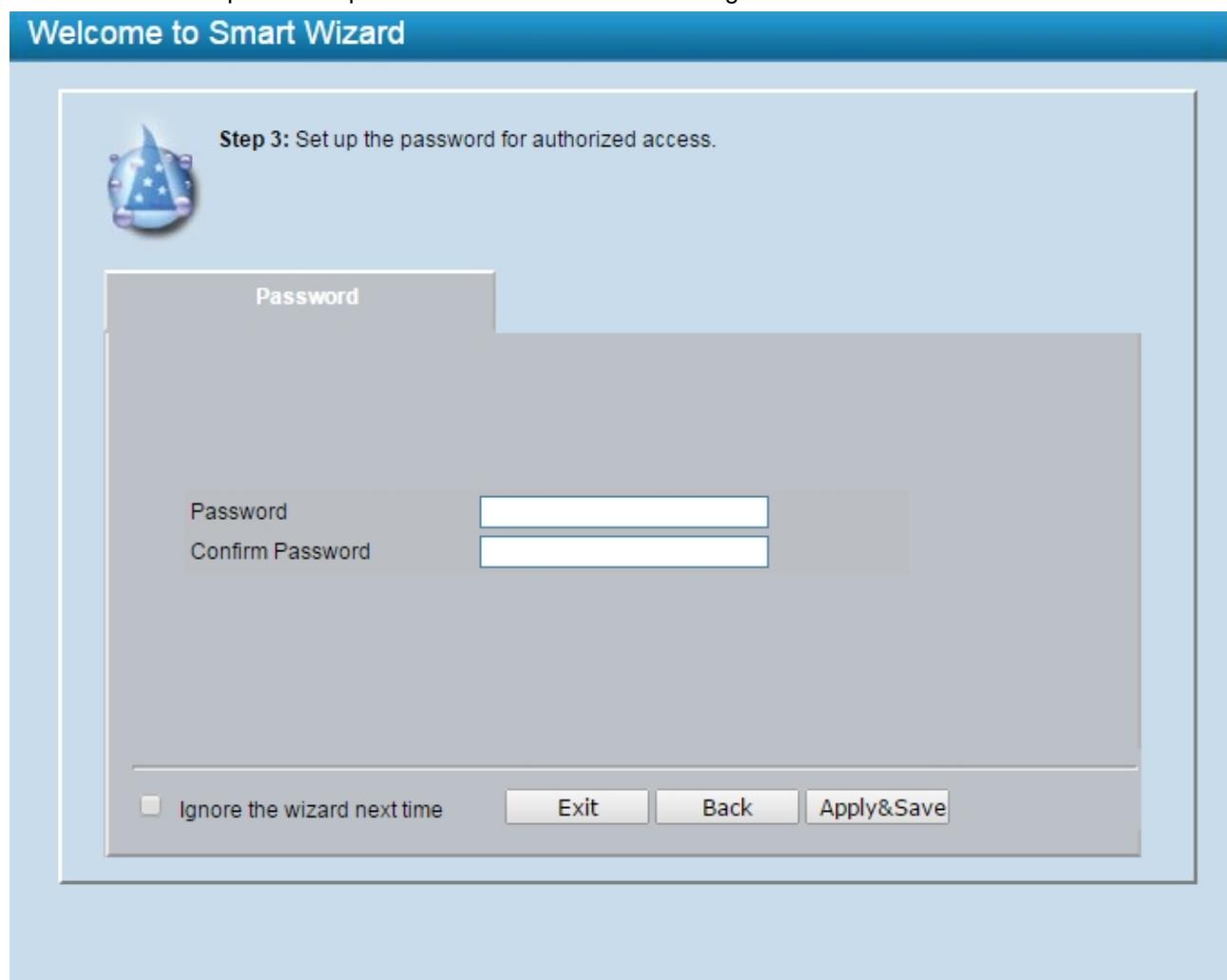


Figure 4.3 – Password in Smart Wizard

Step 4 – SNMP (Only for Standard Mode)

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

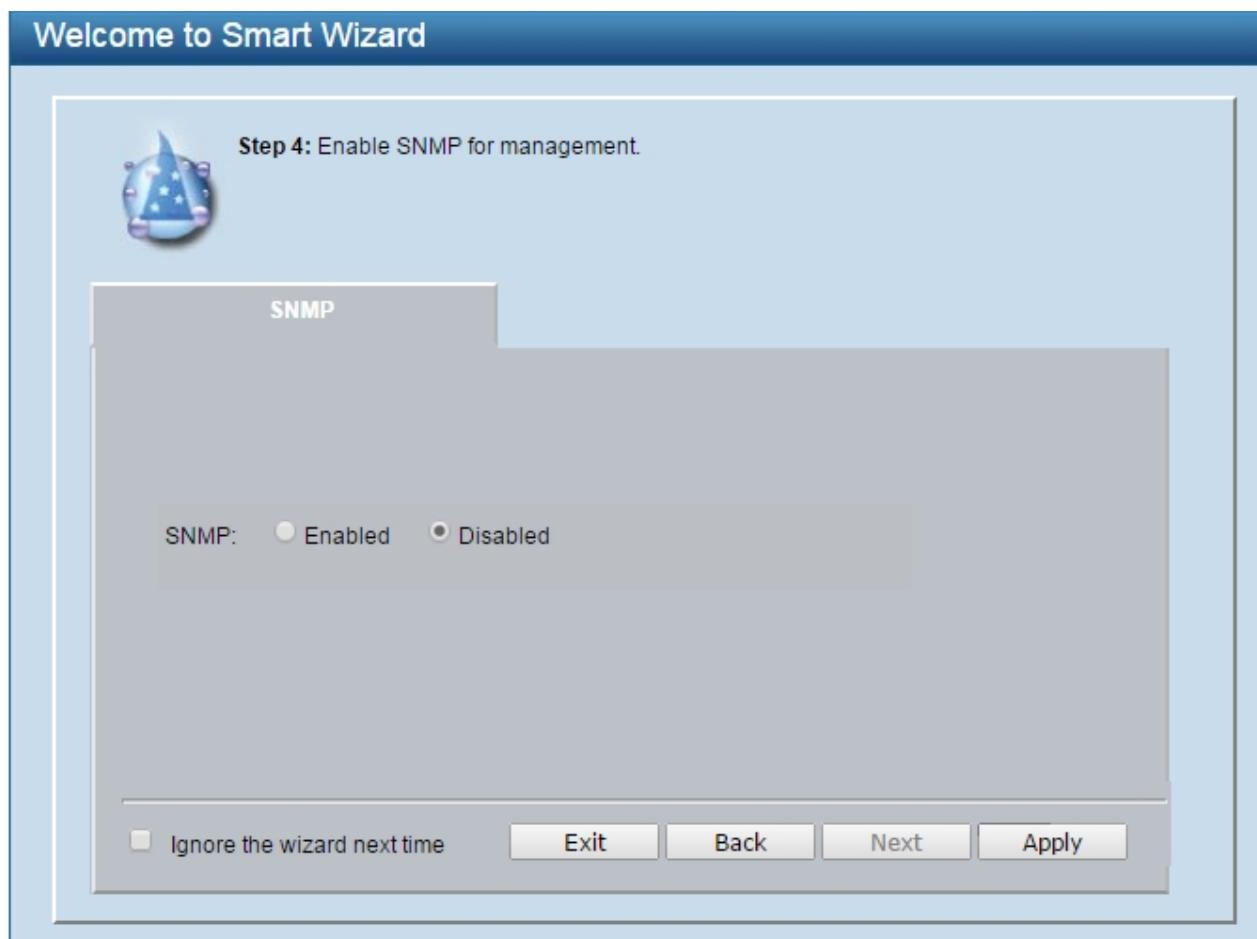


Figure 4.4 – SNMP in Smart Wizard



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



NOTE: Standard Mode and Surveillance Mode Web UIs share the same configuration files. Any features enabled in one interface will be made available in the other interface, for example: PoE scheduling, SNMP settings and the surveillance VLAN in use.

If you want to change the settings, click **Apply** and start a new web browser.

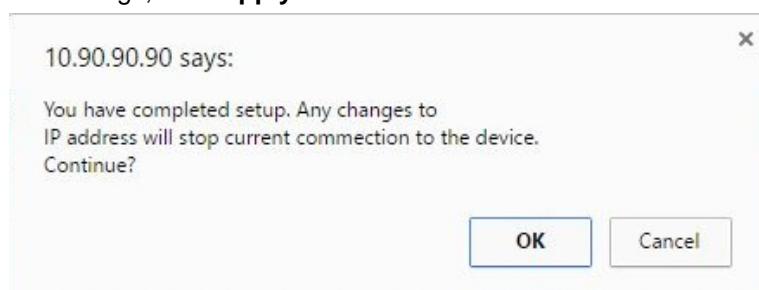


Figure 4.5 – Confirm the changes of IP address in Smart Wizard

Web-based Management

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

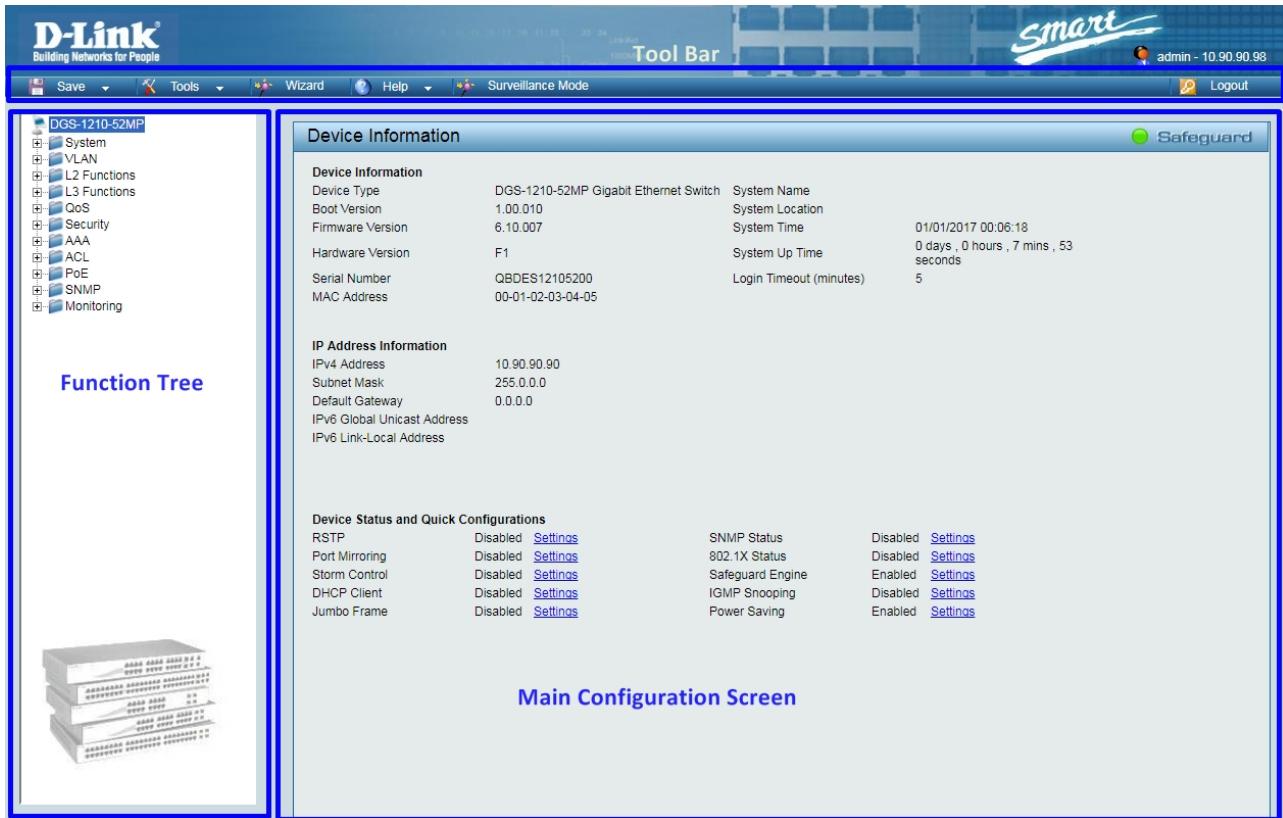


Figure 4.6 – Web-based Management

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.

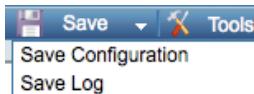


Figure 4.7 – Save Menu

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.



Figure 4.8 – 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).

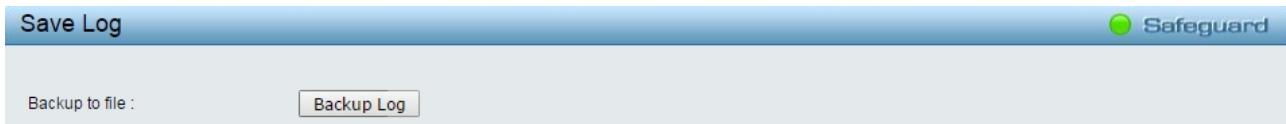


Figure 4.9 – Save Log

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.



Figure 4.10 – Tool Menu

Reset

Provide a safe reset option for the Switch. All configuration settings in non-volatile RAM will be reset to factory default except for the IP address.

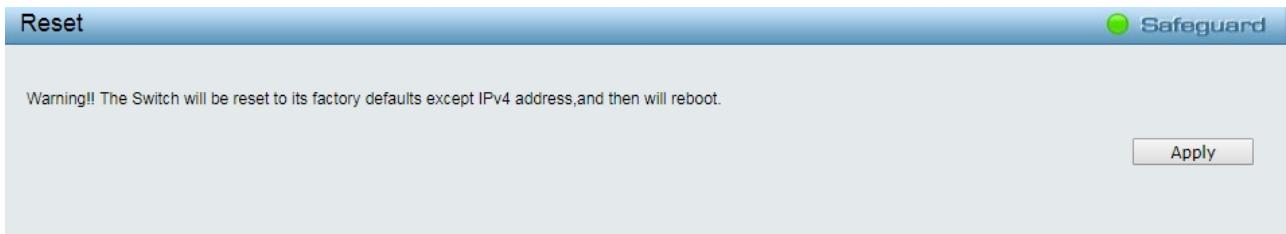


Figure 4.11 – Tool Menu > Reset

Reset System

Provide another safe reset option for the Switch. All configuration settings in non-volatile RAM will reset to factory default and the Switch will reboot.



Figure 4.12 – Tool Menu > Reset System

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 4.13 – 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**.

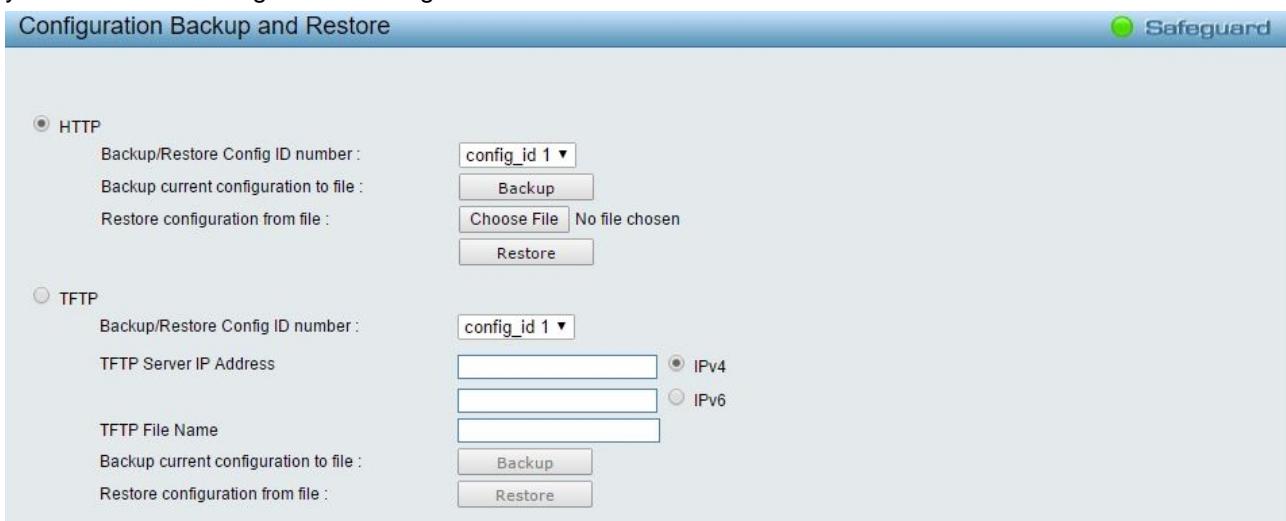


Figure 4.14 – Tool Menu > Configure Backup and Restore

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

Backup/Restore Config ID Number: Select config_id 1 or config_id 2.

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. Specifies the configuration 1 or 2 to be specified, **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.

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**.

The screenshot shows the 'Firmware Backup and Upgrade' section of the tool menu. It has two main sections: 'HTTP' and 'TFTP'.
HTTP Section:
 - 'Backup firmware to file:' dropdown set to 'Image_id 1' with a 'Backup' button.
 - 'Upgrade firmware from file:' 'Choose File' button with 'No file chosen' message, and an 'Upgrade' button.
TFTP Section:
 - 'TFTP Server IP Address:' input field with radio buttons for 'IPv4' (selected) and 'IPv6'.
 - 'TFTP File Name' input field.
 - 'Backup firmware to file:' dropdown set to 'Image_id 1' with a 'Backup' button.
 - 'Upgrade firmware from file:' 'Choose File' button with 'No file chosen' message, and an 'Upgrade' button.

Figure 4.15 – 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.



CAUTION: 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.

Flash Information

This page displays the flash detail information of the Switch.

The screenshot shows the 'Flash Information' section of the tool menu. It contains two tables:
Summary Table:

Flash ID	MX25L25635F			
Flash Size	32MB			

Detailed Memory Usage Table:

	Used	Total	Available	Usage %
Boot	1000000	1000000	0	100
Image1	9744416	14155776	4411360	68
Image2	9744416	14155776	4411360	68
Jffs2	303104	3932160	3629056	7

Figure 4.16 – Tool Menu > Flash Information

Tool Bar > Wizard

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

Tool Bar > Online Help

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



Figure 4.17 – Online Help

Tool Bar > Surveillance Mode

By clicking the **Surveillance Mode** button to access the Surveillance Mode Web UI on the Switch. After clicking the Surveillance Mode option in the Toolbar, the following pop-up window will appear.

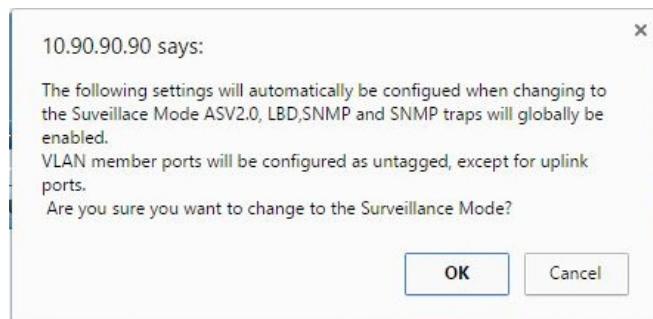


Figure 4.18 – Surveillance Mode Confirmation Message

The pop-up message window above displays a message that mentioned configurations need to be changed when access to the Surveillance Mode is given.

Click the **OK** button to continue.

Click the **Cancel** button and return to the **Standard Mode**.

After successfully switching to the Surveillance Mode on the Web UI of the Switch, the following window will be presented.

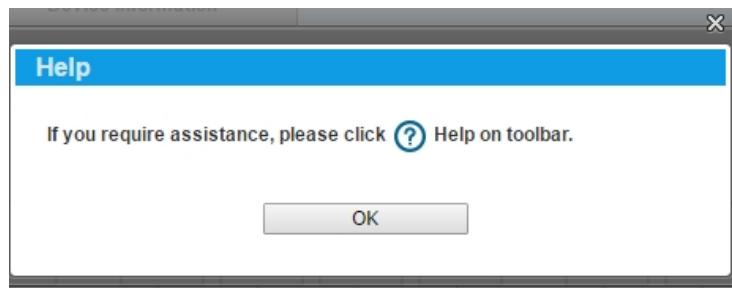


Figure 4.19 – Surveillance Mode Help Message

Click the **OK** button to continue, the following page will be presented.

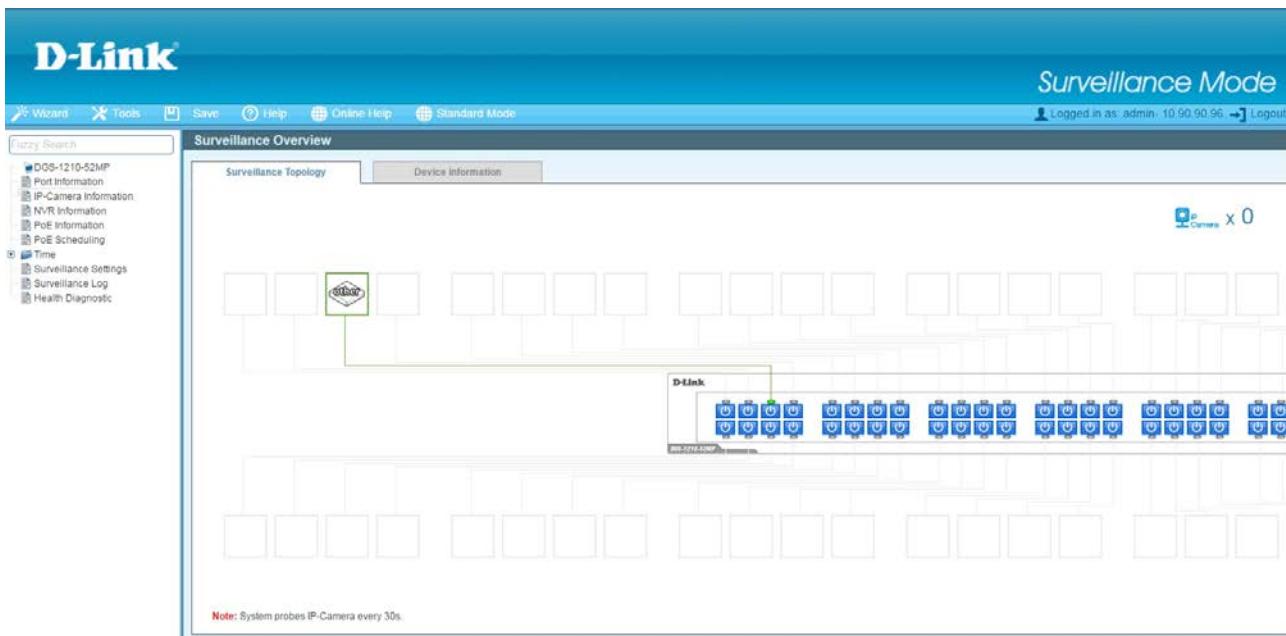


Figure 4.20 – Surveillance Mode

Scroll to the bottom of the page and click the **OK** button to continue to the Web UI. For more detail information of Surveillance Mode. Please refer to Chapter 5 [Surveillance Mode Configuration](#) for detailed instructions.

Function Tree

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

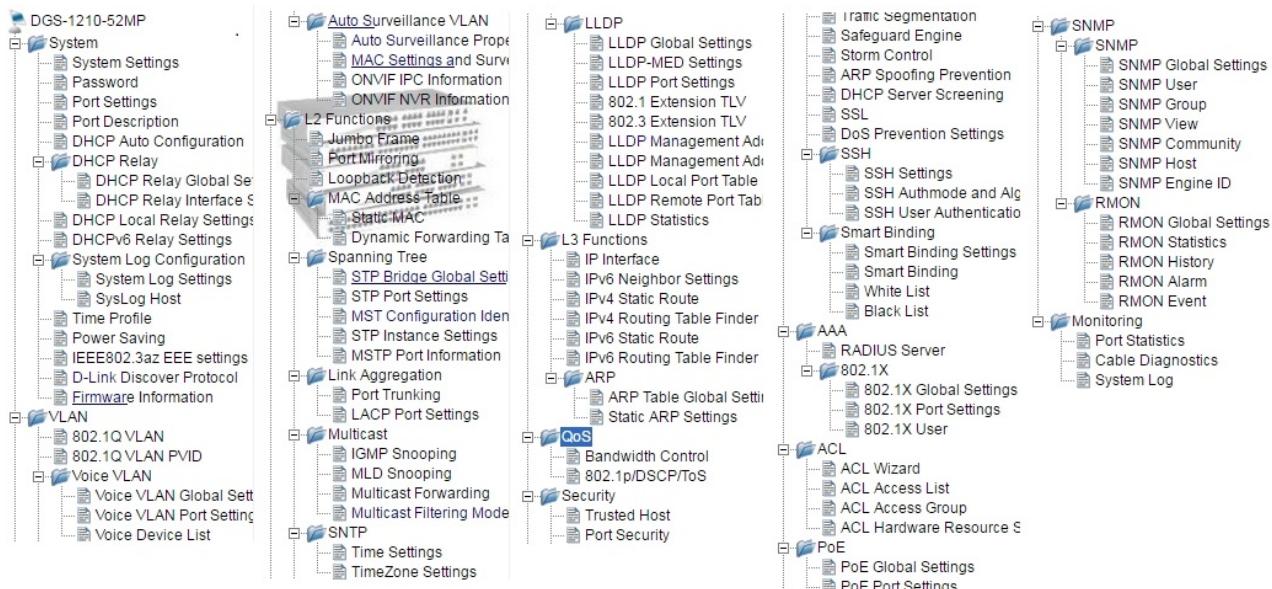


Figure 4.21 –Function Tree

Device Information

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

Device Information			
Safeguard			
Device Information			
Device Type	DGS-1210-52MP Gigabit Ethernet Switch	System Name	
Boot Version	1.00.010	System Location	
Firmware Version	6.10.007	System Time	01/01/2017 00:17:37
Hardware Version	F1	System Up Time	0 days , 0 hours , 19 mins , 12 seconds
Serial Number	QBDES12105200	Login Timeout (minutes)	5
MAC Address	00-01-02-03-04-05		
IP Address Information			
IPv4 Address	10.90.90.90		
Subnet Mask	255.0.0.0		
Default Gateway	0.0.0.0		
IPv6 Global Unicast Address			
IPv6 Link-Local Address			
Device Status and Quick Configurations			
RSTP	Disabled Settings	SNMP Status	Disabled Settings
Port Mirroring	Disabled Settings	802.1X Status	Disabled Settings
Storm Control	Disabled Settings	Safeguard Engine	Enabled Settings
DHCP Client	Disabled Settings	IGMP Snooping	Disabled Settings
Jumbo Frame	Disabled Settings	Power Saving	Enabled Settings

Figure 4.22 – Device Information

It also offers an overall status of common software features:

RSTP: Click **Settings** to link to L2 Functions > Spanning Tree > STP Global Settings. Default is disabled.

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

Storm Control: Click **Settings** to link to Security > Storm Control. Default is disabled.

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.

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.

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.

The screenshot shows the 'System Settings' page with two main sections: 'IPv4 Information' and 'System Information'.
IPv4 Information:
 - Radio buttons for Static (selected), DHCP, and BOOTP.
 - Interface Name: System
 - VLAN Name: default
 - Interface Admin State: Enabled
 - IPv4 Address: 10.90.90.90
 - Netmask: 8 (255.0.0.0)
 - Gateway: 0.0.0.0
 - DHCP Option 12 State: Disabled
 - DHCP Option 12 Host Name: DGS-1210-52MP
 - DHCP retry Times (0-120): 7
 - Buttons: Apply
System Information:
 - System Name: [empty]
 - System Location: [empty]
 - Login Timeout (3-30 minutes): 5
 - Buttons: Apply

Figure 4.23 – 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: By entering a **System Name** and **System Location**, the device can more easily be recognized through the SmartConsole Utility and from other Web-Smart devices on the LAN.

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 > Password

Setting a password is a critical tool for managers to secure the Web-Smart Switch. After entering the old password and the new password twice, click **Apply** for the changes to take effect.

The screenshot shows the 'Password Access Control' page with the following fields:
 - Old Password
 - New Password
 - Confirm Password
 - Note: Maximum 20 characters.
 - Buttons: Apply

Figure 4.24 – System > Password Access Control

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.

Figure 4.25 – System > Port Settings

Speed: Gigabit Fiber connections can operate in 1000M Auto or Disabled. Copper connections can operate in Forced Mode settings (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 auto-negotiation.

System > Port Description

Port description can be given on this page.

Port	Description
01	
02	
03	
04	
05	
06	
07	
08	
09	
10	
11	
12	
13	

Figure 4.26 – 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 > DHCP Auto Configuration

This page allows you 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.

If DHCP Auto Configuration is enabled, the switch will load a previously saved configuration file from TFTP server after every boot up.

If the switch is unable to complete the Auto Configuration process, the last configuration file saved in switch flash memory will be loaded.

Figure 4.27 – System > DHCP Auto Configuration

System > DHCP Relay > DHCP Relay Global Settings

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

Figure 4.28 – 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 user may add up to four server IPs per IP interface on the Switch. Entries may be deleted by clicking Delete button.

The screenshot shows the 'DHCP Relay Interface Settings' page. At the top, there are fields for 'Interface' (set to 'System') and 'Server IP'. An 'Apply' button is located to the right. Below this is a table titled 'DHCP Relay Interface Table' with four rows, each labeled 'Server1', 'Server2', 'Server3', and 'Server4' respectively. The table has columns for 'Interface' and 'Server IP'.

Figure 4.29 – System > DHCP Relay > DHCP 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 server. Up to four server IPs can be configured per IP Interface. 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 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.

The screenshot shows the 'DHCP Local Relay Settings' page. It includes a section for 'Config DHCP Local Relay for VLAN' where 'Config VLAN by' is set to 'VID' and 'State' is set to 'Disabled'. An 'Apply' button is located to the right. Below this is a section for 'DHCP Local Relay VID List'.

Figure 4.30 - 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.

The screenshot shows the 'DHCPv6 Relay Settings' configuration page. It includes fields for '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), and a 'Server IP' field containing '4A-6F-6E-01-01-01'. There are 'Apply' buttons at the bottom of each section. Below this, there's a 'DHCPv6 Relay Interface Table' with columns for 'Interface' (System) and 'Server Address' (empty). A 'Delete' button is also present.

Figure 4.31 - 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 an 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.

The screenshot shows the 'System Log Settings' configuration page. It has a 'System Log' section with 'Enabled' selected. Below it is a 'System Log Save Mode Settings' section with 'Save Mode' set to 'On Demand' and a timer set to '30 minutes (1-65535)'. There are 'Apply' and 'Save Log' buttons at the bottom.

Figure 4.32 – 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 occurs on the Switch.

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.

SysLog Host Settings		Safeguard
Server IP Address	<input checked="" type="radio"/> IPv4 <input type="text" value="0.0.0.0"/> <input type="radio"/> IPv6 <input type="text" value=""/>	Severity <input type="button" value="All"/>
UDP Port (1-65535)	<input type="text" value="514"/>	Facility <input type="button" value="Local 0"/>
Time Stamp	<input type="button" value="Enabled"/>	<input type="button" value="Apply"/>

Figure 4.33 – 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 - 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. And this is the default value.

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 Settings		Safeguard				
Time Profile						
Profile Name	<input type="text"/>					
Time(HH MM)	Start Time <input type="button" value="00"/>	<input type="button" value="00"/>				
Weekdays	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat					
Date <input type="checkbox"/>	From Day <input type="button" value="2011"/>	<input type="button" value="1"/>				
	To Day <input type="button" value="2011"/>	<input type="button" value="1"/>				
<input type="button" value="Add"/>						
Total Entries:0						
Profile Name	Start Time	End Time	Weekdays	From Day	To Day	Delete

Figure 4.34 – 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

The Power Saving mode feature reduces power consumption automatically when the RJ-45 port is link down or the connected devices are turned 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.

The screenshot shows the 'Power Saving Settings' configuration page. It includes sections for 'Global Settings' and 'Advanced Power Saving Settings'. In 'Global Settings', there is a radio button for 'Enabled' and one for 'Disabled'. An 'Apply' button is also present. The 'Advanced Power Saving Settings' section contains two dropdown menus for 'Type' (set to 'LED Shut-off') and 'State' (set to 'Disabled'). Below these are two dropdown menus for 'Time Profile 1' and 'Time Profile 2', both set to 'None'. A large table lists ports 01 through 52, each with a checkbox for selecting individual ports. Below this is a summary table with three rows: Type (LED Shut-off, Port Shut-off, System Hibernation), State (Disabled for all), Time Profile 1 (None for all), Time Profile 2 (None for all), and Port (None for all).

Type	State	Time Profile 1	Time Profile 2	Port
LED Shut-off	Disabled			None
Port Shut-off	Disabled			None
System Hibernation	Disabled			All Port

Figure 4.35 – 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 - 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 state 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 configured 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 compliant. 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.

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 4.36 – 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:

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

System > D-Link Discover Protocol Settings

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

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 4.37 – System > D-Link Discover Protocol Settings

D-Link Discover Protocol State: Enable or disable the Discover Protocol state. The default value is enabled.

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.

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

DDP Port Setting:

From Port / To Port: Specifies the range of ports to be configured for D-Link Discover Protocol of the Switch.

State: Specifies to enable or disable the D-Link Discover Protocol state for the specified ports.

Click **Apply** to implement changes made.

System > Firmware Information

The Firmware Information page displays the information of firmware. The user can specify which image file to boot up when power on the Switch next time.

The screenshot shows the 'Firmware Information' section of the web interface. At the top, there is a table with columns: ID, Version, Size (B), Update Time, From, and User. Two rows are listed: one for version 6.10.007 (Size 10608880, From 10.90.90.66, User admin (Web)) and another for version 6.00.006 (Size 12288000, From N/A, User Anonymous (factory)). Below the table, a message says 'Please select the boot up image of device.' followed by a dropdown menu labeled 'Image_id 1 ▼' and a 'Apply' button. At the bottom, there is a legend mapping update methods to protocols: *: Boot up firmware, (SSH): Firmware update through SSH, (Web): Firmware update through Web, (SNMP): Firmware update through SNMP, and (Telnet): Firmware update through Telnet.

Figure 4.38 – System > Firmware Information

System > Configuration Information

The Configuration Information page displays the information of configuration. The user can specify which configuration file to be viewed of the Switch.

The screenshot shows the 'Configuration Information' section of the web interface. At the top, there is a table with columns: ID, Size (B), Update Time, From, and User. Two rows are listed: both marked as 'N/A'. Below the table, a message says 'Please select the boot up config of device.' followed by a dropdown menu labeled 'config_id 1 ▼' and a 'Apply' button. At the bottom, there is a legend mapping update methods to protocols: *: Boot up config, (SSH): Config update through SSH, (Web): Config update through Web, (SNMP): Config update through SNMP, and (Telnet): Config update through Telnet.

Figure 4.38 – System > Configuration Information

VLAN > 802.1Q VLAN

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

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

The IEEE 802.1Q VLAN 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.

The screenshot shows the '802.1Q VLAN Settings' page. At the top, there are two radio buttons: 'Enabled' (unchecked) and 'Disabled' (checked). Below them is a note: 'Total static VLAN entries: 1' and 'Maximum 256 entries.' An 'Add' button is available. The main table has columns for VID, VLAN Name, Untagged, and Tagged. One row is shown: VID 1, VLAN Name default, Untagged 01-52, and Tagged (empty). There are 'Delete' buttons for both rows. At the bottom, there are 'Page' (01), 'Back', and 'Next' buttons.

VID	VLAN Name	Untagged	Tagged	Delete
1	default	01-52		Delete

Figure 4.39 – Configuration > 802.1Q VLAN

Click **Add** to create a new VID group, entering the VID and VLAN name, assigning ports from 01 to 52 as **Untag, Tag or Not Member**. To save the VID group, click **Apply**.

The screenshot shows the 'VID Settings' page with the 'Add VID' section. It has fields for 'VID' (1) and 'VLAN Name' (default). A note says 'Maximum 20 characters.' Below is a grid for port assignments. The first row has 'Port' (Select All), '01' through '26'. Subsequent rows show 'Untagged' (All), 'Tagged' (All), and 'Not member' (All) for each port. The grid is 3 rows by 26 columns. At the bottom right are 'Back' and 'Apply' buttons.

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
Untagged	All	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Tagged	All	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Not member	All	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Port	Select All	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
Untagged	All	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Tagged	All	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Not member	All	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	

Figure 4.40 – Configuration > 802.1Q VLAN > Add VID

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

The screenshot shows the '802.1Q VLAN Settings' page. At the top, there are buttons for 'Asymmetric VLAN' (selected), '[Example]', and radio buttons for 'Enabled' (selected) and 'Disabled'. On the right, there are 'Apply' and 'Safeguard' buttons. Below this, a message says 'Total static VLAN entries: 2' and 'Maximum 256 entries.' A note indicates 'Untagged' and 'Tagged' ports. The main table has columns for VID, VLAN Name, Untagged (01-52), Tagged (13-15, 43-44), and Delete. Two rows are listed: VID 1 (VLAN Name default, Untagged 01-52, Tagged 13-15, 43-44), and VID 2 (VLAN Name vlan2, Untagged 01-52, Tagged 13-15, 43-44). There are three 'Delete' buttons in the last column. At the bottom, there are 'Page' (01), 'Back', and 'Next' buttons.

Figure 4.41 – 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.

The screenshot shows the 'VID Settings' page for VID 1. It includes fields for VID (1), VLAN Name (default), and buttons for 'Back' and 'Apply'. The main part is a grid of port assignments for VID 1 across 52 ports. The grid has rows for Port, Untagged, Tagged, and Not Member status. The first row shows 'Select All' and 'All' for all ports. Subsequent rows show specific port assignments. At the bottom, there are 'Back' and 'Apply' buttons.

Figure 4.42 - Configuration > 802.1Q VLAN > VID Assignments

VLAN > 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.

Port	01	02	03	04	05	06	07	08	09	10	11	12	13
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1
Port	14	15	16	17	18	19	20	21	22	23	24	25	26
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1
Port	27	28	29	30	31	32	33	34	35	36	37	38	39
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1
Port	40	41	42	43	44	45	46	47	48	49	50	51	52
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1

Figure 4.43 – Configuration > 802.1Q VLAN PVID

VLAN > 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.

ID	Description	Telephony OUI	OUI Mask	Delete

Figure 4.44 – 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 you want to assign voice traffic to. You must first create a VLAN from the 802.1Q VLAN page before you can assign a dedicated Voice VLAN. The member port you 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 Organizational 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: You can manually create a Telephony OUI with a description. The maximum number of user defined OUs 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.

VLAN > 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.

Voice VLAN Port Settings
Safeguard

From Port	To Port	Auto Detection	Tagged / Untagged		
01	52	Disabled	Untagged	<input type="button" value="Refresh"/>	<input type="button" value="Apply"/>
Port	Auto Detection	Tagged / Untagged	Current State	Status	
01	Disabled	Untagged	None	Static	
02	Disabled	Untagged	None	Static	
03	Disabled	Untagged	None	Static	
04	Disabled	Untagged	None	Static	
05	Disabled	Untagged	None	Static	
06	Disabled	Untagged	None	Static	
07	Disabled	Untagged	None	Static	
08	Disabled	Untagged	None	Static	
09	Disabled	Untagged	None	Static	
10	Disabled	Untagged	None	Static	
11	Disabled	Untagged	None	Static	
12	Disabled	Untagged	None	Static	
13	Disabled	Untagged	None	Static	
14	Disabled	Untagged	None	Static	
15	Disabled	Untagged	None	Static	
16	Disabled	Untagged	None	Static	

Figure 4.45 – VLAN > Voice VLAN > Voice VLAN Port Settings

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

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.

VLAN > Voice VLAN > Voice Device List

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

Voice Device List						Safeguard
Port	All	Search				
ID	Port	MAC Address	Priority	Type	Delete	

Figure 4.46 – VLAN > Voice VLAN > Voice Device List

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

VLAN > 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		Safeguard
Global Settings		
Auto Surveillance VLAN	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
Surveillance VLAN ID	4094	
Surveillance VLAN CoS	5	
Tagged Uplink/Downlink Port	<input type="text"/> Ex:(1,2,4-6)	
Aging Time (1-65535)	720	
Discover Port (554,1024-65535)	554	
Log State	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
Note: Surveillance VLAN ID and Voice VLAN ID cannot be the same.		
Apply		
ONVIF Global Status		
Surveillance Device Detected (OUI)	0	
IP-Camera Detected (ONVIF)	0	
NVR Detected (ONVIF)	0	

Figure 4.47 – 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.

Tagged Uplink/Downlink Port: Specifies the port or ports to be tagged uplink port or downlink port for the Auto Surveillance VLAN.

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.

VLAN > 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.

The screenshot shows the 'MAC Settings and Surveillance Device' configuration page. At the top, there's a header bar with tabs for 'MAC Settings and Surveillance Device' and 'Safeguard'. Below the header, a section titled 'User-defined MAC Settings' contains a note: 'To add more device(s) for Auto Surveillance VLAN by user-defined configuration as below'. It includes fields for 'Component Type' (set to 'Video Management Server'), 'Description', 'MAC Address' (format XX-XX-XX-XX-XX-XX), and 'Mask'. A note says 'Maximum number of user-defined MAC is 5 entries.' Below this is a table with columns: ID, Component Type, Description, MAC Address, Mask, and Delete. The table lists four entries for D-Link Surveillance Devices. At the bottom, there's an 'Auto Surveillance VLAN Summary' table with columns: Port, Component Type, and Description, showing eight ports all assigned to 'None'.

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

Port	Component Type	Description
1	None	None
2	None	None
3	None	None
4	None	None
5	None	None
6	None	None
7	None	None
8	None	None

Figure 4.48 – VLAN > Auto Surveillance VLAN > MAC Settings and Surveillance Device

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.

VLAN > Auto Surveillance VLAN > ONVIF IPC Information

The ONVIF IPC Information page displays the information on each IP camera connected to the switch. Including the port number, IP address, MAC address, throughput and other information such as port description and model name.

Ports	IP Address	MAC Address	Model	Manufacturer	Traffic	Description	Throughput
Total Entries Discovered: 0							

Note: System probes IP-Camera every 30s.

Figure 4.49 – VLAN > Auto Surveillance VLAN > ONVIF IPC Information

VLAN > Auto Surveillance VLAN > ONVIF NVR Information

The ONVIF 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.

Ports	IP Address	MAC Address	IP-Camera Number	Throughput	Group	Description
Total Entries Discovered: 0						

Note: System probes IP-Camera every 30s.

Figure 4.50 – VLAN > Auto Surveillance VLAN > ONVIF NVR Information

L2 Functions > Jumbo Frame

D-Link Gigabit Smart Managed 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 Enabled Disabled

Maximum Length is 10000 bytes.

Apply

Figure 4.51 – L2 Functions > Jumbo Frame

L2 Functions > 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.

Source Port Selection																										Apply	
Sniffer Mode	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
TX	All	<input type="checkbox"/>	<input type="checkbox"/>																								
RX	All	<input type="checkbox"/>	<input type="checkbox"/>																								
TX/RX	All	<input type="checkbox"/>	<input type="checkbox"/>																								
None	All	<input checked="" type="checkbox"/>																									
Sniffer Mode	Select All	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
TX	All	<input type="checkbox"/>	<input type="checkbox"/>																								
RX	All	<input type="checkbox"/>	<input type="checkbox"/>																								
TX/RX	All	<input type="checkbox"/>	<input type="checkbox"/>																								
None	All	<input checked="" type="checkbox"/>																									

Figure 4.52 – 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.

L2 Functions > Loopback Detection

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

Loopback Detection Settings

Loopback Detection <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled Mode: Port-based VLAN List: <input type="text"/> Interval (1-32767): <input type="text" value="2"/> sec Recover Time (0 or 60-1000000): <input type="text" value="60"/> sec	 Safeguard																																																																																																																																										
<input type="button" value="Apply"/>																																																																																																																																											
From Port	To Port	State																																																																																																																																									
01	52	Disabled	<input type="button" value="Refresh"/>	<input type="button" value="Apply"/>																																																																																																																																							
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Port</th> <th style="text-align: left;">State</th> <th colspan="3" style="text-align: center;">Loop Status</th> </tr> </thead> <tbody> <tr><td>01</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>02</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>03</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>04</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>05</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>06</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>07</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>08</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>09</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>10</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>11</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>12</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>13</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>14</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>15</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>16</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>17</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>18</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>19</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>20</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>21</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>22</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>23</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>24</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>25</td><td>Disabled</td><td colspan="3">Normal</td></tr> <tr><td>26</td><td>Disabled</td><td colspan="3">Normal</td></tr> </tbody> </table>					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			12	Disabled	Normal			13	Disabled	Normal			14	Disabled	Normal			15	Disabled	Normal			16	Disabled	Normal			17	Disabled	Normal			18	Disabled	Normal			19	Disabled	Normal			20	Disabled	Normal			21	Disabled	Normal			22	Disabled	Normal			23	Disabled	Normal			24	Disabled	Normal			25	Disabled	Normal			26	Disabled	Normal		
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																																																																																																																																									
12	Disabled	Normal																																																																																																																																									
13	Disabled	Normal																																																																																																																																									
14	Disabled	Normal																																																																																																																																									
15	Disabled	Normal																																																																																																																																									
16	Disabled	Normal																																																																																																																																									
17	Disabled	Normal																																																																																																																																									
18	Disabled	Normal																																																																																																																																									
19	Disabled	Normal																																																																																																																																									
20	Disabled	Normal																																																																																																																																									
21	Disabled	Normal																																																																																																																																									
22	Disabled	Normal																																																																																																																																									
23	Disabled	Normal																																																																																																																																									
24	Disabled	Normal																																																																																																																																									
25	Disabled	Normal																																																																																																																																									
26	Disabled	Normal																																																																																																																																									

Figure 4.53 – 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.

L2 Functions > MAC Address Table > Static MAC

This feature provides two distinct functions. The **MAC Address** Learning table allows turning off the function of learning MAC address automatically, if a port isn't specified as an uplink port (for example, connects to a DHCP Server or Gateway). By default, this feature is disabled.

The screenshot shows the 'Static MAC Settings' section of the web-based switch configuration. At the top, there's a radio button for 'MAC Address Learning' with options 'Enabled' (selected) and 'Disabled'. Below this is a grid table with columns labeled 'Port' (01-26) and 'Learning' (checkboxes). A horizontal bar with buttons 'Select All', 'Clear', and 'Apply' is positioned above a second grid for ports 27-52. Below the grids is a 'Add Static MAC Address' form with dropdowns for 'Port' (01), 'MAC Address' (empty input), and 'VID' (1). To the right is an 'Add' button. At the bottom is a 'Static MAC Address Lists' table with columns 'ID', 'Port', 'MAC Address', 'VID', and 'Delete'.

ID	Port	MAC Address	VID	Delete
1	5	3C-97-0E-E5-76-4D	1	<input type="button" value="Delete"/>

Figure 4.54 – 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.

L2 Functions > 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.

The screenshot shows the 'Dynamic Forwarding Table' section. It includes a 'Port' dropdown set to 'All', a 'Search' button, and a horizontal bar with 'Select All', 'Clear', and 'Apply' buttons. Below is a table with columns 'ID', 'Port', 'MAC Address', 'VID', 'Type' (Dynamic), and 'Add to Static MAC' (checkbox).

ID	Port	MAC Address	VID	Type	Add to Static MAC
1	5	3C-97-0E-E5-76-4D	1	Dynamic	<input type="checkbox"/>

Figure 4.55 – L2 Functions > MAC Address Table > Dynamic Forwarding Table

L2 Functions > 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:

Parameter	Value	Parameter	Value
STP Version	MSTP	Root Bridge	00:00:00:00:00:00:00
Bridge Priority	32768	Root Cost	0
Tx Hold Count (1-10)	3	Root Maximum Age	20
Maximum Age (6-40 secs)	20	Root Forward Delay	15
Hello Time (1-10 secs)	2	Root Port	0
Forward Delay (4-30 secs)	15		
Forwarding BPDU	Enabled		

Figure 4.56 – L2 Functions > Spanning Tree > STP Bridge Global Settings

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

STP Version: You can 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.

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

Root Cost: Displays the cost of the Root Bridge.

Root Maximum Age: Displays the Maximum Age of the Root Bridge.

Root Forward Delay: Displays the Forward Delay of the Root Bridge.

Root port: Displays the root port.

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

Click **Refresh** to renew the page.

L2 Functions > 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.

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

Port	State	Priority	External Cost	Edge	P2P	Restricted Role	Restricted TCN	Forward BPDU	Hello Time	Port State
01	Enable	128	20000	Auto	Auto	False	False	Enable	2	Disabled
02	Enable	128	20000	Auto	Auto	False	False	Enable	2	Disabled
03	Enable	128	20000	Auto	Auto	False	False	Enable	2	Disabled
04	Enable	128	20000	Auto	Auto	False	False	Enable	2	Disabled
05	Enable	128	20000	Auto	Auto	False	False	Enable	2	Forwarding
06	Enable	128	20000	Auto	Auto	False	False	Enable	2	Disabled
07	Enable	128	20000	Auto	Auto	False	False	Enable	2	Disabled
08	Enable	128	20000	Auto	Auto	False	False	Enable	2	Disabled
09	Enable	128	20000	Auto	Auto	False	False	Enable	2	Disabled
10	Enable	128	20000	Auto	Auto	False	False	Enable	2	Disabled
11	Enable	128	20000	Auto	Auto	False	False	Enable	2	Disabled
12	Enable	128	20000	Auto	Auto	False	False	Enable	2	Disabled

Figure 4.57 – L2 Functions > 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. The default value is 0 (auto).

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

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

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 have edge port status or not have edge port status automatically.

Priority: Specifies 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 the **Apply** button to implement changes made. Click **Refresh** to renew the page.

L2 Functions > 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.

The screenshot shows the 'MST Configuration Identification' page with the following sections:

- MST Configuration Identification Settings:**
 - Configuration Name: 00-E0-4C-00-00-00
 - Revision Level (0-65535): 0
 - Buttons: Apply, Safeguard
- Instance ID Settings:**
 - MSTI ID (1-15): 1
 - Type: Add VID
 - VID List (1-4094):
 - Buttons: Apply
- Total Entries: 1**
- MSTI Instances Table:**

MSTI ID	VID List	Edit	Delete
CIST	1-4094	Edit	Delete

Figure 4.58 – L2 Functions > 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 Settings** 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 conjunction with the VID List parameter.

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

Click **Apply** to implement changes made.

L2 Functions > Spanning Tree > STP Instance Settings

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

The screenshot shows the 'STP Instance Settings' configuration page. At the top, there's a header bar with tabs and a 'Safeguard' button. Below it, a section for 'STP Priority Settings' includes fields for 'MSTI ID' (with a dropdown menu) and 'Priority' (set to 0). A large table lists 'Total Entries: 1'. The table has columns for 'Instance Type' (CIST), 'Instance Status' (Enabled), and 'Instance Priority' (32768). To the right of the table are 'Edit' and 'View' buttons. Below the table, another section titled 'STP Instance Operational Status' lists various parameters like 'MSTP ID', 'External Root Cost', etc., each with a corresponding value field.

Figure 4.59 – L2 Functions > Spanning Tree > STP Instance Settings

To modify an entry on the table, click the **Edit** button. To view more information about an 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 the **Apply** button to implement changes made.

L2 Functions > 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**.

The screenshot shows the 'MSTP Port Information' configuration page. At the top, there's a header bar with tabs and a 'Safeguard' button. Below it, a section for 'MSTP Port Setting' includes a 'Port' dropdown set to 1 and a 'Find' button. A table lists port settings for 'Instance ID' (0), 'Internal Path Cost (0-200000000; 0=AUTO)', 'Priority' (0), and 'Status' (Enabled). To the right of the table are 'Edit' and 'Apply' buttons. Below the table, another section lists port details for 'MSTI' (0), 'Designated Bridge' (N/A), 'Internal Path Cost' (20000), 'Priority' (128), 'Status' (Enabled), and 'Role' (Disabled).

Figure 4.60 – L2 Functions > 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.

L2 Functions > Link Aggregation > Port Trunking

The Trunking 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 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.

Link Aggregation Settings				
Group	01	Type	LACP	Apply
Port	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			
Port	27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52			

Maximum 8 ports in static group and 8 ports in LACP group.

Group	Type	Ports	Delete

Figure 4.61 – L2 Functions > Link Aggregation > Port Trunking



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

L2 Functions > 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.

From Port	To Port	Activity	Timeout	Apply
01	52	Passive	Short (3 sec)	Apply
Port	Activity	Timeout		
01	Active	Long (90 sec)		
02	Active	Long (90 sec)		
03	Active	Long (90 sec)		
04	Active	Long (90 sec)		
05	Active	Long (90 sec)		
06	Active	Long (90 sec)		
07	Active	Long (90 sec)		
08	Active	Long (90 sec)		
09	Active	Long (90 sec)		
10	Active	Long (90 sec)		
11	Active	Long (90 sec)		
12	Active	Long (90 sec)		

Figure 4.62 – L2 Functions > 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.

Activity: There are two different roles of LACP ports:

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: Specifies 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 the **Apply** button to implement changes made.

L2 Functions > Multicast > IGMP Snooping

With Internet Group Management Protocol (IGMP) snooping, the Smart Managed 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 Smart Managed Switch will forward multicast traffic only to connections that have group members attached.

The default IGMP Snooping version is v3, which works compatible with IGMP versions v1 and v2.

The DGS-1210 series support IGMP v1/v2/v3 awareness. And the IGMP v3 awareness means that we do support IGMP v3 snooping, in other words, switch can read/understand the IGMP control packet which is version3. The Switch still can based on its report/leave packet to do the correct behavior. But from the RFC point of view, full IGMP v3 means that it should support source filtering and it's not possible to support on the L2 switch.

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

VLAN ID	VLAN Name	State	Querier State	Fast Leave	Router Ports	Multicast Entries
1	default	Enabled	Disabled	Disabled	View	

Figure 4.63 – L2 Functions > Multicast > IGMP Snooping

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

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.

Robustness Variable (2-255 sec): The Robustness Variable allows adjustment for the expected packet loss on a subnet. If a subnet is expected to be lossy, the Robustness Variable may need to be increased. 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.

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 are no Query control messages received for 'Router Port Purge Interval' time, the learned router port entry will be purged. Default is 260 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.

To enable IGMP snooping for a given VLAN, select enable and click on the **Apply** button. Then press the **VLAN ID** number, and select the ports to be assigned as router ports for IGMP snooping for the VLAN, and press **Apply** for changes to take effect. A router port configured manually is a **Static Router Port**, and a **Dynamic Router Port** is dynamically configured by the Switch when query control message is received.

Static Router Ports																									
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	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]

Dynamic Router Ports																									
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	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]	[]

Figure 4.64 – L2 Functions > Multicast > IGMP Snooping VLAN Settings

State: Specifies the State to be enabled or disabled.

Querier State: D-Link Smart Switch is able to send out the IGMP Queries to check the status of multicast clients. Default is disabled.

Fast Leave: Specifies the Fast Leave feature to be enabled or disabled.

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

Group ID	VLAN ID	VLAN Name	Multicast Group	Multicast MAC address	Member Port	Delete
001	1	default	239.255.255.250	01-00-5E-7F-FF-FA	01	<input type="button" value="Delete"/>

Figure 4.65 – L2 Functions > Multicast > IGMP Multicast Entry Table

Click **Delete** to remove a specified entry or click **Delete All** to remove all entries.

L2 Functions > Multicast > MLD Snooping

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

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

The screenshot shows the 'MLD Snooping Configuration' interface. At the top, there is a 'Safeguard' button. Below it, the 'MLD Snooping Global Settings' section contains fields for Host Timeout (260 sec), Router Timeout (125 sec), Robustness Variable (2), Last Member Query Interval (1 sec), and Max Response Time (10 sec). A note says 'When Querier state is enabled, the Host Timeout is calculated as the formula : (Host Timeout = Robustness Variable * Query Interval + Max Response Time)' with an 'Apply' button. The 'MLD Snooping VLAN Settings' section displays a table:

VLAN ID	VLAN Name	State	Querier State	Fast Leave	Router Ports	Multicast Entries
1	default	Enabled	Disabled	Disabled		View
4094	ASV_4094	Enabled	Disabled	Disabled		View

At the bottom, there are navigation buttons for Page (01), Back, and Next.

Figure 4.66 – L2 Functions > Multicast > MLD Snooping

MLD Global Settings:

MLD Snooping: Enable or disable the MLD Snooping.

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.

Robustness Variable (2-255): The Robustness Variable allows adjustment for the expected packet loss on a subnet. If a subnet is expected to be lossy, the Robustness Variable may be increased. The

Robustness Variable cannot be set to zero, and SHOULD NOT be one. Default is 2 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 network. A reduced value results in reduced time to detect the loss of the last member of a group. The default value is 1 second.

Query Interval (60-600 sec): The Query Interval is the interval between General Queries sent. By adjusting the Query Interval, the number of MLD messages can increase or decrease; larger values cause MLD Queries to be sent less often. Default is 125 seconds.

Max Response Time (10-25 sec): Specifies the time interval in seconds after which a port is removed from the Multicast membership group. Ports are removed from the Multicast membership when the port sends a Done Message, indicating the port requests to leave the Multicast group. The field range is 10-25 seconds. The default timeout is 10 seconds.

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

MLD Snooping VLAN Settings List:

Click the number of VLAN ID to modify the settings:

MLD Snooping VLAN Settings

VLAN ID	1																								
VLAN Name	default																								
State	Enabled ▾																								
Querier State	Disabled ▾																								
Fast Leave	Disabled ▾																								
<input type="button" value="Apply"/>																									
Static Router Ports																									
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
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Dynamic Router Ports																									
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
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="button" value="Back"/> <input type="button" value="Apply"/>																									

Figure 4.67 – L2 Functions > Multicast > Multicast Forwarding

State: Specifies the state of MLD Snooping VLAN to be enabled or disabled.

Querier State: Specifies the querier state to be enabled or disabled.

Fast Leave: Specifies the fast leave feature to be enabled or disabled.

Click **Apply** to implement changes made.

Static Router Ports: Selects the ports to be static router ports and assigned for MLD snooping for the VLAN.

Dynamic Router Ports: Select the ports to be dynamic router ports and assigned for MLD snooping for the VLAN.

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

L2 Functions > Multicast > Multicast Forwarding

The Multicast Forwarding page displays all of the entries made into the Switch's static multicast forwarding table. To implement the Multicast Forwarding Settings, input **VID**, **Multicast MAC Address** and port settings, then click **Add**.

Multicast Forwarding Settings

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	
Member	All	<input type="radio"/>																										
None	All	<input checked="" type="radio"/>																										
Port	Select All	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	
Member	All	<input type="radio"/>	<input type="radio"/>																									
None	All	<input checked="" type="radio"/>																										

Total Static Entries: 0

VID | MAC Address | Member Ports | Delete

Figure 4.68 – L2 Functions > Multicast > Multicast Forwarding

VID: The VLAN ID of the VLAN to which the corresponding MAC address belongs.

Multicast MAC Address: The MAC address of the static source of multicast packets. This must be a multicast MAC address.

Port Settings: Allows the selection of ports that will be members of the static multicast group and ports either that are forbidden from joining dynamically, or that can join the multicast group dynamically, using GMRP.

Member - The port is a static member of the multicast group.

None - No restrictions on the port dynamically joining the multicast group. When **None** is chosen, the port will not be a member of the Static Multicast Group.

L2 Functions > Multicast > Multicast Filtering Mode

The **Multicast Filtering Mode** function allows users to select the filtering mode for IGMP group per VLAN basis.

Multicast Filtering Mode

From Port	To Port	Filtering Mode
1	52	Forward Unregistered Groups

Multicast Filtering Mode Table

Forwarding List	1-52
Filtering List	

Figure 4.69 – L2 Functions > Multicast > Multicast Filtering Mode

VLAN ID: Specifies the VLAN ID.

Filtering Mode:

Forward Unregistered Groups: The multicast stream will be forwarded based on the register table in registered group, but it will be flooded to all ports of the VLAN in unregistered group.

Filter Unregistered Groups: The registered group will be forwarded based on the register table and the unregister group will be filtered.

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

L2 Functions > SNTP > 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.

Clock Source: Specifies 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 implement changes made.

Figure 4.70 – L2 Functions > SNTP > Time Settings

Clock Source: Specifies 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 implement changes made.

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.

L2 Functions > SNTP > TimeZone Settings

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

Daylight Saving Time: Options to enable or disable daylight saving time. The default is **Enabled**.

Daylight Saving Time Offset: Set the offset in minutes. The default is 60 min.

Time Zone Offset: GMT +/-HH:MM: Set the time zone offset.

Daylight Saving Time Settings: Define the start and end dates for Daylight Saving Time.

From: Month / Day	Jan	01
From: HH / MM	00	00
To: Month / Day	Jan	01
To: HH / MM	00	00

Figure 4.71 – L2 Functions > 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 your local DST offset - 30, 60, 90, or 120 minutes.

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

Daylight Saving Time Settings:

From: Month / Day: Enter the month DST and date DST will start on, each year.

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

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

L2 Functions > LLDP > LLDP Global Settings

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

The screenshot shows the 'LLDP Global Settings' configuration page. At the top, there is a radio button for 'Enabled' (selected) and one for 'Disabled'. Below this are four input fields for 'Message TX Hold Multiplier' (set to 4), 'Message TX Interval' (set to 30 sec), 'LLDP Reinit Delay' (set to 2 sec), and 'LLDP TX Delay' (set to 2 sec). An 'Apply' button is located to the right of these fields. Below the configuration section is a table titled 'LLDP System Information' with two rows. The first row contains 'Chassis ID Subtype' (macAddress) and 'Chassis ID' (00-01-02-03-04-05). The second row contains 'System Name' (DGS-1210-52MP) and 'System Description' (6.10.0007).

Figure 4.72 – L2 Functions > 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: $1 < \text{txDelay} < (0.25^{\circ} - \text{msgTxInterval})$. The default value is **2** seconds.

L2 Functions > LLDP > LLDP-MED Settings

LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) is an enhancement of LLDP. It improves the LLDP operation between endpoint devices such as IP phones and APs. LLDP-MED supports features such as Auto-discovery of LAN policies and device location discovery.

This page allows user to configure the **Power PSE TLV** (Type-length-value) state of 802.3at ports. Select **From Port/ To Port** and **Enable / Disable** and then click **Apply** to turn on/off the **Power PSE TLV** transmission.

The screenshot shows the 'LLDP MED Settings' page. At the top, there are dropdown menus for 'From Port' (set to 1) and 'To Port' (set to 48), and a dropdown for 'Extended PSE TLV' (set to 'Disabled'). Below these are two buttons: 'Refresh' and 'Apply'. The main area is a table with columns 'Port' (1-13) and 'Extended PSE TLV' (all set to 'Disabled').

Port	Extended PSE TLV
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 4.73 – L2 Functions > LLDP > LLDP-MED Settings

L2 Functions > LLDP > LLDP Port Settings

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

The screenshot shows the 'Basic LLDP Port Settings' page. At the top, there are dropdown menus for 'From Port' (set to 1) and 'To Port' (set to 52), and dropdowns for 'Notification State' (set to 'Disabled'), 'Admin Status' (set to 'TX_Only'), 'Port Description' (set to 'Disabled'), 'System Name' (set to 'Disabled'), 'System Description' (set to 'Disabled'), and 'System Capabilities' (set to 'Disabled'). Below these are two buttons: 'Refresh' and 'Apply'. The main area is a table with columns 'Port' (1-11), 'Notification State' (all set to 'Disabled'), 'Admin Status' (all set to 'TX_and_RX'), 'Port Description' (all set to 'Disabled'), 'System Name' (all set to 'Disabled'), 'System Description' (all set to 'Disabled'), and 'System Capabilities' (all set to 'Disabled').

Port	Notification State	Admin Status	Port Description	System Name	System Description	System Capabilities
1	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
2	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
3	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
4	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
5	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
6	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
7	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
8	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
9	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
10	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
11	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled

Figure 4.74 – L2 Functions > LLDP > 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 the **Apply** button to implement changes made and click **Refresh** to refresh the table information.

L2 Functions > LLDP > 802.1 Extension TLV

This 802.1 Extension TLV page is used to configure the LLDP Port settings.

The screenshot shows the '802.1 Extension LLDP Port Settings' configuration page. At the top, there are dropdown menus for 'From Port' (set to 1) and 'To Port' (set to 52). Below these are four configuration fields: 'Port VLAN ID' (disabled), 'VLAN Name' (disabled), 'VLAN ID' (empty), and 'Protocol Identity' (disabled). To the right of these fields are 'Refresh' and 'Apply' buttons. Below this section is a table titled 'Port' showing settings for ports 1 through 14. The table columns are 'Port', 'Port VLAN ID', 'VLAN ID', and 'Protocol Identity'. All entries in the table show 'Disabled' for 'Port VLAN ID' and '(None)' for both 'VLAN ID' and 'Protocol Identity'.

Port	Port VLAN ID	VLAN ID	Protocol Identity
1	Disabled	(None)	(None)
2	Disabled	(None)	(None)
3	Disabled	(None)	(None)
4	Disabled	(None)	(None)
5	Disabled	(None)	(None)
6	Disabled	(None)	(None)
7	Disabled	(None)	(None)
8	Disabled	(None)	(None)
9	Disabled	(None)	(None)
10	Disabled	(None)	(None)
11	Disabled	(None)	(None)
12	Disabled	(None)	(None)
13	Disabled	(None)	(None)
14	Disabled	(None)	(None)

Figure 4.75 – L2 Functions > LLDP > 802.1 Extension TLV 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.

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 ID or VLAN Name or all.

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 the **Apply** button to implement changes made and click **Refresh** to refresh the table information.

L2 Functions > LLDP > 802.3 Extension TLV

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.

Port	MAC/PHY Configuration/Status	Power Via MDI	Link Aggregation	Maximum Frame Size
1	Disabled	Disabled	Disabled	Disabled
2	Disabled	Disabled	Disabled	Disabled
3	Disabled	Disabled	Disabled	Disabled
4	Disabled	Disabled	Disabled	Disabled
5	Disabled	Disabled	Disabled	Disabled
6	Disabled	Disabled	Disabled	Disabled
7	Disabled	Disabled	Disabled	Disabled
8	Disabled	Disabled	Disabled	Disabled
9	Disabled	Disabled	Disabled	Disabled
10	Disabled	Disabled	Disabled	Disabled
11	Disabled	Disabled	Disabled	Disabled
12	Disabled	Disabled	Disabled	Disabled
13	Disabled	Disabled	Disabled	Disabled

Figure 4.76 – L2 Functions > LLDP > 802.3 Extension TLV

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 the **Apply** button to implement changes made and click **Refresh** to refresh the table information.

L2 Functions > LLDP > LLDP Management Address Settings

The LLDP Management Address Settings allows the user to set management address which is included in LLDP information transmitted.

Port	Enabled Management Address	Port State
01	None	Disabled
02	None	Disabled
03	None	Disabled
04	None	Disabled
05	None	Disabled
06	None	Disabled
07	None	Disabled
08	None	Disabled
09	None	Disabled
10	None	Disabled
11	None	Disabled
12	None	Disabled
13	None	Disabled
14	None	Disabled

Figure 4.77 – L2 Functions > LLDP > LLDP Management Address Settings

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

Address Type: Specifies the LLDP address type on the port. The value is always IPv4.

Address: Specifies the address.

Port State: Specifies 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 the **Apply** button to implement changes made.

L2 Functions > LLDP > LLDP Management Address Table

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

No.	Subtype	Management Address	IF Type	OID	Advertising Ports
1	IPv4	10.90.90.90	ifIndex	1.3.6.1.2.1.2.2.1.1	(NONE)

Figure 4.78 – L2 Functions > LLDP > LLDP Management Address Table

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

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

Subtype: Displays the managed address subtype. For example, MAC address or IPv4 address.

Management Address: Displays the IP address.

IF Type: Displays the IF Type.

OID: Displays the SNMP OID.

Advertising Ports: Displays the advertising ports.

L2 Functions > LLDP > LLDP Local Port Table

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

LLDP Local Port Brief Table				Safeguard	
Port	Port ID Subtype	Port ID	Port Description	Normal	Detailed
01	Interface Alias	Slot0/1	Ethernet Interface	View	View
02	Interface Alias	Slot0/2	Ethernet Interface	View	View
03	Interface Alias	Slot0/3	Ethernet Interface	View	View
04	Interface Alias	Slot0/4	Ethernet Interface	View	View
05	Interface Alias	Slot0/5	Ethernet Interface	View	View
06	Interface Alias	Slot0/6	Ethernet Interface	View	View
07	Interface Alias	Slot0/7	Ethernet Interface	View	View
08	Interface Alias	Slot0/8	Ethernet Interface	View	View
09	Interface Alias	Slot0/9	Ethernet Interface	View	View
10	Interface Alias	Slot0/10	Ethernet Interface	View	View
11	Interface Alias	Slot0/11	Ethernet Interface	View	View
12	Interface Alias	Slot0/12	Ethernet Interface	View	View
13	Interface Alias	Slot0/13	Ethernet Interface	View	View
14	Interface Alias	Slot0/14	Ethernet Interface	View	View

Figure 4.79 – L2 Functions > LLDP > LLDP Local Port Table

Port: Displays the port number.

Port ID Subtype: Displays the port ID subtype.

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

Port Description: Displays the port description.

Click **View** of Normal column to display more information.

LLDP Local Port Normal Table		Safeguard
No.	5	
Port Id Subtype	Interface Alias	
Port Id	Slot0/5	
Port Description	D-Link DGS-1210-52MP Rev.F1/6.00.005 Port 5	
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 4.80 – L2 Functions > LLDP > LLDP Local Port Normal Table

Click **View** of Detailed column to display detail information.

Port ID : 5

Port Id Subtype : Interface Alias
Port Id : Slot0/5
Port Description : D-Link DGS-1210-52MP Rev.F1/6.00.005 Port 5
Port PVID : 1
Management Address Count : 1
SubType : IPv4
Address : 10.90.90.90
IF Type : ifIndex
OID : 1.3.6.1.2.1.2.2.1.1
PPVID Entries Count : 0
(NONE)
VLAN Name Entries Count : 1
Entry : 1
VLAN ID : 1
VLAN Name : default
Protocol Identity Entries Count : 0
(NONE)
MAC/PHY Configuration/Status :
Auto-negotiation Support : Supported
Auto-negotiation Enabled : Disabled
Auto-negotiation Advertised Capability : 0000(hex)

[Show LLDP Local Port Brief Table](#)
[Show LLDP Local Port Normal Table](#)

Figure 4.81 – L2 Functions > LLDP > LLDP Local Port Detailed Table

L2 Functions > 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.

Port : 01 ▾

Port ID : 1

Remote Entities Count : 0
(NONE)

Normal : [View Normal](#)
Detailed : [View Detailed](#)

Figure 4.82 – L2 Functions > LLDP > LLDP Remote Port Table

To view the settings for a remote port, click **View Normal** and the following page displays.

The screenshot shows a web-based configuration interface for a D-Link Smart Managed Switch. The title bar at the top reads "LLDP Remote Port Normal Table". In the top right corner, there is a green circular icon with a white dot and the word "Safeguard". Below the title, the text "Port ID : 1" is displayed above a horizontal dashed line. Underneath the line, it says "Remote Entities Count: 0 (NONE)". At the bottom of the page, there are two blue hyperlinks: "Show LLDP Remote Port Brief Table" and "Show LLDP Remote Port Detailed Table".

Figure 4.83 – L2 Functions > 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		Safeguard
Port ID : 1		
Remote Entities Count : 0 (NONE)		
Show LLDP Remote Port Brief Table		
Show LLDP Remote Port Normal Table		

Figure 4.84 – L2 Functions > LLDP > LLDP Remote Port Detailed Table

L2 Functions > LLDP > LLDP Statistics

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

LLDP Statistics Table									Safeguard
LLDP Statistics System									
Last Change Time									
Number of Table Insert									
Number of Table Delete									
Number of Table Drop									
Number of Table Age Out									
LLDP Port Statistics									
<input type="button" value="Refresh"/> <input type="button" value="Clear"/>									
Port	TxPort Frames	RxPort Frames Discarded	RxPort Frames Errors	RxPort Frames	RxPort TLVs Discarded	RxPort TLVs Unrecognized	RxPort Ageouts		
1	0	0	0	0	0	0	0		
2	0	0	0	0	0	0	0		
3	0	0	0	0	0	0	0		
4	0	0	0	0	0	0	0		
5	25	0	0	0	0	0	0		
6	0	0	0	0	0	0	0		
7	0	0	0	0	0	0	0		
8	0	0	0	0	0	0	0		
9	0	0	0	0	0	0	0		
10	0	0	0	0	0	0	0		
11	0	0	0	0	0	0	0		
12	0	0	0	0	0	0	0		

Figure 4.85 – L2 Functions > LLDP > LLDP Statistics

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 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 an unknown 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.

Click **Refresh** to renew the page, and click **Clear** to clean out all statistics.

L3 Functions > IP Interface

The IP Interface page allows user to configure the IPv6 system settings.

IP Interface Settings							Safeguard																			
Interface Name	<input type="text"/>																									
VLAN Name	<input type="text"/>																									
IPv4 Address	<input type="text"/>																									
Netmask	<input type="text"/> 24 (255.255.255.0)																									
Interface Admin State	<input type="text"/> Enabled																									
<input type="button" value="Add"/>																										
<p>Maximum 4 entries.</p> <table border="1"> <thead> <tr> <th>Interface Name</th> <th>VLAN Name</th> <th>IPv4 Address</th> <th>Netmask</th> <th>Admin State</th> <th>Link State</th> <th>Edit</th> <th>IPv6</th> <th>Delete</th> </tr> </thead> <tbody> <tr> <td>System</td> <td>default</td> <td>10.90.90.90</td> <td>255.0.0.0</td> <td>Enabled</td> <td>Link Up</td> <td><input type="button" value="Edit"/></td> <td><input type="button" value="IPv6"/></td> <td><input type="button" value="Delete"/></td> </tr> </tbody> </table>									Interface Name	VLAN Name	IPv4 Address	Netmask	Admin State	Link State	Edit	IPv6	Delete	System	default	10.90.90.90	255.0.0.0	Enabled	Link Up	<input type="button" value="Edit"/>	<input type="button" value="IPv6"/>	<input type="button" value="Delete"/>
Interface Name	VLAN Name	IPv4 Address	Netmask	Admin State	Link State	Edit	IPv6	Delete																		
System	default	10.90.90.90	255.0.0.0	Enabled	Link Up	<input type="button" value="Edit"/>	<input type="button" value="IPv6"/>	<input type="button" value="Delete"/>																		

Figure 4.86 – L3 Functions > IP Interface

Interface Name: Specifies the name of IP interface.

VLAN Name: Specifies the VLAN name of IP interface.

IPv4 Address: Specifies the IPv4 address for the interface.

Netmask: Select the netmask of IP address.

Interface Admin State: Enables or disables the interface administration state.

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

Click the **Edit** button to modify the IP settings:

The screenshot shows the 'IP Interface Settings' page. At the top, there are input fields for 'Interface Name', 'VLAN Name', 'IPv4 Address', 'Netmask', and 'Interface Admin State'. Below these is a button labeled 'Add'. A note says 'Maximum 4 entries.' followed by a table with one row:

Interface Name	VLAN Name	IPv4 Address	Netmask	Admin State	Link State	Edit	IPv6	Delete
System	default	10.90.90.90	8 (255.0.0.1)	Enabled	Link Up	Apply	IPv6	Delete

Figure 4.87 – L3 Functions > IPv6 Interface Settings - Edit

IPv4 Address: Specifies the IPv4 address for the interface.

Netmask: Select the netmask of IP address.

Admin State: Enables or disables the interface administration state.

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

Click the **IPv6** button to configure the IPv6 interface settings:

The screenshot shows the 'IPv6 Interface Settings' page. It includes sections for 'IPv6 Interface Settings' (with fields for 'Interface Name' set to 'System', 'IPv6 State' set to 'Enabled', and 'DHCPv6 Client' set to 'Disabled'), 'NS Retransmit Time Settings' (with a field for 'NS Retransmit Time (1-3600)' set to '1'), 'Automatic Link Local State Settings' (with 'Automatic Link Local Address' set to 'Disabled'), and a section for 'View All IPv6 Address' (with a table header showing columns for 'Address Type', 'IPv6 Address', and 'Delete').

Figure 4.87 – L3 Functions > IPv6 Interface Settings – IPv6

IPv6 System Settings:

Interface Name: Displays the interface name of IPv6.

IPv6 State: Specifies the IPv6 to be enabled or disabled.

Interface Admin State: Displays the interface admin status.

DHCPv6 Client: Specifies the DHCPv6 client to be enabled or disabled.

IPv6 Network Address: Specifies the IPv6 Network Address.

NS Retransmit Time Settings:

NS Retransmit Time (1-3600): Enter the Neighbor solicitation's retransmit timer in second here. Specifies the NS retransmit time for IPv6. The field range is 1-3600, and default is 1 second.

Automatic Link Local State Settings:

Automatic Link Local Address: Specifies the automatic link is enabled or disabled.

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

L3 Functions > IPv6 Neighbor Settings

The user can configure the Switch's IPv6 neighbor settings. The Switch's current IPv6 neighbor settings will be displayed in the table at the bottom of this window.

Neighbor	Link Layer Address	Interface Name	State
Total Entries : 0			

Figure 4.88 – L3 Functions > IPv6 Neighbor Settings

Interface Name: Enter the interface name of the IPv6 neighbor.

Neighbor IPv6 Address: Specifies the neighbor IPv6 address.

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

Click **Apply** to implement changes made.

Interface Name: Specifies the interface name of the IPv6 neighbor. 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.

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

Click **Clear** to clear all the information entered in the fields.

L3 Functions > IPv4 Static Route

The Switch supports static routing for IPv4 formatted addressing. User can create up to 256 static route entries for IPv4. For IPv4 static routes, once a static route has been set, the Switch will send an ARP request packet to the next hop router that has been set by the user. Once an ARP response has been retrieved by the Switch from that next hop, the route becomes enabled. However, if the ARP entry already exists, an ARP request will not be sent.

The Switch also supports a floating static route, which means that the user may create an alternative static route to a different next hop. This secondary next hop device route is considered as a backup static route for when the primary static route is down. If the primary route is lost, the backup route will uplink and its status will become active. Entries into the Switch's forwarding table can be made using both an IP address subnet mask and a gateway.

The IPv4 Static Route page allows user to enable and configure the IPv4 route settings.

The screenshot shows the 'Static Route Settings' page. At the top, there is a radio button for 'IPv4 Static Route' with options 'Enabled' (selected) and 'Disabled'. Below this is a table with four rows: 'IPv4 Address' (empty), 'Netmask' (set to '24 (255.255.255.0)'), 'Gateway' (empty), and 'Metric (1-65535)' (empty). To the right of the table is an 'Apply' button. Below the table, a message says 'Total Entries : 0 / Active Entries : 0 / Inactive Entries : 0'. At the bottom, there is a horizontal menu bar with tabs: 'IPv4 Address', 'Netmask', 'Gateway', 'Metric', 'Protocol', 'Backup', 'Status', and 'Delete'. The 'IPv4 Address' tab is currently selected.

Figure 4.89 – L3 Functions > IPv4 Static Route

IPv4 Static Route: Specifies to enable or disable the IPv4 static route feature on the Switch.

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

IPv4 Address: Specifies an IPv4 address to be assigned to the static route.

Netmask: Specifies a subnet mask to be applied to the corresponding subnet mask of the IPv4 address.

Gateway: The corresponding IPv4 address for the next hop Gateway address in IPv4 format.

Metric: Represents the metric value of the IP interface entered into the table. This field may read a number between 1 and 65535.

Backup State: The user may choose between *Primary* and *Backup*. If the Primary Static Route fails, the Backup Route will support the entry. Please take note that the Primary and Backup entries cannot have the same Gateway.

Click **Add** to create a static route.

To create a new IPv4 static route entry for example, enter the configuration displayed below then click **Add**:

The screenshot shows the 'Static Route Settings' page. The 'IPv4 Static Route' is set to 'Enabled'. Below is a table with five rows: 'IPv4 Address' (set to '10.90.90.90'), 'Netmask' (set to '24 (255.255.255.0)'), 'Gateway' (set to '10.90.90.254'), 'Metric (1-65535)' (set to '2'), and 'Backup State' (set to 'Primary'). To the right of the table is an 'Add' button. Below the table, a message says 'Total Entries : 0 / Active Entries : 0 / Inactive Entries : 0'. At the bottom, there is a horizontal menu bar with tabs: 'IPv4 Address', 'Netmask', 'Gateway', 'Metric', 'Protocol', 'Backup', 'Status', and 'Delete'. The 'IPv4 Address' tab is currently selected.

Figure 4.90 – L3 Functions > IPv4 Static Route – Add

The new entry will be displayed in the IPv4 static route table:

The screenshot shows the 'Static Route Settings' page. The 'IPv4 Static Route' is set to 'Enabled'. Below is a table with eight columns: 'IPv4 Address', 'Netmask', 'Gateway', 'Metric', 'Protocol', 'Backup', 'Status', and 'Delete'. There is one entry: '10.90.90.90' (IPv4 Address), '255.255.255.0' (Netmask), '10.90.90.254' (Gateway), '2' (Metric), 'Static' (Protocol), 'Primary' (Backup), and 'Inactive' (Status). To the right of the table is an 'Add' button. Below the table, a message says 'Total Entries : 1 / Active Entries : 0 / Inactive Entries : 1'. At the bottom, there is a horizontal menu bar with tabs: 'IPv4 Address', 'Netmask', 'Gateway', 'Metric', 'Protocol', 'Backup', 'Status', and 'Delete'. The 'IPv4 Address' tab is currently selected.

Figure 4.91 – L3 Functions > IPv4 Static Route – Static Route Table

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

L3 Functions > IPv4 Routing Table Finder

The IPv4 Routing Table Finder page shows the current IPv4 routing table of the Switch. To find a specific IPv4 route, enter and IPv4 address into the **Network Address** field and click the **Search** button.

IPv4 Routing Table Finder					
Network Address		Ex:(172.18.208.11 or 172.18.208.11/24)		Search	
Total Entries : 0					
IP Address 10.0.0.0	Netmask 255.0.0.0	Gateway 0.0.0.0	Interface Name System	Metric 1	Protocol Local

Figure 4.92 – L3 Functions > IPv4 Routing Table Finder

L3 Functions > IPv6 Static Route

The IPv6 Static Route page allows user to enable and configure the IPv6 route settings.

IPv6 Static Route Settings						
<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled						
IPv6 Address/Prefix Length Nexthop Address (e.g.: 3FFE::1) Metric (1-65535) Backup State Primary						
Total Entries : 0						
IPv6 Address/Prefix	Next Hop	Metric	Protocol	Backup	Status	Delete

Figure 4.93 – L3 Functions > IPv6 Static Route

IPv6 Static Route: Specifies to enable or disable the IPv6 static route feature on the Switch.

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

IPv6 Address/Prefix Length: Specifies that packets matching that address will be translated.

Nexthop Address: Specifies the corresponding IPv6 address for the next hop gateway address in IPv6 format.

Metric (1-65535): Specifies a metric of the IPv6 interface into the table representing the number of routers between the Switch and the IPv6 address above. The value ranges between 1 and 65535.

Backup State: Each IP address can only have one primary route, while other routes should be assigned to the backup state. When the primary route failed, switch will try the backup routes according to the order learnt by the routing table until route success. The field represents the Backup state that the Static and Default Route is configured for.

Click **Add** to create a new IPv6 Static Route.

L3 Functions > IPv6 Routing Table Finder

The IPv6 Routing Table Finder page shows the current Ipv6 routing table of the Switch. To find a specific Ipv6 route, enter and IPv6 address into the **IPv6 Network Address** field and click **Search**.

IPv6 Routing Table Finder						
IPv6 Network Address		Ex:(1234::1234 or 1234::1234/64)		Search		
Total Entries : 0						
IPv6 Address/Prefix	Next Hop	Interface Name	Protocol	Backup	Metric	Status

Figure 4.94 – L3 Functions > IPv6 Routing Table Finder

IPv6 Network Address: Specifies the IPv6 address.



NOTE: The Static Route settings and Routing Table Finder of Ipv4 / IPv6 need to be configured with different setting pages.

L3 Functions > ARP > ARP Table Global Settings

The ARP Table Global Settings page displays the current ARP entries on the Switch. The table allows network managers to view, define, modify, and delete ARP information for specific device. Static entries can be defined in the ARP table. When static entries are defined, a permanent entry is entered and is used to translate IP addresses to MAC addresses.

ARP Table Global Settings
 Safeguard

Global Settings					
ARP Aging Time (0-65535) <input type="text" value="5"/> min <input type="button" value="Apply"/>					
Interface Name <input type="text"/> IP Address <input type="text"/> MAC Address <input type="text"/> <input type="button" value="Search"/>					
Static ARP entries used/maximum:0/384 <input type="button" value="Select All"/> <input type="button" value="Clear"/> <input type="button" value="Apply"/>					
ID	Interface Name	IP Address	MAC Address	Type	Add to Static ARP
01	System	10.0.0.0	ff-ff-ff-ff-ff-ff	Static	<input type="checkbox"/>
02	System	10.90.90.90	4a-6f-6e-01-01-01	Static	<input type="checkbox"/>
03	System	10.90.90.96	3c-97-0e-e5-76-4d	Dynamic / Inactive	<input type="checkbox"/>
04	System	10.255.255.255	ff-ff-ff-ff-ff-ff	Static	<input type="checkbox"/>

Page

Figure 4.95 – L3 Functions > ARP > ARP Table Global Settings

Global Settings:

ARP Aging Time (0-65535): Specifies the ARP entry age-out time, in minutes. The default is 5 minutes.

Interface Name: Enter or view the Interface name used.

IP Address: Enter or view the IP Address used.

MAC Address: Enter or view the MAC address used.

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

Click the **Select All** button to

Click the **Clear** button to remove the entry listed in the table.

L3 Functions > ARP > Static ARP Settings

The Address Resolution Protocol is a TCP/IP protocol that converts IP address into physical addresses. The table allows network managers to view, define, modify, and delete ARP information for specific device. Static entries can be defined in the ARP table. When static entries are defined, a permanent entry is entered and is used to translate IP addresses to MAC addresses.

Total Entries : 0				
Interface Name	IP Address	MAC Adress	Type	Delete
System	10.0.0.0	FF-FF-FF-FF-FF-FF	LOCAL/BROADCAST	<input type="button" value="Delete"/>
System	10.90.90.90	4A-6F-6E-01-01-01	LOCAL	<input type="button" value="Delete"/>
System	10.255.255.255	FF-FF-FF-FF-FF-FF	LOCAL/BROADCAST	<input type="button" value="Delete"/>

Figure 4.96 – L3 Functions > ARP > Static ARP Settings

IP Address: Specifies the IP address.

MAC Address: Specifies the MAC address.

Click the **Add** button to create a static ARP entry.

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

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

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.

Port	Tx Rate (Kbits/sec)	Rx Rate (Kbits/sec)
01	No Limit	No Limit
02	No Limit	No Limit
03	No Limit	No Limit
04	No Limit	No Limit
05	No Limit	No Limit
06	No Limit	No Limit
07	No Limit	No Limit
08	No Limit	No Limit
09	No Limit	No Limit
10	No Limit	No Limit
11	No Limit	No Limit
12	No Limit	No Limit
13	No Limit	No Limit

Figure 4.97 – 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 you 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 you to specify that the selected port will have no bandwidth limit.

Enabled disables the limit.

Rate (64-1024000): This field allows you to enter the data rate, in Kbits per second, will be the limit for the selected port. The value is between 64 and 1024000.

Click **Apply** to set the bandwidth control for the selected ports.

QoS > 802.1p/DSCP/ToS

QoS is an implementation of the IEEE 802.1p standard that allows network administrators to reserve bandwidth for important functions that require a larger bandwidth or that might have a higher priority, such as VoIP (voice-over Internet Protocol), web browsing applications, file server applications or video conferencing. Thus with larger bandwidth, less critical traffic is limited, and therefore excessive bandwidth can be saved.

The following figure displays the status of Quality of Service priority levels of each port, higher priority means the traffic from this port will be first handled by the switch. For packets that are untagged, the switch will assign the priority depending on your configuration.

The screenshot shows the '802.1p Priority Settings' configuration page. At the top, there are dropdown menus for 'Select QoS Mode' (set to '802.1p') and 'Queuing mechanism' (set to 'Strict Priority'). Below these are two tables. The first table shows port priorities for 24 ports (01 to 24) across eight priority classes (Class-0 to Class-7). The second table shows the mapping between 802.1p priority (0 to 7) and queue numbers (0 to 7). A note states: 'For ingress untagged packets, the per port "Default Priority" settings will be applied to packets of each port to provide port-based traffic prioritization.' Another note says: 'For ingress tagged packets, D-Link Smart Switches will refer to their 802.1p information for prioritization.'

Port	Priority
01	0
02	0
03	0
04	0
05	0
06	0
07	0
08	0
09	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0
17	0
18	0
19	0
20	0
21	0
22	0
23	0
24	0

802.1p priority	0	1	2	3	4	5	6	7
Queue number	2	0	1	3	4	5	6	7

Note: Queue priority from low to high is 0 to 7

Figure 4.98 – QoS > 802.1p/DSCP/ToS

Select QoS Mode: Specifies the QoS mode to be 802.1p, DSCP or ToS.

Queuing Mechanism:

Strict Priority: Denoting a Strict scheduling will set the highest queue to be emptied first while the other queues will follow the weighted round-robin scheduling scheme

WRR: Use the weighted round-robin (WRR) algorithm to handle packets in an even distribution in priority classes of service.

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

From Port / To Port: Defines the port range which the port packet priorities are defined.

Priority: Defines the priority assigned to the port. The priority range is between 0 and 7 with 0 being assigned to the lowest priority and 7 assigned to the highest.

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

Security > Trusted Host

Use Trusted Host function to manage the switch from a remote station. You can enter up to ten designated management stations networks by defining the IPv4 Address/Netmask or IPv6 Address/Prefix as seen in the

figure below. The first thing after the function is enabled is to add your local host IP address as a trusted host. Otherwise, you may lose the connection.

The screenshot shows the 'Trusted Host Settings' section. It includes a radio button for 'Enabled' (selected) and 'Disabled'. Below are fields for 'IPv4 Address' (24.255.255.0) and 'Netmask' (24 (255.255.255.0)), and 'IPv6 Address' with 'Prefix' (1-128). A note says 'Please add your local host IP address first to make it trusted. Otherwise, the connection will be stopped.' An 'Apply' button is at the top right, and an 'Add' button is on the right side of the address fields. Below is a 'Trusted Host Table' with a note 'Maximum 10 entries.' and a table with columns 'ID', 'IP Address', 'Netmask/Prefix', and 'Delete'.

Figure 4.99 Security > Trusted Host

Trusted Host: Specifies the Trusted Host to be enabled or disabled. The default is disabled.

To define a management station IP setting, click the **Add** button and type in the IP address and Subnet mask. Click the **Apply** button to save your settings. You may permit only single or a range of IP addresses by different IP mask setting, the format can be either 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 > 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 can not be changed once the port lock is enabled. Using the drop-down menu, change **Admin State** to *Enabled*, input Max Learning Address, and then click **Apply**.

The screenshot shows the 'Port Security' page. It has fields for 'From Port' (01), 'To Port' (52), 'Admin State' (Disabled), and 'Max Learning Address (0-64)' (0). An 'Apply' button is at the top right. Below is a 'Port Security' table with columns 'Port', 'Admin State', and 'Max Learning Address'.

Port	Admin State	Max Learning Address
01	Disabled	0
02	Disabled	0
03	Disabled	0
04	Disabled	0
05	Disabled	0
06	Disabled	0
07	Disabled	0
08	Disabled	0
09	Disabled	0
10	Disabled	0
11	Disabled	0
12	Disabled	0
13	Disabled	0
14	Disabled	0
15	Disabled	0

Figure 4.100 – Security > Port Security

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.

The screenshot shows the 'Traffic Segmentation Settings' page. At the top, there is a header bar with a 'Safeguard' button. Below it is a section titled 'Forwarding Port Settings' with a 'From Port' dropdown set to 'All'. There are two radio buttons: 'Enabled' (unchecked) and 'Disabled' (checked). To the right are 'Apply' and 'Cancel' buttons. Below this is a table with two rows: 'To Port' and 'From Port'. The 'To Port' row lists ports 01 through 26, and the 'From Port' row lists ports 27 through 52. A 'Forwarding Port Table' follows, showing a mapping from each port number to a range of forwarding ports (1-52). The table has columns for 'Port' and 'Forwarding Port'.

Port	Forwarding Port
1	1-52
2	1-52
3	1-52
4	1-52
5	1-52
6	1-52
7	1-52
8	1-52
9	1-52
10	1-52
11	1-52

Figure 4.101 – Security > Traffic Segmentation

Forwarding Port Settings: Click **Enabled** or **Disabled** and click **Apply** to configure this feature.

From Port: Use the drop-down menu to select a port or all ports from that switch. This is the port that will be transmitting packets.

To Port: Click the box of ports and will be able to forward packets. These ports will be allowed to receive packets from the port specified above.

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

Click **Select All** button to check all ports or click **Clear** button to uncheck all ports.

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 Web-Smart Switch from being interrupted by malicious viruses or worm attacks. This option is enabled by default.

The screenshot shows the 'Safeguard Engine Settings' page. It features a 'Safeguard Engine State' section with 'Enabled' checked and 'Disabled' unchecked, followed by an 'Apply' button. Below this is a note: 'D-Link Safeguard Engine is a robust and innovative technology developed by D-Link, which will automatically throttle the impact of packet flooding into the switch's CPU. It will keep D-Link Switches better protected from being too frequently interrupted by malicious viruses or worm attacks.' The note includes a small icon of a shield.

Figure 4.102 – Security > Safeguard Engine

Security > Storm Control

The Storm 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.

Storm Control Settings

Storm Control Enabled Disabled

Storm Control Type: Multicast & Broadcast & Unknown Unica...

Threshold (16Kbps * N): 16Kbps * 1 = 16 Kbps

Apply

Figure 4.103 – Security > Storm Control

Storm Control Type: User can select the different Storm type from Broadcast Only, Multicast & Broadcast, and Multicast & Broadcast & Unknown Unicast.

Threshold (16Kbps * N): If storm control is enabled (default is disabled), the threshold is from of 16 ~ 1,024,000 Kbit per second, with steps (N) of 16Kbps. N can be from 1 to 64000.

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

Security > ARP Spoofing Prevention

ARP spoofing, also known as ARP poisoning, is a method to attack an Ethernet network by allowing an attacker to sniff data frames on a LAN, modifying the traffic, or stopping the traffic (known as a Denial of Service – DoS attack). The main idea of ARP spoofing is to send fake or spoofed ARP messages to an Ethernet network. It associates the attacker's or random MAC address with the IP address of another node such as the default gateway. Any traffic meant for that IP address would be mistakenly re-directed to the node specified by the attacker.

A common DoS attack today can be done by associating a nonexistent or specified MAC address to the IP address of the network's default gateway. The malicious attacker only needs to broadcast one gratuitous ARP to the network claiming to be the gateway, so that the whole network operation is turned down as all packets to the Internet will be directed to the wrong node.

The ARP Spoofing Prevention function can discard the ARP Spoofing Attack in the network by checking the gratuitous ARP packets and filtering those with illegal IP or MAC addresses.

ARP Spoofing Prevention Settings

IP Address: [] MAC Address: [] Ports: [] Ex:(1,2,4-6) Add

Total Entries: 0 Delete All

IP Address	MAC Address	Ports	Delete

ARP is the standard for finding a host's MAC address. However, this protocol is vulnerable that cracker can spoof the IP and MAC information in the ARP packets to attack a LAN.

The main purpose of this feature is to protect network from Man-in-the-Middle or ARP spoofing attack including router / gateway or specific client.

Figure 4.104 – Security > ARP Spoofing Prevention

Enter the **IP Address**, **MAC Address**, **Ports** and then click **Add** to create a checking/filtering rule. Click **Delete** to remove an existing rule and **Delete All** to clear all the entries.

Security > DHCP Server Screening

DHCP Server Screening function allows user to restrict the illegal DHCP server by discarding the DHCP service from distrusted ports. This page allows you to configure the DHCP Server Screening state for each port and designed trusted DHCP server IP address. Select **Ports** and then click **Apply** to enable or disable the function.

Port	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
Port	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Port	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Trusted DHCP Server IP Settings

IPv4

IPv6 Ex:(1234::1234)

Trusted DHCP Server IP Lists

Maximum 5 entries.

Index	IP Address	Delete

Figure 4.105 – Security > DHCP Server Screening

Trusted DHCP Server IP Settings: Select IPv4 or IPv6 and specify the IP address then click **Add** to create Trusted DHCP Server. For default, the ports are all enabled of trusted DHCP Server.

Click **Add** to add a trusted DHCP server.

Security > SSL/TLS

Secure Sockets Layer (SSL) is a security feature that provides a secure communication path between a Web Management host and the Switch Web UI by using authentication, digital signatures and encryption. These security functions are implemented by Ciphersuite, a security string that determines the cryptographic parameters, encryption algorithms and key sizes to be used for an authentication session and consists of three levels: key exchange, encryption and has algorithm.

This page allows you to configure the SSL global state and the Ciphersuite settings. Select **Enable** or **Disable** and then click **Apply** to change the SSL state or the Ciphersuite settings of the Switch. By default, SSL is **Disabled** and all Ciphersuites are **Enabled**.

SSL/TLS Settings

SSL State Enabled Disabled

HTTP will be disabled if SSL is enabled.

SSL Ciphersuite Settings

ECDHE-RSA-AES128-SHA	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
ECDHE-ECDSA-AES256-SHA	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
DHE-RSA-AES256-SHA	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
ECDHE-RSA-AES256-SHA	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
ECDHE-ECDSA-AES128-SHA	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
DHE-RSA-AES128-SHA	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
RSA-AES128-SHA	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
RSA-AES256-SHA	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled

Figure 4.106 – Security > SSL/TLS



NOTE: When SSL is enabled, it will take longer time to open a web page due to encryption and HTTP will be disabled.

Version of the SSL protocol which listed below:

Version	Description
SSL v2.0	First SSL protocol for which implementations exist.
SSL v3.0	Revision to prevent specific security attack, add non-RSA ciphers and support for certificate chains.
TLS v1.0	Revision of SSL 3.0 to update the MAC layer to HMAC, add block padding for block ciphers, message order standardization and more alert messages.
TLS V1.2	Revision to 1.2 of Transport Layer Security (TLS) protocol. The TLS protocol provides communications security over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.



NOTE: The DGS-1210 series support TLS 1.2, TLS 1.1 and do not support SSL v3.0.

SSL (Secure Sockets Layer) is the secure communications protocol of choice for a large part of the Internet community. There are many applications of SSL in existence, since it is capable of securing any transmission over TCP.

Transport Layer Security (TLS), is the successor to SSL and provides much the same functionality. It ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message.

Hyper Test Transfer Protocol Secure (HTTPS) is the secure version of HTTP which is often used to protect highly confidential information, enhance encryption and authentication, and running on top of SSL/TLS. HTTPS is used to secure web browsing service between a browser and a web server.

To browse the web via HTTPS with highly encryption and authentication, select **Enabled** and click **Apply** button to enable SSL state and the HTTP will be disabled.

Safeguard
SSL/TLS Settings

SSL State

Enabled
 Disabled
 HTTP will be disabled if SSL is enabled.

Apply

SSL Ciphersuite Settings	
ECDHE-RSA-AES128-SHA	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
ECDHE-ECDSA-AES256-SHA	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
DHE-RSA-AES256-SHA	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
ECDHE-RSA-AES256-SHA	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
ECDHE-ECDSA-AES128-SHA	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
DHE-RSA-AES128-SHA	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
RSA-AES128-SHA	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
RSA-AES256-SHA	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Apply

Figure 4.107 – Security > SSL Settings - Enable

SSL Ciphersuite Settings:

ECDHE-RSA-AES128-SHA: Specifies ECDHE and RSA key exchange with AES128 encryption and SHA hash is enabled or disabled.

ECDHE-ECDSA-AES256-SHA: Specifies ECDHE and ECDSA key exchange with AES256 encryption and SHA hash is enabled or disabled.

DHE-RSA-AES256-SHA: Specifies DHE and RSA key exchange with AES256 encryption and SHA hash is enabled or disabled.

ECDHE-RSA-AES256-SHA: Specifies ECDHE and RSA key exchange with AES256 encryption and SHA hash is enabled or disabled.

ECDHE-ECDSA-AES128-SHA: Specifies ECDHE and ECDSA key exchange with AES128 encryption and SHA hash is enabled or disabled.

DHE-RSA-AES128-SHA: Specifies DHE and RSA key exchange with AES128 encryption and SHA hash is enabled or disabled.

RSA-AES128-SHA: Specifies RSA key exchange with AES128 encryption and SHA hash is enabled or disabled.

RSA-AES256-SHA: Specifies RSA key exchange with AES256 encryption and SHA hash is enabled or disabled.

Enter https://10.90.90.90 to re-login the Web management page:



Figure 4.108 – Security > SSL Settings – HTTPS enable

Security > DoS Prevention Settings

The user can enable or disable the prevention of each DoS attacks. As long as user enables DoS Prevention, switch can stop the packet matching DoS Attachk Prevention type listed on below table. The packet matching will be done by hardware.

DoS Prevention Settings		Safeguard												
Prevention Settings														
State: <input type="button" value="Disabled ▾"/>		<input type="button" value="Apply"/>												
Prevention Settings														
Type	<input type="checkbox"/> Land Attack <input type="checkbox"/> TCP Xmascan <input type="checkbox"/> TCP SYN SrcPort less 1024	<input type="checkbox"/> TCP Null Scan <input type="checkbox"/> TCP SYNFIN <input type="checkbox"/> All												
State: <input type="button" value="Enabled ▾"/>		<input type="button" value="Apply"/>												
DoS Attack Prevention List														
<table border="1"> <thead> <tr> <th>DoS Type</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Land Attack</td> <td>Disabled</td> </tr> <tr> <td>Tcp Null Scan</td> <td>Disabled</td> </tr> <tr> <td>Tcp Xmascan</td> <td>Disabled</td> </tr> <tr> <td>Tcp Synfin</td> <td>Disabled</td> </tr> <tr> <td>Tcp Syn Srcport less 1024</td> <td>Disabled</td> </tr> </tbody> </table>		DoS Type	State	Land Attack	Disabled	Tcp Null Scan	Disabled	Tcp Xmascan	Disabled	Tcp Synfin	Disabled	Tcp Syn Srcport less 1024	Disabled	
DoS Type	State													
Land Attack	Disabled													
Tcp Null Scan	Disabled													
Tcp Xmascan	Disabled													
Tcp Synfin	Disabled													
Tcp Syn Srcport less 1024	Disabled													

Figure 4.109 – Security > DoS Prevention Settings

State: Specifies the state to be enabled or disabled.

Click **Apply** to implement changes made.

Prevention Settings:

Type: Selects the attack types to be prevented. The types are *Land Attack*, *TCP Null Scan*, *TCP Xmascan*, *TCP SYNFIN*, *TCP SYN SrcPortless 1024* or *All*.

State: Specifies the state to be enabled or disabled.

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

Security > SSH > SSH Settings

SSH is an abbreviation of Secure Shell, which is a program allowing secure remote login and secure network services over an insecure network. It allows a secure login to remote host computers, a safe method of executing commands on a remote end node, and will provide secure encrypted and authenticated communication between two non-trusted hosts. SSH, with its array of unmatched security features is an essential tool in today's networking environment. It is a powerful guardian against numerous existing security hazards that now threaten network communications.

The screenshot shows the 'SSH Settings' configuration page. At the top left is the title 'SSH Settings'. On the right is a green circular icon with a white dot labeled 'Safeguard'. Below the title are several configuration fields:

- SSH Global Settings**
- SSH State:** A radio button group where 'Enabled' is unselected and 'Disabled' is selected.
- Max. Session (1-4):** An input field containing the value '4'.
- Connection Timeout (120-600):** An input field containing the value '120 sec'.
- Authfail Attempts (2-20):** An input field containing the value '2 times'.
- Rekey Timeout:** A dropdown menu currently set to '60min'.

At the bottom right of the form is a grey rectangular button labeled 'Apply'.

Figure 4.110 – Security > SSH > SSH Settings

To configure the SSH server on the Switch, modify the following parameters and click **Apply**:

SSH State: Enabled or Disabled SSH on the Switch. The default is *Disabled*.

Max Session (1 - 4): Enter a value between 1 and 4 to set the number of users that may simultaneously access the Switch. The default setting is 1.

Connection Timeout (120 - 600): Allows the user to set the connection timeout. The user may set a time between 120 and 600 seconds. The default setting is 120 seconds.

Authfail Attempts (2 - 20): Allows the Administrator to set the maximum number of attempts that a user may try to log on to the SSH Server utilizing the SSH authentication. After the maximum number of attempts has been exceeded, the Switch will be disconnected and the user must reconnect to the Switch to attempt another login. The number of maximum attempts may be set between 2 and 20. The default setting is 2.

Rekey Timeout: Using the pull-down menu uses this field to set the time period that the Switch will change the security shell encryptions. The available options are *Never*, *10 min*, *30 min*, and *60 min*. The default setting is *60 min*.

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

Security > SSH > SSH Authmode and Algorithm Settings

The SSH Authentication and Algorithm Settings page allows user to configure the desired types of SSH algorithms used for authentication encryption.

SSH Authentication Mode Settings

Password Public Key Host Based

Encryption Algorithm

3DES-CBC

Data Integrity Algorithm

HMAC-MD5 HMAC-SHA1

Public Key Algorithm

HMAC-RSA

Apply

Figure 4.111 – Security > SSH > SSH Settings

SSH Authentication Mode Settings:

Password: Allows user to use a locally configured password for authentication on the Switch.

Public Key: This parameter may be enabled if the administrator wishes to use a public key configuration set on a SSH server, for authentication on the Switch.

Host Based: This parameter may be enabled if the administrator wishes to use a host computer for authentication. This parameter is intended for Linux users requiring SSH authentication techniques and the host computer is running the Linux operating system with a SSH program previously installed.

Encryption Algorithm:

3DES-CBC: Use the check box to enable or disable the Triple Data Encryption Standard encryption algorithm with Cipher Block Chaining. The default is enabled.

Data Integrity Algorithm:

HMAC-MD5: Use the check box to enable the supports of hash for message Authentication Code (HMAC) MD5 Message Digest (MD5) mechanism.

HMAC-SHA1: Use the check box to enable the supports of hash for message Authentication Code (HMAC) Secure Hash Algorithm (SHA) mechanism.

Public Key Algorithm:

HMAC-RSA: Use the check box to enable the supports of Hash for Message Authentication Code (HMAC) mechanism utilizing the RSA encryption algorithm.

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

Security > SSH > SSH User Authentication Lists

The SSH User Authentication Lists page is used to configure parameters for users attempting to access the Switch through SSH.

SSH User Authentication Lists					Safeguard
Total Entries : 1					
User Name	Auth. Mode	Host Name	Host IPv4	Host IPv6	
admin	Password				Edit

Host Name should be less than 33 characters.

Figure 4.112 – Security > SSH > SSH User Authentication Lists

The user may view the following parameters:

User Name: A name of no more than 15 characters to identify the SSH user. This User Name must be a previously configured user account on the Switch.

Auth. Mode: The administrator may choose one of the following to set the authorization for users attempting to access the Switch.

Host Based – This parameter should be chosen if the administrator wishes to use a remote SSH server for authentication purposes.

Password – This parameter should be chosen if the administrator wishes to use an administrator-defined password for authentication. Upon entry of this parameter, the Switch will prompt the administrator for a password, and then to re-type the password for confirmation.

Public Key – This parameter should be chosen if the administrator wishes to use the public key on an SSH server for authentication.

Host Name: Enter an alphanumeric string of no more than 32 characters to identify the remote SSH user. This parameter is only used in conjunction with the *Host Based* choice in the Auth. Mode field.

Host IPv4: Enter the corresponding IPv4 address of the SSH user. This parameter is only used in conjunction with the *Host Based* choice in the Auth. Mode field.

Host IPv6: Enter the corresponding IPv6 address of the SSH user. This parameter is only used in conjunction with the *Host Based* choice in the Auth. Mode field.

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 **Inspection packets** and **DHCP Snooping** on the Switch.

The screenshot shows the 'Smart Binding Settings' page. At the top, there are dropdown menus for 'From Port' (set to 01), 'To Port' (set to 52), and 'State' (set to 'Disabled'). Below these are two dropdown menus: 'Packet Inspection' (set to 'ARP Inspection') and 'DHCP Snooping' (set to 'Disabled'). An 'Apply' button is located to the right of the DHCP Snooping dropdown. Below these controls is a table titled 'IMPB Setting' with 13 rows, each representing a port from 01 to 13. The columns are 'Port', 'Admin State', 'Also inspect IP packets', and 'DHCP Snooping'. All ports are currently set to 'Disabled' in all three columns.

Port	Admin State	Also inspect IP packets	DHCP Snooping
01	Disabled	Disabled	Disabled
02	Disabled	Disabled	Disabled
03	Disabled	Disabled	Disabled
04	Disabled	Disabled	Disabled
05	Disabled	Disabled	Disabled
06	Disabled	Disabled	Disabled
07	Disabled	Disabled	Disabled
08	Disabled	Disabled	Disabled
09	Disabled	Disabled	Disabled
10	Disabled	Disabled	Disabled
11	Disabled	Disabled	Disabled
12	Disabled	Disabled	Disabled
13	Disabled	Disabled	Disabled

Figure 4.113 – 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.

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.

Packet Inspection: Specifies ARP Inspection or IP+ARP Inspection for the IP packets. If ARP inspection is selected, 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. If **ARP+ IP Inspection** mode is selected, 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.

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. This includes DHCPv6 snooping.

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

Security > Smart Binding > Smart Binding

The Smart Binding Settings page allows users to set IP-MAC-Port Binding entries by manually entering required information, or by scanning all connected devices and clicking to bind.

The screenshot shows the 'Smart Binding' configuration page. At the top, there's a 'Manual Binding' section with dropdowns for 'From Port' (01) and 'To Port' (01), and input fields for 'IP Address' and 'MAC Address'. A large 'Add' button is to the right. Below this is an 'Auto Scan' section with a note to enter a range of IP addresses. It has 'IP Address From' and 'To' fields, a 'Scan' button, and checkboxes for 'Select All', 'Clear All', and 'Apply'. At the bottom, there are tabs for 'VLAN', 'IP Address', 'MAC Address', 'Port', and 'Binding', with 'Binding' currently selected.

Figure 4.114 – Security > Smart Binding > Smart Binding

The Manual Binding Settings contains the following fields:

From Port / To Port: Specifies the switch port ranges for which to configure this IP-MAC binding entry (IP Address + MAC Address).

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: The Auto Scan Setting can list connected devices and easily select to bind. It contains the following fields:

IP Address From/To: Specifies the range of IP Address to find desired devices, or leaves the fields blank to see all connected devices.

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 is 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. You can cancel a device's authorization by deleting it from the table.

The screenshot shows the 'White List' configuration page. It has a header with 'White List' and 'Safeguard'. Below is a table with columns for 'Total Entries: 0', 'IP Address', 'Mac Address', 'Port', and 'Delete'. At the bottom are buttons for 'Delete', 'Select All', and 'Clean'.

Figure 4.115 – Security > Smart Binding > White List

Select the check box of entry then click **Delete** to remove it.

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.

VID	IP Address	Mac Address	Port	
-----	------------	-------------	------	--

Figure 4.116 – Security > Smart Binding > Black List

By giving conditions, desired devices information can be screened out below and 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 to.

Check a box of Delete column to release an entry from the forbidden list and 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

AAA > RADIUS Server

The RUAIUS Server of the Switch allows you to facilitate centralized user administration as well as providing protection against a sniffing, active hacker.

Index	IP Address	Auth-Port	Acct-Port	Timeout	Retransmit	Key	Delete
1							
2							
3							
4							
5							

Figure 4.117 – AAA > RADIUS Server

Index: Choose the desired RADIUS server to configure: 1, 2 or 3. The user can create maximum 5 RADIUS servers.

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

AAA > 802.1X > 802.1X Global 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.

Authentication State	<input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled
Forward EAPOL PDU	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Authentication Protocol	Local	
Apply		

Figure 4.118 – AAA > 802.1x Global Settings

Authentication State: Specifies to enable or disable the 802.1X function.

Forward EAPOL PDU: This is a global setting to control the forwarding of EAPOL PDU. When 802.1X functionality is disabled globally or for a port, and if 802.1X forward PDU is enabled both globally and for the port, a received EAPOL packet on the port will be flooded in the same VLAN to those ports for which 802.1X forward PDU is enabled and 802.1X is disabled (globally or just for the port). The default state is disabled.

Authentication Protocol: Indicates the 802.1X Protocol on the device. The possible field values are *Local* and *RADIUS*.

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

AAA > 802.1X > 802.1X Port Settings

To use EAP for security, set the 802.1X Port Settings for the Radius Server and applicable authentication information.

802.1X Port Settings

Safeguard

802.1X Port Access Control			
From Port	1	To Port	52
QuietPeriod (0-65535)	60	SuppTimeout (1-65535)	30 sec
ServerTimeout (1-65535)	30	MaxReq (1-10)	2 times
TxPeriod (1-65535)	30	ReAuthPeriod (1-65535)	3600 sec
ReAuthentication	Disabled	Port Control	ForceAuthorized
Capability	None	Direction	Both
<input type="button" value="Refresh"/> <input type="button" value="Apply"/>			

Port	AdmDir	Oper CriDir	Port Control	TxPeriod	Quiet Period	Supp - Timeout	Server - Timeout	MaxReq	ReAuth Period	ReAuth	Capability	Port Status	Session Time	U: I
1	Both	Both	Force Authorized	30	60	30	30	2	3600	Disabled	None	Unauthorized	0	**
2	Both	Both	Force Authorized	30	60	30	30	2	3600	Disabled	None	Unauthorized	0	**
3	Both	Both	Force Authorized	30	60	30	30	2	3600	Disabled	None	Unauthorized	0	**
4	Both	Both	Force Authorized	30	60	30	30	2	3600	Disabled	None	Unauthorized	0	**
5	Both	Both	Force Authorized	30	60	30	30	2	3600	Disabled	None	Unauthorized	0	**
6	Both	Both	Force Authorized	30	60	30	30	2	3600	Disabled	None	Unauthorized	0	**
7	Both	Both	Force Authorized	30	60	30	30	2	3600	Disabled	None	Unauthorized	0	**
8	Both	Both	Force Authorized	30	60	30	30	2	3600	Disabled	None	Unauthorized	0	**
9	Both	Both	Force Authorized	30	60	30	30	2	3600	Disabled	None	Unauthorized	0	**
10	Both	Both	Force Authorized	30	60	30	30	2	3600	Disabled	None	Unauthorized	0	**
11	Both	Both	Force Authorized	30	60	30	30	2	3600	Disabled	None	Unauthorized	0	**

Figure 4.119 – AAA > 802.1X > 802.1X Port Settings

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 – Specifies 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-5challneg) 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 – Specifies 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 the **Apply** button to implement changes made.

[AAA > 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.

The screenshot shows the '802.1X User' configuration page. At the top, there are input fields for 'User Name' (with a note 'Maximum 15 characters'), 'Password', and 'Confirm Password'. Below these is a button labeled 'Add'. A message 'Total Entries: 0' is displayed. A table follows, with columns for 'User Name' and 'Password'. The first row in the table has a 'Delete' button next to it. A 'Safeguard' icon is in the top right corner of the page header.

Figure 4.120 - AAA > 802.1X > 802.1X User

Click **Add** to add a new 802.1X user.

[ACL > ACL Wizard](#)

Access Control List (ACL) allows you to establish criteria to determine whether or not the Switch will forward packets based on the information contained in each packet's header. This criteria can be specified on a basis of the 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 200 Rules in total for the switch.

To create a new access rule, select **Create** and enter the **Access-List Name** then click **Next** button.

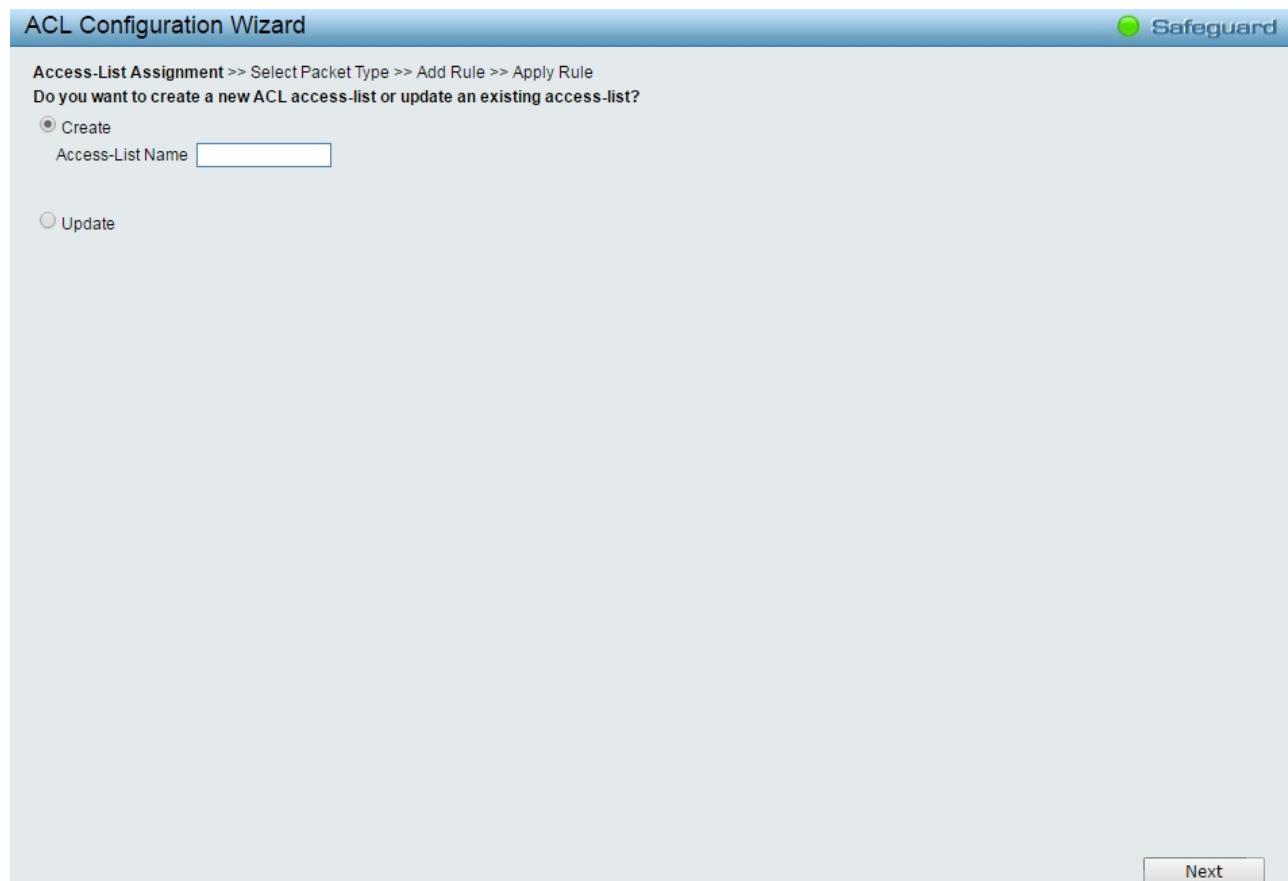


Figure 4.121 - ACL > ACL Wizard – Create Access-List

The steps of adding an access profile are described below:

- 1) Select the **Packet Type: MAC, IPv4 or IPv6**.

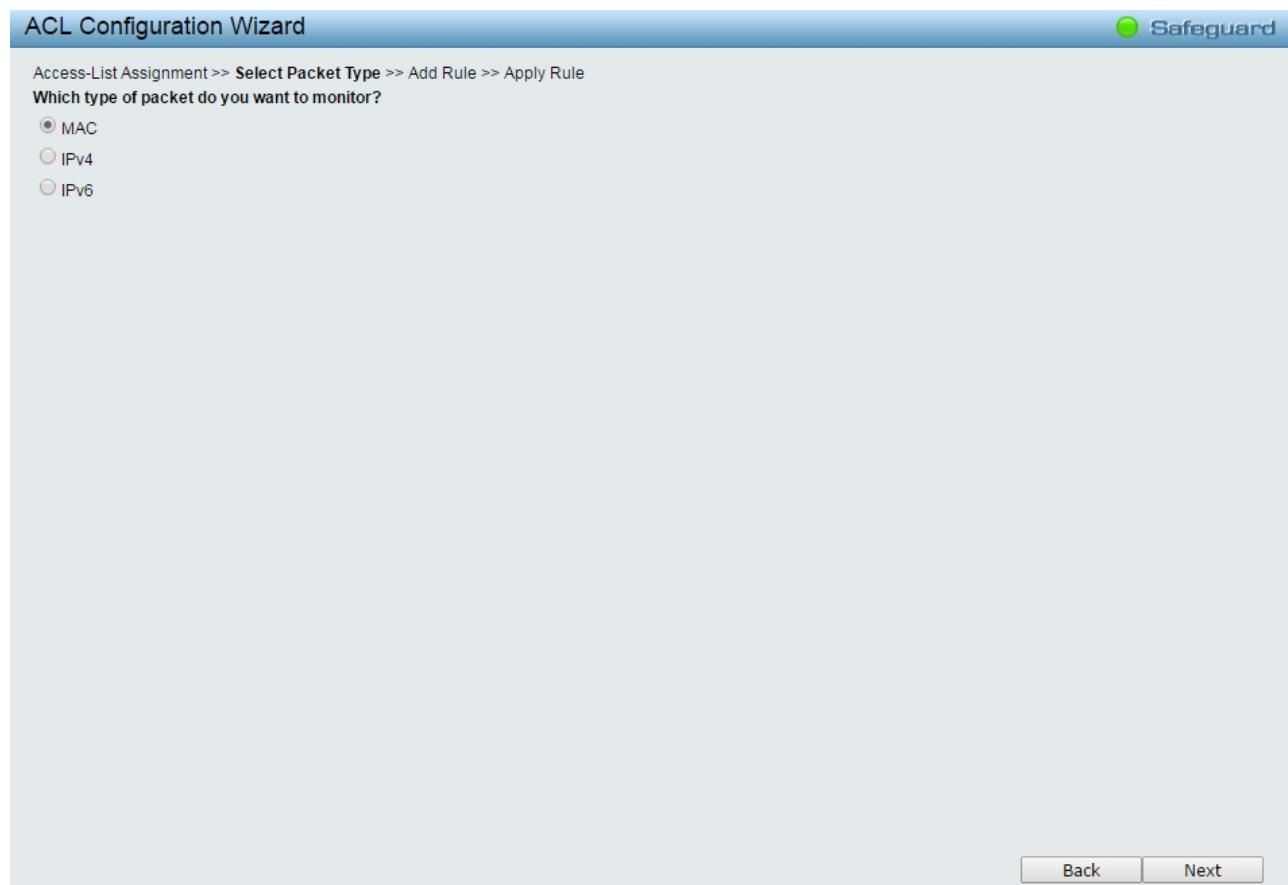


Figure 4.122 - ACL > ACL Wizard – Select Packet Type

Select packet type based on MAC address, IPv4 address, IPv6 address or packet content. This will change the window according to the requirements for the type of profile.

MAC: Defines the ACL profile Layer 2 protocols. Select MAC to monitor MAC address of each packet.

IPv4: Defines the IPv4 ACL profile protocols. Select IPv4 to monitor IPv4 address of each packet.

IPv6: Defines the IPv6 ACL profile protocols. Select IPv6 to monitor IPv6 address of each packet.

- **To define the MAC ACL Rule:** Select **MAC** click **Next** button. The updates to show the follows:

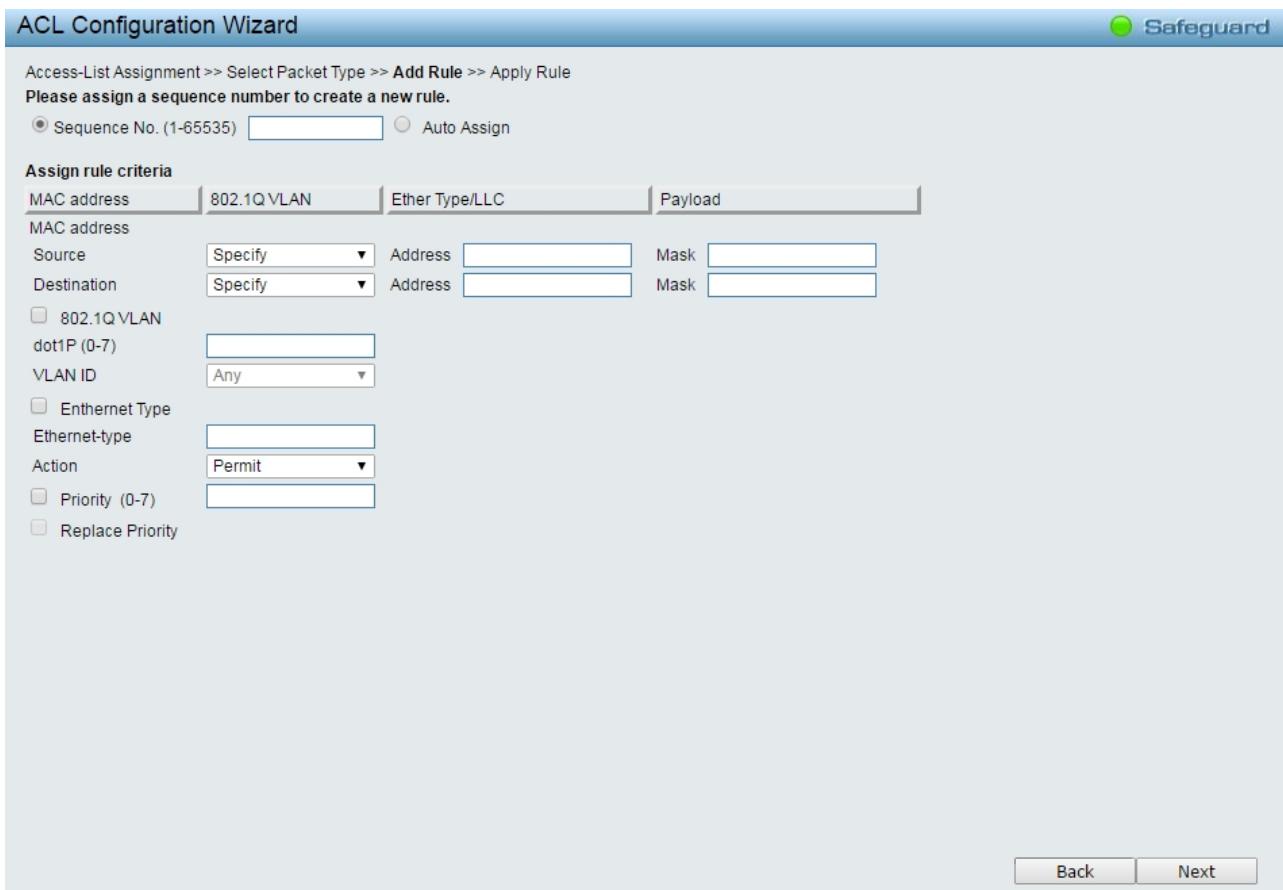


Figure 4.123 – Add Access Rule - MAC

Assign sequence number:

Sequence No. (1-65535): Specifies the sequence number. The value is from 1 to 65535.

Auto Assign: Auto assign the sequence number for a new rule.

Assign Rule Criteria: Specifies the MAC address settings.

Source: Select the source MAC to be specified or Any. Enter a source MAC address and source MAC mask, e.g. FF-FF-FF-FF-FF-FF.

Destination: Select the destination MAC to be specified or Any. Enter a destination MAC address and destination MAC mask, e.g. FF-FF-FF-FF-FF-FF.

If user selects the **802.1Q VLAN** box, then need to specify the **dot1p** and **VLAN ID**.

Dot1p (0-7): Specifies the dot1p priority.

VLAN ID: Selecting this option instructs the Switch to examine the 802.1p priority value of each packet header and use this as the, or part of the criterion for forwarding.

If user selects the **Ethernet Type** box, then need to specify the **Ethernet Type** and select the **Action**.

Ethernet Type: Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.

Action: Specifies 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.

Priority (0-7): Specifies the MAC ACL priority which values are 0-7.

Replace Priority: Check the box to enable the Replace Priority feature.

Click **Next** button then the ACL profile is added.

- To define the IPv4 ACL ICMP Rule: Select **IPv4** and click **Next** button. Select the **Protocol Type** to **ICMP**, the updates to show the follows:

The screenshot shows the 'ACL Configuration Wizard' interface for adding an access rule. At the top, it says 'Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Rule'. A note below says 'Please assign a sequence number to create a new rule.' There are two options for sequence number: 'Sequence No. (1-65535)' and 'Auto Assign' (which is selected). The 'Assign rule criteria' section includes tabs for 'L2 Header', 'TOS', 'IPv4 Address' (selected), and 'Protocol'. Under 'Protocol', 'Protocol Type' is set to 'ICMP'. Other fields include 'Source' and 'Destination' address and mask fields, and 'Source Port', 'Destination Port', and 'Code (0-255)' fields. The 'Action' dropdown is set to 'Permit'. At the bottom right are 'Back' and 'Next' buttons.

Figure 4.124 - Add Access Rule – IPv4 ICMP

Assign sequence number:

Sequence No. (1-65535): Specifies the sequence number. The value is from 1 to 65535.

Auto Assign: Auto assign the sequence number for a new rule.

Assign Rule Criteria: Specifies the IPv4 ACL settings.

ToS: Check the box to specify the ToS priority and DSCP value.

ToS (0-7): Specifies the ToS value.

DSCP (0-63): Specifies the DSCP value. The values are between 0 and 63.

IPv4 Address: Specifies the IPv4 Source and destination address.

Source: Select the source IP to be specified or Any relevant to the ACL rules. Enter a source IP address and source IP mask. For example, to set 176.212.XX.XX, use mask 255.255.0.0.

Destination: Select the destination IP to be specified or Any relevant to the ACL rules. Enter a destination IP address and destination IP mask. For example, to set 176.212.XX.XX, use mask 255.255.0.0.

Protocol: Check **Protocol** to configure the related settings.

Protocol Type: Select the protocol type for IPv4. The possible fields are **ICMP**, **IGMP**, **TCP**, **UDP** and **Protocol ID**.

ICMP Type (0-255): Sets the ICMP Type field as an essential field to match.

Code (0-255): Sets the ICMP code field as an essential field to match.

Select the ports which added into the **Access-List** and click **Next** button then the ACL profile was added.

- To define the IPv4 ACL IGMP Rule: Select IPv4 ACL and click Next button. Select the Protocol Type to IGMP, the updates to show the follows:

The screenshot shows the 'ACL Configuration Wizard' interface for adding an access rule. At the top, it says 'Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Rule'. Below that, it says 'Please assign a sequence number to create a new rule.' There are two radio buttons: 'Sequence No. (1-65535)' and 'Auto Assign', with 'Auto Assign' selected.

The 'Assign rule criteria' section has tabs for 'L2 Header', 'TOS', 'IPv4 Address', and 'Protocol'. The 'Protocol' tab is active. Under 'Protocol', the 'Protocol Type' dropdown is set to 'IGMP'. Other protocol-related fields include 'Protocol ID (0-255)', 'Source Port', 'Destination Port', 'ICMP Type (0-255)', and 'IGMP (0-255)'. An 'Action' dropdown is set to 'Permit'.

At the bottom right, there are 'Back' and 'Next' buttons.

Figure 4.125 - Add Access Rule – IPv4 IGMP

IGMP Type (0-255): Sets the IGMP Type field as an essential field to match.

Click **Next** button then the ACL profile is added.

- To define the IPv4 ACL TCP Rule: Select IPv4 ACL and click Next button. Select the Protocol Type to TCP, the updates to show the follows:

The screenshot shows the 'ACL Configuration Wizard' interface for adding an access rule. At the top, it says 'Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Rule'. A note says 'Please assign a sequence number to create a new rule.' There are two radio buttons: 'Sequence No. (1-65535)' and 'Auto Assign' (which is selected). Below this is a section titled 'Assign rule criteria' with tabs for 'L2 Header', 'TOS', 'IPv4 Address' (which is selected), and 'Protocol'. Under 'Protocol', 'TCP' is selected from a dropdown. Other protocol options like 'Protocol ID (0-255)', 'Source Port', 'Destination Port', 'ICMP Type (0-255)', and 'IGMP (0-255)' are also listed. The 'Action' dropdown is set to 'Permit'. At the bottom right are 'Back' and 'Next' buttons.

Figure 4.126 - Add Access Rule – IPv4 TCP

IPv4 Address: Defines the range of source Ports relevant to the ACL rules.

Source: Defines the range of source Ports relevant to the ACL rules. For example, to set 0 – 15, set mask of FFF0.

Destination: Defines the range of destination IP addresses, relevant to the ACL rules. For example, to set 0 – 15, set mask of FFF0.

Click **Next** button then the ACL profile is added.

- **To define the IPv4 ACL UDP Rule:** Select **IPv4 ACL** and click **Next** button. Select the **Protocol Type** to **UDP**, the updates to show the follows:

The screenshot shows the 'ACL Configuration Wizard' interface. At the top, it says 'Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Rule'. A note below says 'Please assign a sequence number to create a new rule.' There are two radio buttons: 'Sequence No. (1-65535)' and 'Auto Assign', with 'Auto Assign' selected.

Assign rule criteria:

- L2 Header:** ToS (selected)
- TOS:** ToS (0-7) (selected), input field:
- IPv4 Address:**
 - Source:** Specify, Address: Mask:
 - Destination:** Specify, Address: Mask:
- Protocol:** (checkbox checked)
- Protocol Type:** UDP (selected)
- Protocol ID (0-255):**
- Source Port:** Source Port Mask:
- Destination Port:** Destination Port Mask:
- ICMP Type (0-255):** Code (0-255):
- IGMP (0-255):**
- Action:** Permit (selected)
- Priority (0-7):**
- Replace Priority:**

At the bottom right are 'Back' and 'Next' buttons.

Figure 4.127 - Add Access Rule – IPv4 UDP

IPv4 Address: Defines the range of source Ports relevant to the ACL rules.

Source: Defines the range of source Ports relevant to the ACL rules. For example, to set 0 – 15, set mask of FFF0.

Destination: Defines the range of destination IP addresses, relevant to the ACL rules. For example, to set 0 – 15, set mask of FFF0.

Click **Next** button then the ACL profile is added.

- **To define the IPv4 ACL Protocol ID Rule:** Select **IPv4 ACL** and click **Next** button. Select the **Protocol Type** to **Protocol ID**, the updates to show the follows:

The screenshot shows the 'ACL Configuration Wizard' interface. At the top, it says 'Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Rule'. A note below says 'Please assign a sequence number to create a new rule.' There are two radio button options: 'Sequence No. (1-65535)' and 'Auto Assign'. The 'Auto Assign' option is selected.

Assign rule criteria:

- L2 Header:** Tos
- TOS:** Tos (0-7)
- IPv4 Address:**
 - Source:** Specify Address [] Mask []
 - Destination:** Specify Address [] Mask []
- Protocol:** (checkbox checked)
- Protocol Type:** Protocol ID (dropdown menu)
- Protocol ID (0-255):** []
- Source Port:** [] Source Port Mask []
- Destination Port:** [] Destination Port Mask []
- ICMP Type (0-255):** [] Code (0-255) []
- IGMP (0-255):** []
- Action:** Permit (dropdown menu)
- Priority (0-7):** []
- Replace Priority:** []

At the bottom right are 'Back' and 'Next' buttons.

Figure 4.128 - Add Access Rule – IPv4 Protocol ID

IPv4 Address: Defines the range of source Ports relevant to the ACL rules.

Source: Defines the range of source Ports relevant to the ACL rules. For example, to set 0 – 15, set mask of FFF0.

Destination: Defines the range of destination IP addresses, relevant to the ACL rules. For example, to set 0 – 15, set mask of FFF0.

Protocol ID (0-255) – Specifies the Protocol ID to be configured.

Click **Next** button then the ACL profile is added.



NOTE: A combination of one or several filtering masks can be selected simultaneously. The page updates with the relevant field(s).

- To define the IPv6 ACL ICMP rule: Select IPv6 ACL with ICMP of Protocol Type and click **Next** button. The updates to show the follows:

The screenshot shows the 'ACL Configuration Wizard' interface. At the top, it says 'Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Rule'. Below that, a note says 'Please assign a sequence number to create a new rule.' There are two radio button options: 'Sequence No. (1-65535)' with a text input field containing 'e' and 'Auto Assign'. The 'Assign rule criteria' section has tabs for 'L2 Header', 'Traffic Class', 'Next Header', and 'IPv6 Address', with 'Next Header' currently selected. Under 'Next Header', the 'Protocol Type' is set to 'ICMP'. Other fields include 'Protocol ID (0-255)', 'Source Port', 'Destination Port', 'ICMPv6 Type (0-255)', and 'IPv6 Address' (with 'Source' and 'Destination' dropdowns both set to 'Specify'). Action settings include 'Action' (set to 'Permit'), 'Priority (0-7)', and 'Replace Priority'. At the bottom right are 'Back' and 'Next' buttons.

Figure 4.129 - Add Access Rule – IPv6 ICMP

IPv6 Class (0-255): Specifies the class of access rule. The field range is from 0 to 255.

ICMPv6 Type: Sets the ICMP Type field as an essential field to match.

Code (0-255): Sets the ICMP code field as an essential field to match.

Source IPv6 Address: Defines the range of source IP addresses, relevant to the ACL rules. For example, to set 2002:0:0:0:0:b0d4:0, use mask 128.

Destination IPv6 Address: Defines the range of destination IP addresses, relevant to the ACL rules. For example, to set 2002:0:0:0:0:bf4d:0, use mask 128.

Action: Specifies 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.

Click **Next** button then the ACL profile is added.

- **To define the IPv6 ACL TCP profile:** Select **IPv6 ACL** with **TCP** of **Protocol Type** and click **Next** button. The updates to show the follows:

The screenshot shows the 'ACL Configuration Wizard' interface. At the top, it says 'Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Rule'. A note below says 'Please assign a sequence number to create a new rule.' There are two radio button options: 'Sequence No. (1-65535)' with a text input field containing 'e' and 'Auto Assign'. Below this is a section titled 'Assign rule criteria' with tabs: L2 Header (selected), Traffic Class, Next Header, and IPv6 Address. Under 'L2 Header', there are checkboxes for 'Traffic Class' (unchecked) and 'IPv6 Class (0-255)' (unchecked). The 'Next Header' tab is selected, showing 'Protocol Type' set to 'TCP', 'Protocol ID (0-255)' as a dropdown menu, 'Source Port' and 'Destination Port' fields, and 'ICMPv6 Type (0-255)' as a dropdown menu. Under 'IPv6 Address', there are sections for 'Source' and 'Destination' with dropdown menus 'Specify' and address fields, and 'Prefix Length' fields. Under 'Action', there is a dropdown menu set to 'Permit' and checkboxes for 'Priority (0-7)' (unchecked) and 'Replace Priority' (unchecked). At the bottom right are 'Back' and 'Next' buttons.

Figure 4.130 - Add Access Rule – IPv6 TCP

Source Port: Specifies the source port.

Source Port Mask: Defines the range of source IP addresses, relevant to the ACL rules. For example, to set 0 – 15, set mask of FFF0.

Destination Port: Specifies the destination port.

Destination Port Mask: Defines the range of destination IP addresses, relevant to the ACL rules. For example, to set 0 – 15, set mask of FFF0.

Click **Next** button then the ACL profile is added.

- **To define the IPv6 ACL UDP profile:** Select **IPv6 ACL** with **UDP** of **Protocol Type** and click **Next** button. The updates to show the follows:

The screenshot shows the 'ACL Configuration Wizard' interface. At the top, it says 'Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Rule'. Below that, it says 'Please assign a sequence number to create a new rule.' There are two radio buttons: 'Sequence No. (1-65535)' with a value of 'e' and 'Auto Assign'. The 'Assign rule criteria' tab is selected, showing tabs for L2 Header, Traffic Class, Next Header, and IPv6 Address. Under 'Next Header', 'IPv6 Class (0-255)' is selected. Under 'Protocol Type', 'UDP' is selected. Under 'Source Port', there is a field. Under 'Destination Port', there is a field. Under 'Action', 'Permit' is selected. At the bottom right, there are 'Back' and 'Next' buttons.

Figure 4.131 - Add Access Rule – IPv6 UDP

Source Port: Specifies the source port.

Source Port Mask: Defines the range of source IP addresses, relevant to the ACL rules. For example, to set 0 – 15, set mask of FFF0.

Destination Port: Specifies the destination port.

Destination Port Mask: Defines the range of destination IP addresses, relevant to the ACL rules. For example, to set 0 – 15, set mask of FFFF.

Click **Next** button then the ACL profile is added.

- **To define the IPv6 ACL Protocol ID profile:** Select **IPv6 ACL** with **Protocol ID** of **Protocol Type** and click **Next** button. The updates to show the follows:

The screenshot shows the 'ACL Configuration Wizard' interface. At the top, it says 'Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Rule'. Below that, it says 'Please assign a sequence number to create a new rule.' There are two radio buttons: 'Sequence No. (1-65535)' with a text input field containing 'e' and 'Auto Assign'. The 'Assign rule criteria' tab is selected, showing tabs for 'L2 Header', 'Traffic Class', 'Next Header', and 'IPv6 Address'. The 'Next Header' tab is active, displaying fields for 'Protocol Type' (set to 'Protocol ID'), 'Protocol ID (0-255)', 'Source Port', 'Destination Port', 'ICMPv6 Type (0-255)', 'IPv6 Address', 'Source', and 'Destination'. Under 'Action', 'Permit' is selected. At the bottom right are 'Back' and 'Next' buttons.

Figure 4.132 - Add Access Rule – IPv6 Protocol ID

Source Port: Specifies the source port.

Source Port Mask: Defines the range of source IP addresses, relevant to the ACL rules. For example, to set 0 – 15, set mask of FFF0.

Destination Port: Specifies the destination port.

Destination Port Mask: Defines the range of destination IP addresses, relevant to the ACL rules. For example, to set 0 – 15, set mask of FFF0.

Source IPv6 Address: Defines the range of source IP addresses, relevant to the ACL rules. For example, to set 2002:0:0:0:0:b0d4:0, use mask 128.

Destination IPv6 Address: Defines the range of destination IP addresses, relevant to the ACL rules. For example, to set 2002:0:0:0:0:bf4d:0, use mask 128.

Action: Specifies 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.

Click **Next** button then the ACL profile is added.



NOTE: A combination of one or several filtering masks can be selected simultaneously. The page updates with the relevant field(s).

2) Selecting the field of interest will display the next page which shows the follows:

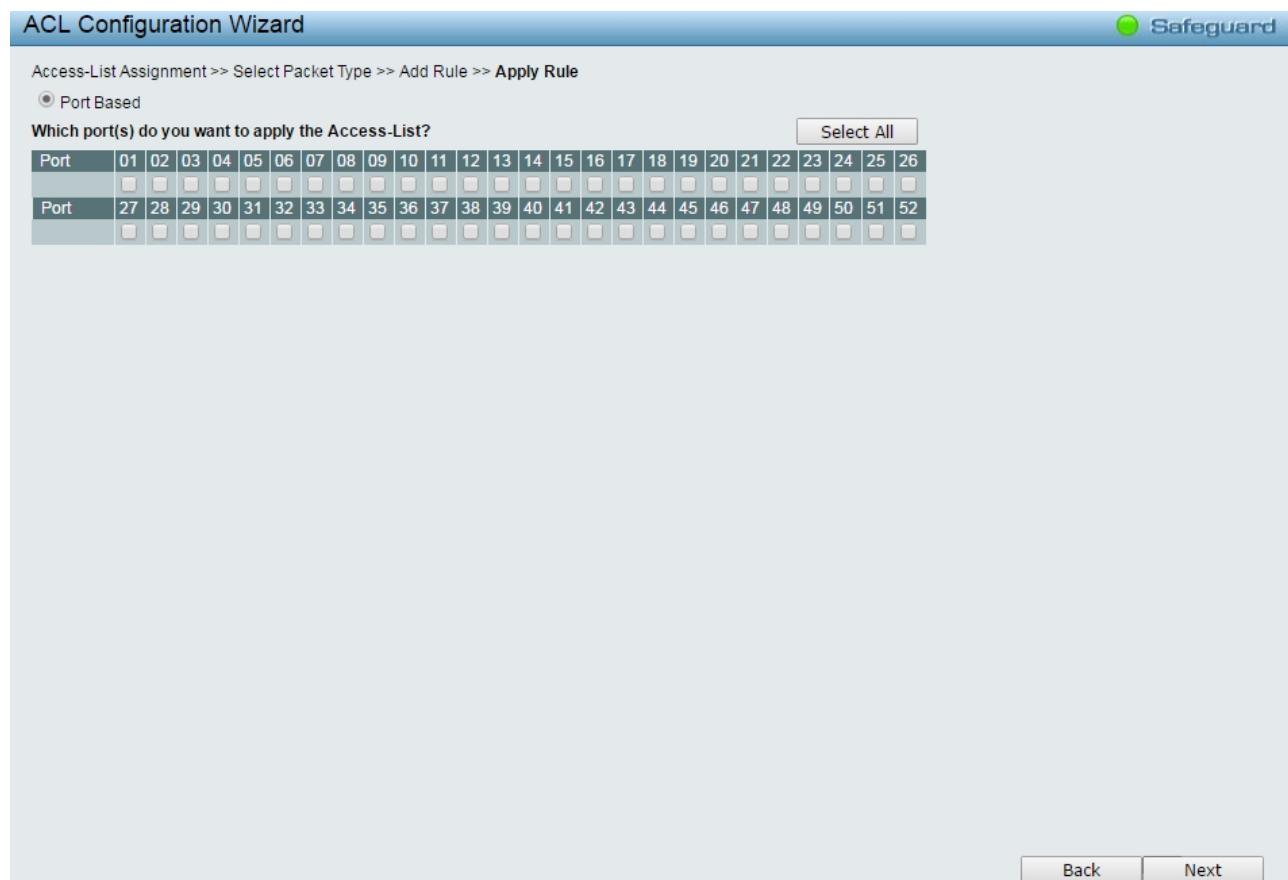


Figure 4.133 - Add Access Rule – Ports

Click **Next** button then the ACL profile is added.

3) To modify an existing rule, please select **Update** and the **Access-List Name** hyperlink and click **Next** button.

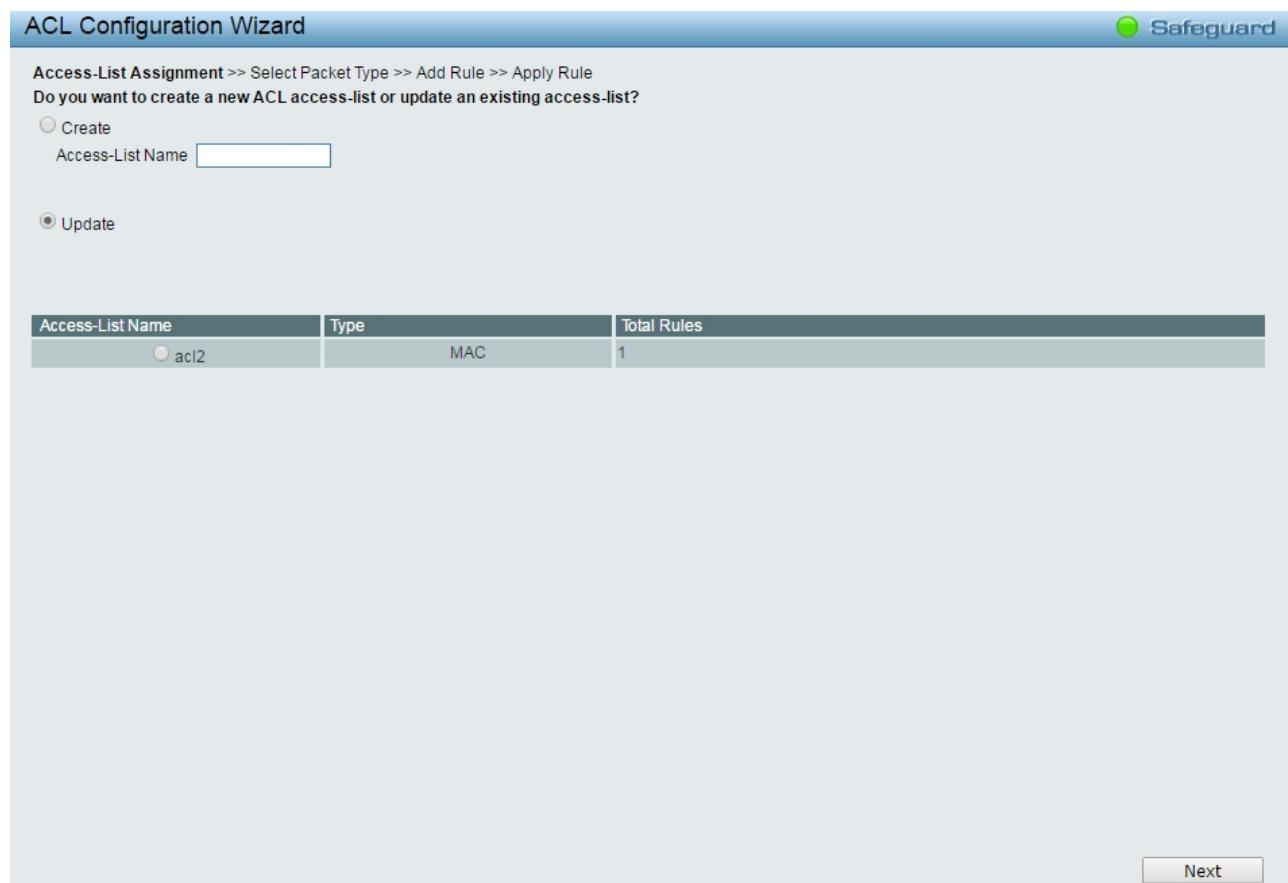


Figure 4.134 - ACL > ACL Wizard – Update ACL List

ACL > ACL Access List

The **ACL Access List** page provides information for configuring ACL Access manually. Click **Edit Rules** button to modify the access profile or click **Delete** button to remove the ACL profile.

ACL Access List			
		Safeguard	
<input type="button" value="Add"/> <input type="button" value="Delete All"/>		Current/Max. Profile: 1/50, Current/Max. Rule: 1/1280	
Access-List Name	Type	Total Rules	<input type="button" value="Edit Rules"/> <input type="button" value="Delete"/>
acl2	MAC	1	

Figure 4.135 - ACL > ACL Access List

To add a new profile, click **Add** button. The updates to show the follows:

Add ACL Profile

Access-List Name:

Packet Type: MAC
 IPv4
 IPv4 Extended
 IPv6

Figure 4.136 - ACL > ACL Access List – Add ACL Profile

Access-List: Specifies the access list name for the ACL profile to be added.

Packet Type: Specifies the packet type to be **MAC**, **IPv4**, **IPv4 Extended** or **IPv6** then click **Apply** button.

To modify an existing rule, click **Edit Rules** button and ACL Access list table will be displayed. Please click on the Sequence No. hyperlink.

MAC Access Rule List

Access-List Name : acl2 Type : MAC

Seq. No.	Summary	Action	Delete
1	Destination MAC, Source MAC, VLAN, 802.1p, Ether Type	Permit	<input type="button" value="Delete"/>

Figure 4.137 - ACL > ACL Access List – Update ACL Profile

ACL > ACL Access Group

The **ACL Access Group** page allows user to configure the ACL access group settings.

The screenshot shows the 'ACL Access Group' configuration page. At the top, there are dropdown menus for 'Port' (containing 'MAC Access-List', 'IPv4 Access-List', and 'IPv6 Access-List') and 'acl2'. An 'Apply' button is located to the right of the dropdowns. Below this is a table with 16 rows, each representing a port number from 1 to 16. The table has three columns: 'Port No.' (Port Number), 'MAC' (empty), 'IPv4' (empty), and 'IPv6' (empty). The table is currently empty, indicating no ports have been assigned to the access list.

Port No.	MAC	IPv4	IPv6
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			

Figure 4.138 - ACL > ACL Access Group

Port: Specifies the ports to be added in the access list group.

MAC Access-List: Add the specified ports in the MAC access list group.

IPv4 Access-List: Add the specified ports in the IPv4 access list group.

IPv6 Access-List: Add the specified ports in the IPv6 access list group.

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

ACL > ACL Hardware Resource Status

The **ACL Hardware Resource Status** page displays the information of ACL Hardware Resource status.

The screenshot shows the 'ACL Hardware Resource Status' page. At the top, there is a header bar with 'ACL Hardware Resource Status' and a 'Safeguard' button. Below this is a table with 10 rows, each representing a hardware profile ID from 1 to 10. The table has three columns: 'Hardware Profile ID', 'Access-List Name', and 'Consumed/Total Entries'. The data in the table is as follows:

Hardware Profile ID	Access-List Name	Consumed/Total Entries
1	STATIC_HOST_ROUTE	1 / 128
2	STATIC_NET_ROUTE	1 / 128
3		0 / 128
4		0 / 128
5		0 / 128
6		0 / 128
7		0 / 128
8		0 / 128
9		0 / 128
10		0 / 128

Figure 4.139 - ACL > ACL Hardware Resource Status

PoE > PoE Global Settings (only for DGS-1210-10P/10MP/28P/28MP/52MP)

This page will display the PoE status including System Budget Power, Support Total Power, Remainder Power, and The ratio of system power supply.

PoE Power Threshold (7.1-370.0) Watts
Power Shut Off Sequence

System Power Status
Total PoE Power Budget 370
Power Used 0
Power Left 370
The percentage of system power supplied 0%

💡 1. 7 watts guard band is reserved for system to prevent a PD from being powered off when encountering a sudden increment of PD power supply. When Used Power reaches guard band, a new PD will trigger the action defined in Power Shut Off Sequence.
2. If a sudden increment of a PD power causes PSE power overload, switch will firstly stop power supply to the port with a low priority PD. As a result, high priority PD can work without being affected.

Figure 4.138 – PoE > PoE Global Setting

System Power Threshold: Manually configure the system power budget.

Power Shut Off Sequence: 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 the **Apply** button to implement changes made.

System Power Status: Displays the system power status of device.

Total PoE Power Budget: Displays the total PoE power budget of this switch.

Power Used: Displays the current used power of the switch.

Power Left: Displays the spare power of the switch.

The percentage of system power supplied: Displays the percentage of system power supplied of the switch.

PoE > PoE Port Settings (only for DGS-1210-10P/10MP/28P/28MP/52MP)

The DGS-1210 series supports Power over Ethernet (PoE) as defined by the IEEE specification. The PoE port specification is listed in the table below:

Model Name	PoE Capable Ports	Power Budget
DGS-1210-10P	Port 1 ~ Port 8: Max. PoE Output 30 Watts	65 Watts
DGS-1210-10MP	Port 1 ~ Port 8: Max. PoE Output 30 Watts	130 Watts
DGS-1210-28P	Port 1 ~ Port 24: Max. PoE Output 30 Watts	193 Watts
DGS-1210-28MP	Port 1 ~ Port 24: Max. PoE Output 30 Watts	370 Watts
DGS-1210-52MP	Port 1 ~ Port 48: Max. PoE Output 30 Watts	370 Watts

The DGS-1210 series work 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	Optional	30W

The PoE port table will display the PoE status including, Port Enable, Power Limit, Power (W), Voltage (V), Current (mA), Classification, Port Status. You can select **From Port / To Port** to control the PoE functions of a port. The DGS-1210 series 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.

PoE Port Settings

From Port	To Port	State	Time Range	Priority	Delay Power Detect	Power Limit
1	48	Enabled	N/A	Normal	Disabled	Auto
<input type="button" value="Legacy PD"/> <input type="button" value="Enable"/> <input type="button" value="Refresh"/> <input type="button" value="Apply"/>						

1. The port 1 to port 48 can be set a power limit between 1W and 30W. Max power used by PSE: Class 1: 4W, Class 2: 7W, Class 3: 15.4W, Class 4: 30W.

Port	State	Time Range	Priority	Delay ...	Legacy...	Power ...	Power (W)	Voltage (V)	Current (mA)	Classification	Status
1	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
2	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
3	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
4	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
5	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
6	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
7	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
8	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
9	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
10	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
11	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
12	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
13	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
14	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
15	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
16	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
17	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
18	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
19	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
20	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
21	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
22	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
23	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
24	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
25	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
26	Enabled	N/A	Normal	Disabled	Disabled	Auto	0.0	0.0	0.0	N/A	POWER OFF
27	POWER OFF

Figure 4.139 – PoE > PoE Port Setting

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**.

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.

Power Limit: This function allows you to manually set the port power current limitation to be given to the PD. To protect the DGS-1210 PoE series and the connected devices, the power limit function will disable the PoE function of the port when the power is overloaded. Select from “Class 1”, “Class 2”, “Class 3”, “Class 4”

and "Auto" for the power limit. "Auto" will negotiate and follow the classification from the PD power current based on the 802.3at standard.

User Define: Check the box and input the power budget (from 1 to 30W) to manually assign an upper limit of port power budget on designated port(s).

Legacy PD: Specifies to enable or disable detecting legacy PDs signal.

Click **Apply** to make the configurations take effects 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: 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, you may enable this feature to extend the time interval to 500ms. If the PD is still not powering on, please contact the vendor of your device for support.

SNMP > SNMP > SNMP Global Settings

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

Safeguard
SNMP Global Settings

SNMP Global State	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Trap Settings <input type="checkbox"/> SNMP Authentication Traps <input type="checkbox"/> Device Bootup <input type="checkbox"/> Port Link Up / Link Down <input type="checkbox"/> RSTP Port State Change <input type="checkbox"/> Firmware Upgrade State <input type="checkbox"/> PoE Power On / Off <input type="checkbox"/> PoE Power Error <input type="checkbox"/> PoE over max power budget <input type="checkbox"/> Loopback Detection occurring / recovery	
<input style="border: 1px solid #ccc; padding: 2px 10px;" type="button" value="Apply"/>	

Figure 4.140 – SNMP > SNMP > SNMP Global Settings

Trap Settings: Specifies whether the device can send SNMP notifications.

SNMP Authentication Traps: Specifies the device to send authentication failure notifications.

Device Bootup: System boot-up information.

Illegal Login: Events of incorrect password logins, recording the IP of the originating PC.

Port Link Up / Link Down: Copper port connection information.

RSTP Port State Change: Events of a RSTP port state changes.

Firmware Upgrade State: Information of firmware upgrade - success or failure.

PoE power On / Off: Status of power per port.

PoE Power Error: The four trap events are: power over loading, short circuit, thermal shutdown and power deny.

PoE over max power budget: When the system supplies power to PDs and hits the max PoE power budget, the system will send out this trap message.

Loopback Detection occurring / recovery: Specifies the device to send SNMP Trap when Loopback Detection occurring and recovery.

SNMP > SNMP > SNMP User

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.

The screenshot shows the 'SNMP User Table' configuration page. At the top, there is a form with fields for 'User Name', 'Group Name', 'SNMP Version' (set to v1), 'Encrypt' (set to Disabled), 'Auth-Protocol' (set to MD5), and 'Privacy Protocol' (set to DES). To the right of the form are two password input fields labeled 'Password'. Below the form is a note: '* indicates mandatory data.' At the bottom right of the form is an 'Add' button. Below the form is a table with columns: User Name, Group Name, SNMP Version, Auth Protocol, Privacy Protocol, and Delete. The table contains four rows of data, each with a 'Delete' link in the last column.

User Name	Group Name	SNMP Version	Auth Protocol	Privacy Protocol	Delete
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 4.141 – SNMP > SNMP > SNMP User Table

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

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

SNMP Version: Specifies 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: Specifies 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: Specifies either **no authorization** or **DES 56-bit encryption** and then enter a password for SNMPv3 encryption in the right column.

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

SNMP > SNMP > 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: Specifies the SNMP user group of up to 32 characters.

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

Write View Name: Specifies 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 you select SNMPv3 security level.

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

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

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

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

Group Name	Read View	Write View	Notify View	Security Model	Security Level	Delete
ReadOnly	ReadWrite	---	ReadWrite	v1	NoAuthNoPriv	Delete
ReadOnly	ReadWrite	---	ReadWrite	v2c	NoAuthNoPriv	Delete
ReadWrite	ReadWrite	ReadWrite	ReadWrite	v1	NoAuthNoPriv	Delete
ReadWrite	ReadWrite	ReadWrite	ReadWrite	v2c	NoAuthNoPriv	Delete

Figure 4.142 – SNMP > SNMP > SNMP Group Table

SNMP > SNMP > SNMP View

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

View Name	Subtree OID	OID Mask	View Type	Delete
ReadWrite	1	1	Included	Delete

Figure 4.143 – SNMP > SNMP > SNMP View

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

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

SNMP > SNMP > SNMP Community

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): Specifies the read/write or read-only level permission for the MIB objects accessible to the SNMP community.

Community Name	User Name	Delete
public	ReadOnly	<input type="button" value="Delete"/>
private	ReadWrite	<input type="button" value="Delete"/>

Figure 4.144 –SNMP > SNMP > SNMP Community

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

SNMP > SNMP > SNMP Host

This SNMP Host page is to configure the SNMP trap recipients.

Host IP Address	SNMP Version	Community Name/SNMPv3 User Name	Delete
	V1		<input type="button" value="Delete"/>

Figure 4.145 – SNMP > SNMP > SNMP Host

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

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

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

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

SNMP > SNMP > SNMP Engine ID

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

Input the Engine ID then click **Apply** to apply the changes and click **Default** resets to default value.

Engine ID: 4447532d313231302d35324d504a6f6e0101

Engine ID length is 10-64, the accepted character is from 0 to F.

Figure 4.146 – SNMP > SNMP > SNMP Engine ID

SNMP > RMON > RMON Global 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 Global Settings

RMON Enabled Disabled

Apply

Figure 4.147 - SNMP > RMON > RMON Global Settings

SNMP > RMON > RMON Statistics

The RMON Statistics Configuration page displays the information of RMON Ethernet Statistics and allows the user to configure the settings.

RMON Ethernet Statistics Settings

Index (1~65535) *
Port *
Owner

* indicates mandatory data.

Refresh Add

Index	Port	Drop Events	Octets	Packets	Broadcast Packets	Multicast Packets	Owner	Delete
-------	------	-------------	--------	---------	-------------------	-------------------	-------	--------

Figure 4.148 - SNMP > 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 **Add** to make the configurations take effects and click **Refresh** to redisplay the table information.

SNMP > RMON > RMON History

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 Settings

Index (1~65535) *
Port *
Buckets Requested (1~50) *
Interval (1~3600) sec *
Owner

* indicates mandatory data.

Add

Index	Port	Buckets Requested	Buckets Granted	Interval	Owner	Delete
-------	------	-------------------	-----------------	----------	-------	--------

Figure 4.149 - SNMP > RMON > RMON History Control Settings

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

SNMP > RMON > RMON Alarm

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

The screenshot shows the 'RMON Alarm Settings' page. It includes fields for Index (1~65535), Variable, Rising Threshold (0~2^31-1), Falling Threshold (0~2^31-1), and Event Index (1~65535). A note indicates that a red asterisk (*) denotes mandatory data. An 'Add' button is at the bottom right, and a navigation bar below it includes tabs for Index, Interval, Variable, Sample Type, Rising Threshold, Falling Threshold, Rising Event Index, Falling Event Index, Owner, and Delete.

Figure 4.150 - SNMP > RMON > RMON Alarm Settings

The configuration contains the following fields:

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

Variable: Specifies 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 **Add** to make the configurations take effects.

SNMP > RMON > RMON Event

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

The screenshot shows the 'RMON Event Settings' page. It includes fields for Index (1~65535), Description, Type (with a dropdown menu showing 'None'), Community, and Owner. A note indicates that a red asterisk (*) denotes mandatory data. An 'Add' button is at the bottom right, and a navigation bar below it includes tabs for Index, Description, Type, Community, Owner, Last Time Sent, and Delete.

Figure 4.151 - SNMP > RMON > RMON Event Settings

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 **Add** to add a new RMON event.

Monitoring > Port Statistics

The Port Statistics screen displays the status of each port packet count.

The screenshot shows a table titled "Port Statistics" with columns for Port, TxOK, RxOK, TxError, and RxError. The table lists 13 ports (01 to 13) and their corresponding statistics. Port 09 has the highest TxOK value at 4009, and Port 01 has the highest RxOK value at 3896. All other ports show 0 for both TxOK and RxOK.

Port	TxOK	RxOK	TxError	RxError
01	0	0	0	0
02	0	0	0	0
03	0	0	0	0
04	0	0	0	0
05	0	0	0	0
06	0	0	0	0
07	0	0	0	0
08	0	0	0	0
09	4009	3896	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0

Figure 4.152 – Monitoring > Port Statistics

Refresh: Renews the details collected and displayed.

Clear: 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.

The screenshot shows a detailed view of Port 9 statistics. It includes two tables: "TX" and "RX". The TX table shows OutOctets (3110753), OutUcastPkts (4085), OutNUcastPkts (3), OutErrors (0), LateCollisions (0), ExcessiveCollisions (0), and InternalMacTransmitErrors (0). The RX table shows InOctets (485802), InUcastPkts (3118), InNUcastPkts (842), InDiscards (0), InErrors (0), FCSErrors (0), FrameTooLongs (0), and InternalMacReceiveErrors (0).

TX		RX	
OutOctets	3110753	InOctets	485802
OutUcastPkts	4085	InUcastPkts	3118
OutNUcastPkts	3	InNUcastPkts	842
OutErrors	0	InDiscards	0
LateCollisions	0	InErrors	0
ExcessiveCollisions	0	FCSErrors	0
InternalMacTransmitErrors	0	FrameTooLongs	0

Figure 4.153 – Monitoring > Port Statistics

Back: Go back to the Statistics main page.

Refresh: To renew the details collected and displayed.

Clear: To reset the details displayed.

Monitoring > Cable Diagnostics

The Cable Diagnostics is designed primarily for administrators and customer service representatives to examine 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.

The cable diagnostics feature is designed primarily for administrators or customer service representatives to verify and test copper cables; it can rapidly determine the quality of the cables and the types of error.

1. If cable length is displayed as "N/A" (not available) it means the cable length cannot be detected. The port is unable to determine the cable length either because the link speed is 10/100 Mbps or the cable used is broken or of bad quality.
 2. The deviation of "Cable Length(meters)" and "Cable Fault Distance" are +/- 10 meters, therefore no cable may be displayed under Test Result, when the cable used is less than 10m in length.
 3. Cable diagnostics can also detect the location of the cable fault. This will be shown as "Cable Fault Distance", the distance the switch.

Figure 4.154 – Monitoring > Cable Diagnostic

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".

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, 100~140 meters and >140 meters.



NOTE: Cable length detection is effective on Gigabit ports only.



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



NOTE: The deviation of "Cable Length(meters)" and "Cable Fault Distance" are +/- 10 meters, therefore no cable may be displayed under Test Result, when the cable used is less than 10m in length.

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.



The screenshot shows a table with four columns: ID, Time, Log Description, and Severity. The table has 3 rows of data. A note at the top left says "Maximum 500 entries." and there are "Refresh" and "Clear" buttons at the top right. The "Safeguard" logo is in the top right corner.

ID	Time	Log Description	Severity
1	Jan 1 00:17:10	Successful login through Web (IP: 10.90.90.96)	info
2	Jan 1 00:00:03	System started up	critical
3	Jan 1 00:00:29	Side Fan is in low speed.	info

Figure 4.155 – Monitoring > System Log

ID: Displays an incremented counter of the System Log entry. The Maximum entries are 500.

Time: Displays the time in days, hours, and minutes the log was entered.

Log Description: Displays a description event recorded.

Severity: Displays a severity level of the event recorded.

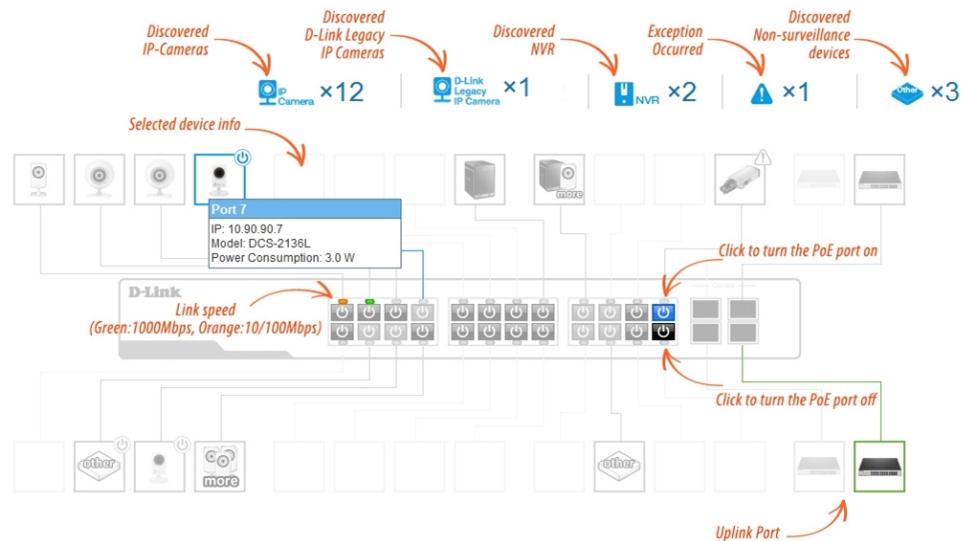
Click **Refresh** to renew the page, and click **Clear** to clean out all log entries.



Note: The system logs will be reset and won't be saved after the switch reboots.

5 Surveillance Mode Configuration

When you complete the Surveillance Mode Smart Wizard, you will be presented with the following screen:



Device Status

Icon	Description	Icon	Description	Icon	Description
	The device is operational but is not powered by PoE.		The device is operational and is powered by PoE.		The device may malfunction. Some problem detected on this port or device.

IPC/NVR Status

Icon	Description	Icon	Description	Icon	Description
	One D-Link ONVIF IP-Camera discovered on this port. For D-Link IP-Camera, a specific icon will be displayed.		One ONVIF IP-Camera discovered on this port.		Multiple ONVIF IP-Cameras discovered on this port.
	One NVR discovered on this port. Any device connect to IP-Camera via HTTP, HTTPS and RTSP will be recognized as an NVR.		Multiple NVRs discovered on this port.		One ONVIF IP-Camera and one NVR discovered on this port.
	Multiple ONVIF IP-Cameras and one NVR discovered on this port.		One ONVIF IP-Camera and multiple NVRs discovered on this port.		Multiple ONVIF IP-Cameras and multiple NVRs discovered on this port.
	The port is up and no ONVIF IP-Camera, NVR, or other surveillance device has been discovered on this port.		This port is set as uplink port and the port status is up. Uplink port joins all VLANs and surveillance discovery process is disabled on this port.		This port is set as uplink port and the port status is down.

OK

Figure 5.1 – Surveillance Mode Congratulations window

Click **OK** button to continue to the Web UI.

Web User Interface

Before enter the Web User interface, the pop-up dialog will be shown as below. Click **OK** to enter the Web user interface.

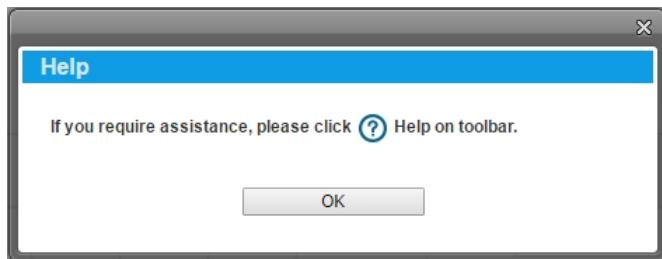


Figure 5.2 – Surveillance Mode > Help

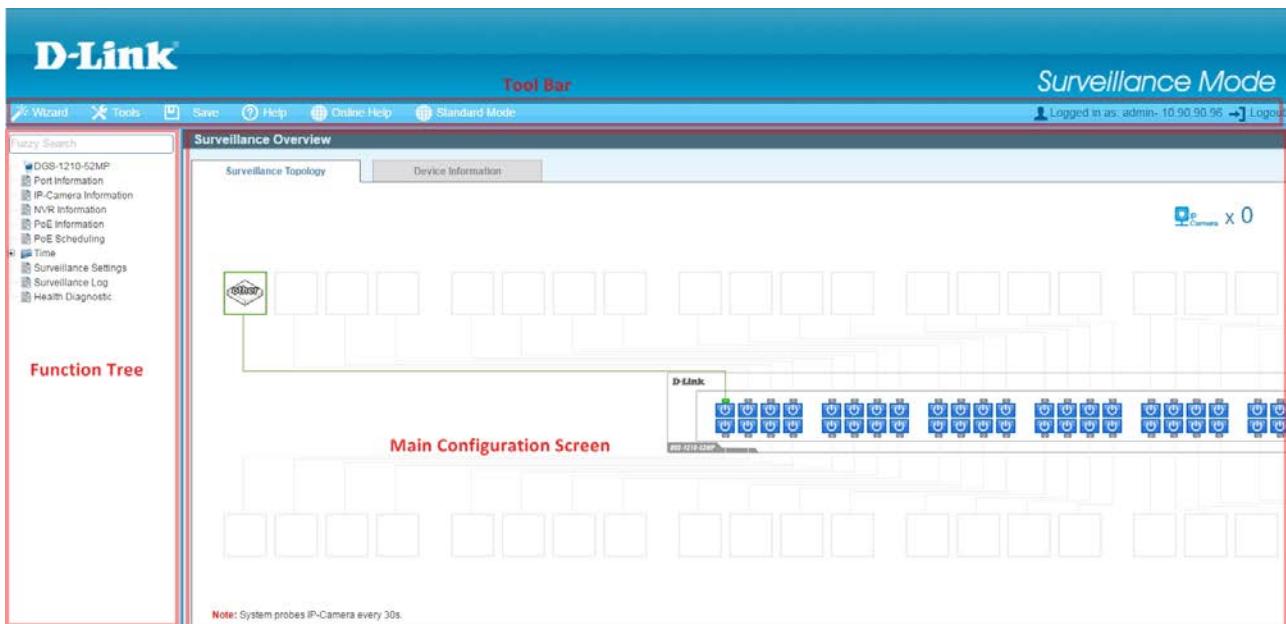


Figure 5.3 – Surveillance Mode > Main Web UI Window

The above image is the Web UI Interface 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 for Surveillance mode.
Function Tree	By choosing different functions in the Function Tree navigation menu, Click on the links and navigate the folder structure to display information on the Main Configuration Screen for Surveillance mode.
Main Configuration Screen	To display the information and configuration options for Surveillance mode on the switch.

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.

Surveillance Overview

This loads automatically when user log-in to the switch and contains two tabs; **Surveillance Topology** and **Device Information**. To return to the Surveillance Overview page after viewing other pages, click the model number of the switch at the top of the navigation menu.

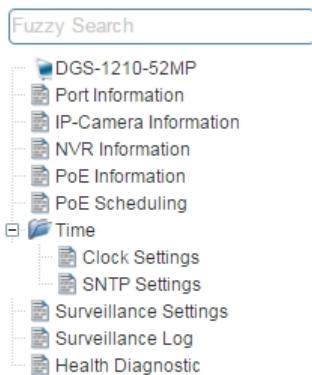


Figure 5.4 – Surveillance Mode > Overview

Surveillance Topology

The Surveillance Topology page contains a diagram of the surveillance topology, including an overview of the devices connected to the switch.

To view the following window, click on the model number of the switch at the top of the navigation menu:

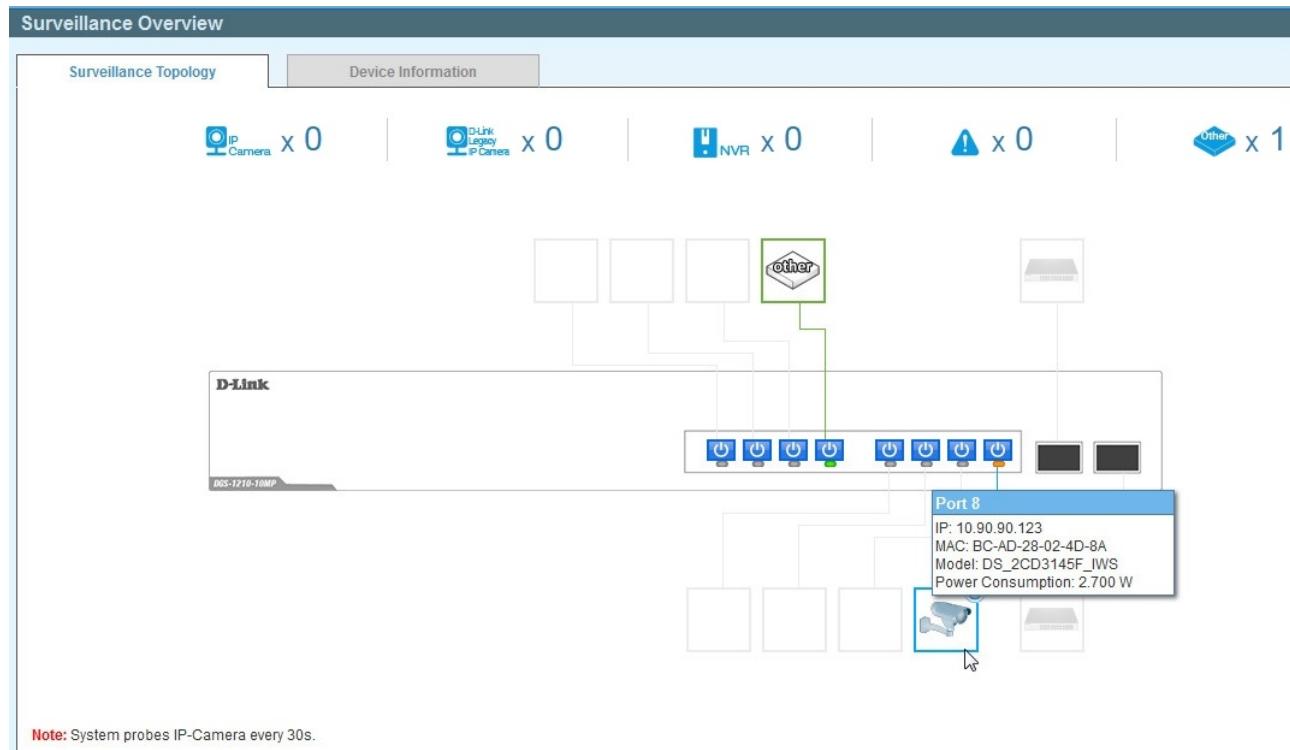


Figure 5.5 – Surveillance Mode > Surveillance Topology Tab

There is a device count at the top of the page, listing the number of connected IP-Cameras, Network Video Recorders (NVRs) and unrecognized devices. It also lists the number of warnings on the system.

The Surveillance Topology provides users more information about what is connected to each port. Hover over each device icon to get more information about the recognized devices, such as: the number of devices, device type, IP address, power consumption, link speed and errors. Click on the ‘more’ link to get more information about the devices connected to a port. Each port can also be powered-on and off using PoE by clicking the power symbol on each port.



CAUTION: Before connecting the Powered Device (PD) and enabling 60/70 Watts PoE, make sure it supports IEEE 802.3bt, as otherwise it will become damaged.



NOTE: The device icons can be found by clicking the **Help** menu at the top of the page.



NOTE: The system probes for new IP-Cameras every 30 seconds.

Device Information

This tab on the Surveillance Overview page and is divided into 3 parts; a device information section, PoE utilization section and bandwidth usage section.

To view the following window, click on the model number of the switch at the top of the navigation menu and the click the **Device Information** tab:

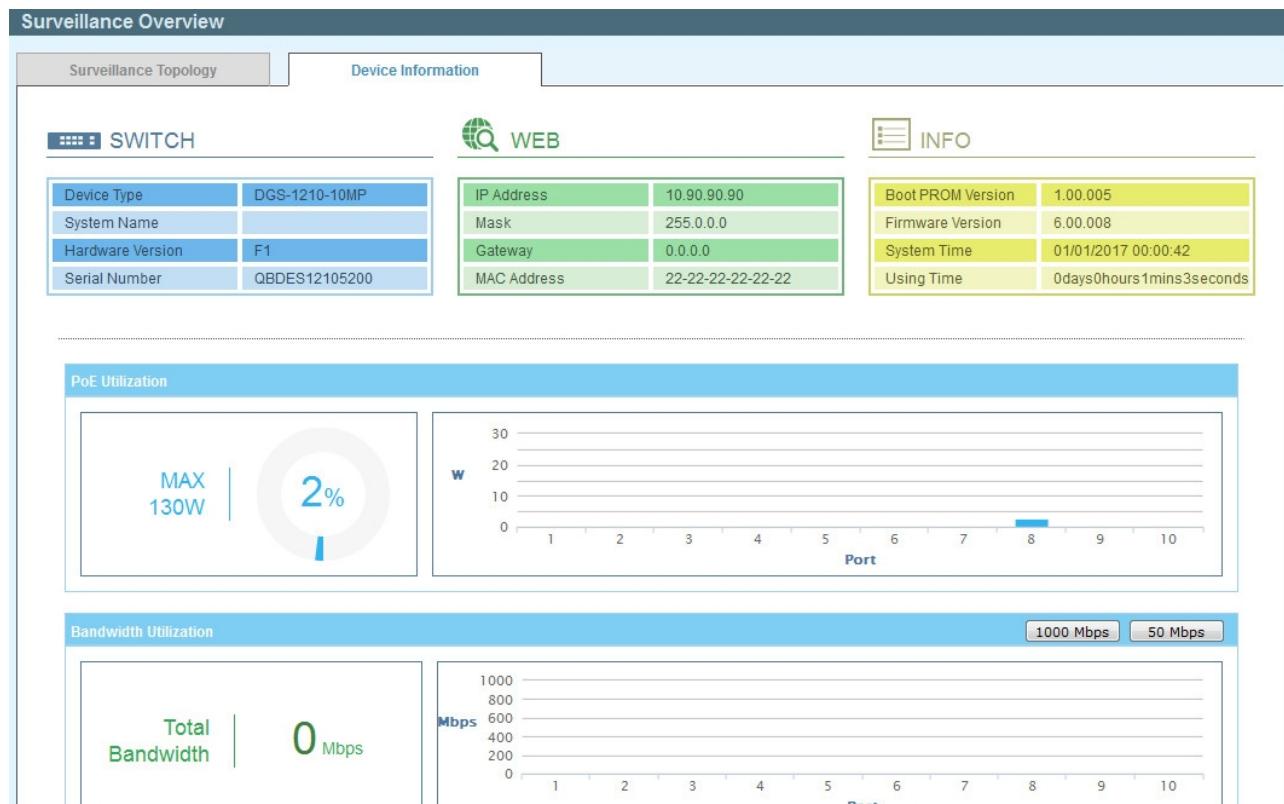


Figure 5.6 – Surveillance Mode > Device Information Tab

The device information section is sub-divided into 3 sections; switch information, web information and system information. It contains information such as the device type, system name, serial number, IP address settings, MAC address settings, firmware versions and system uptime.

The PoE utilization area contains PoE utilization statistics for the switch. On the left is the total PoE utilization, with the total power budget and overall utilization show. On the right is a per-port usage graph, showing the PoE utilization for each individual port.

The bandwidth usage section contains bandwidth utilization for the switch. On the left the total bandwidth shows the total inbound traffic on all ports. There is also a per-port bandwidth utilization graph on the right, showing the inbound traffic for each individual port. The scale of the graph can be changed by pressing the 1000 Mbps and 50 Mbps buttons above the graph.

Click the **1000 Mbps** button to change the maximum bandwidth displayed in the **Bandwidth Utilization** chart to 1 Gbps.

Click the **50 Mbps** button to change the maximum bandwidth displayed in the **Bandwidth Utilization** chart to 50 Mbps.

Port Information

The Port Information page displays the port status for each port. This information includes the throughput, PoE status, Loopback Detection Status, cable length, power consumption and how many IP cameras, NVRs, and other devices are connected to the ports.

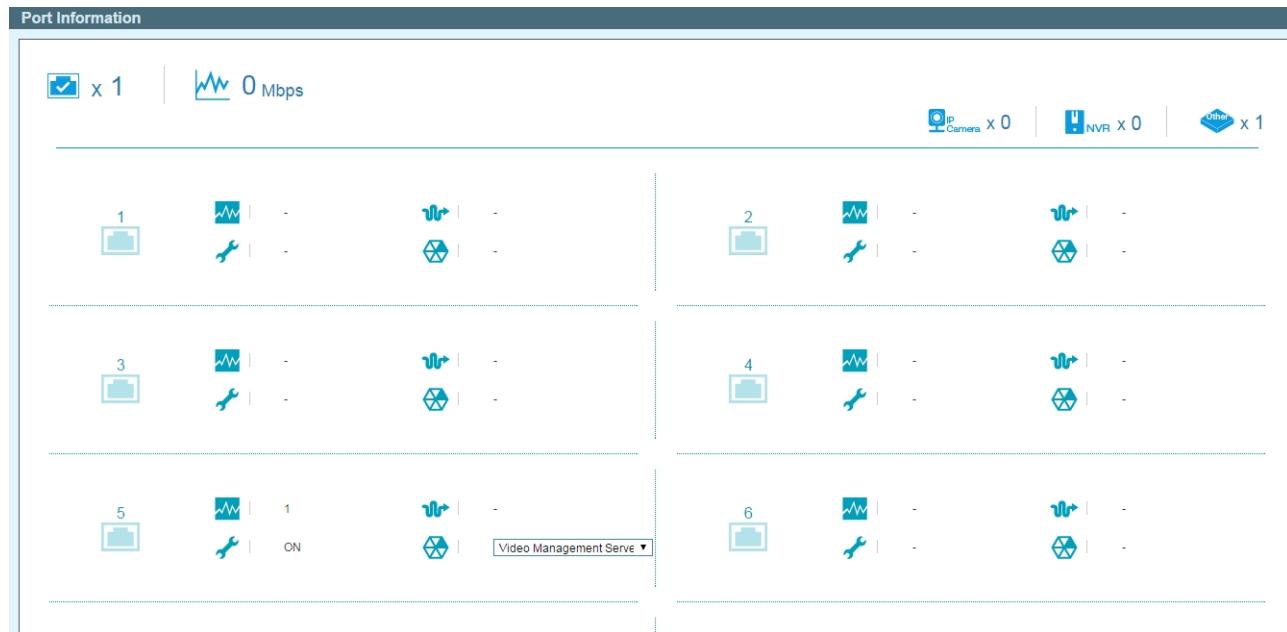


Figure 5.7 – Surveillance Mode > Port Information

IP-Camera Information

The IP-Camera Information page displays information on each camera connected to the switch. It features the port number, device type, throughput, IP address and other information such as port description, power consumption and location.

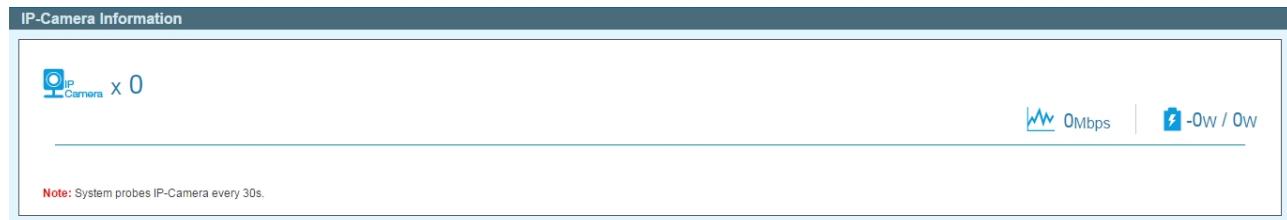


Figure 5.8 – Surveillance Mode > IP-Camera Information

NVR Information

The NVR Information page displays information on each NVR connected to the switch. It features the port number, throughput, IP address and information 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. Hover-over each field to get more information about each value.

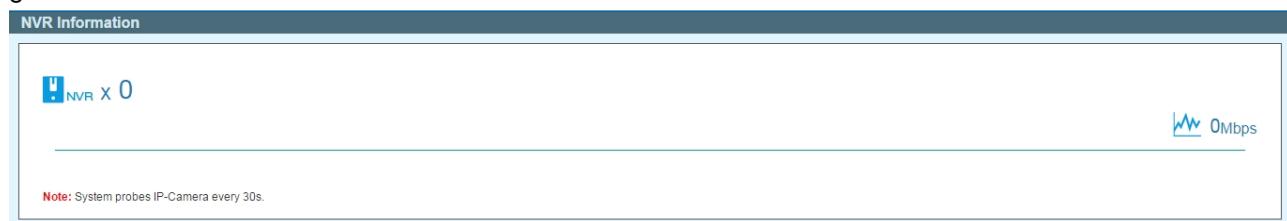


Figure 5.9 – Surveillance Mode > NVR Information

PoE Information

This page displays the Power-over-Ethernet(PoE) usage information of each port on the Switch. The port number, PoE status, health status, PoE budget and power consumption is listed for each port. It is possible to click on the health status to be re-directed to the Health Diagnostic page. Hover-over each field to get more information about each value.

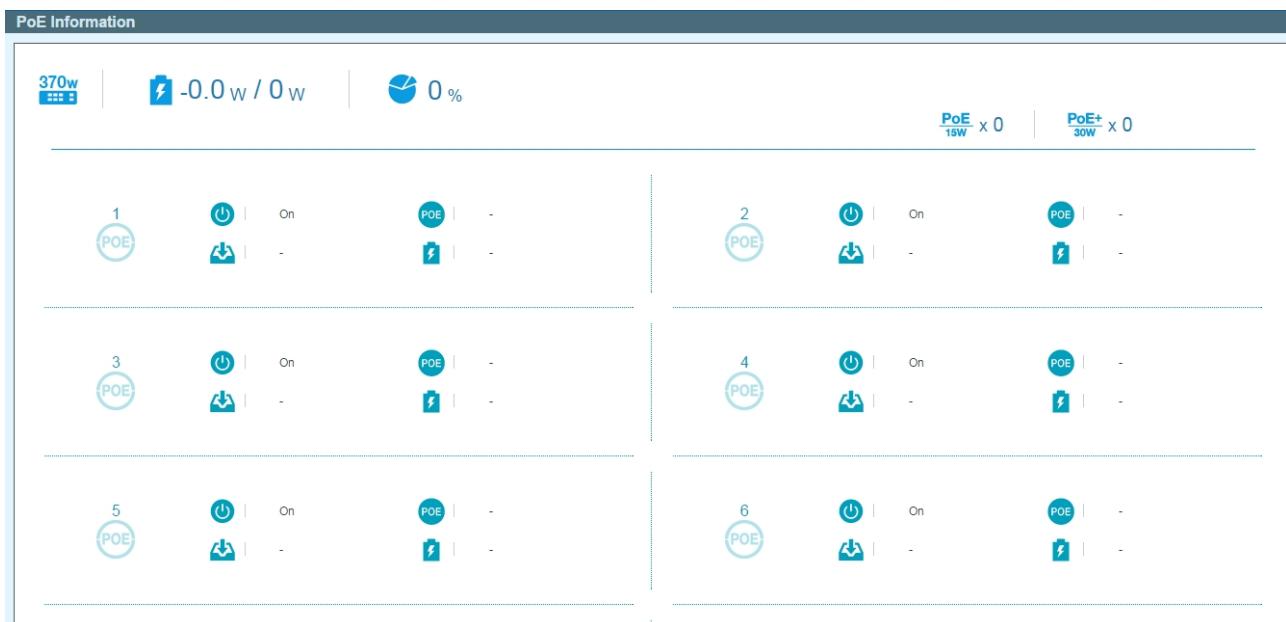


Figure 5.10 – Surveillance Mode > PoE Information

PoE Scheduling

This PoE Scheduling page allows user to specify the amount of time that power is delivered to a PoE port. This can be used to save power when devices are not in use, or as a security feature to prevent wireless access from being available outside of business hours, for example. It is possible to set a schedule name, a start time, and end time and which ports the PoE schedule applies to.

The figure shows the PoE Scheduling interface. At the top, a Time Profile section is displayed with fields for Profile Name, Start Time (00:00), End Time (00:00), Weekdays (Sun, Mon, Tue, Wed, Thu, Fri, Sat), Date (From Day: 2011-01-01, To Day: 2011-01-01), and an Add button. Below this is a table of Total Entries: 1, showing a single schedule entry:

Profile Name	Start Time	End Time	Weekdays	From Day	To Day	Delete
1	00:00	17:00	Sat			<input type="button" value="Delete"/>

Below the table is a PoE Configuration section with From Port (1), To Port (1), Time Profile (N/A), and an Apply button. A table below shows port assignments:

Port	Time Profile	Delete
1	1	<input type="button" value="Delete"/>
2		<input type="button" value="Delete"/>
3		<input type="button" value="Delete"/>

Figure 5.11 – Surveillance Mode > PoE Scheduling

The fields that can be configured in the **Time Profile** section are described below:

Parameter	Description
Profile Name	Specifies the name of the time range schedule.
Time(HH MM)	Select the start time end time with hour and minutes.
Weekdays	Specifies the work day for the scheduling.

Date	Tick the Date and select the From Day / To Day for the scheduling.
-------------	--

Click the **Add** button to create a new time profile for PoE scheduling.

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

The fields that can be configured in the **PoE Configuration** section are described below:

Parameter	Description
From Port / To Port	Select the port range to be used.
Time Profile	Select the time profile to be used.

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

Click the **Delete** button to remove the time range schedule from the specified port.

Time > Clock Settings

This Clock Settings page allows user to configure the time on the Switch.

Figure 5.12 – Surveillance Mode > Time > Clock Settings

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

Parameter	Description
Time (HH:MM:SS)	Set the system time with the format (HH:MM:SS).
Date (DD/MM/YYYY)	Set the date with the format (DD/MM/YYYY).

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

Time > SNTP Settings

The SNTP Settings page allows user to configure an external time source on the switch. Simple Network Time Protocol (SNTP) is a lightweight version of the NTP protocol and can be used to keep the system clock in-sync by using a network-based time source.

Figure 5.13 – Surveillance Mode > Time > SNTP Settings

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

Parameter	Description
-----------	-------------

SNTP State	Specifies to enable or disable the SNTP state.
SNTP Poll Interval (30-99999)	Specifies the poll interval. The range is between 30 and 99999. By default, the value is 30 seconds.

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

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

Parameter	Description
SNTP First Server	Select to enter the IPv4 or IPv6 address for SNTP first server.
SNTP Second Server	Select to enter the IPv4 or IPv6 address for SNTP second server.

Click the **Apply** button to add the SNTP server to the configuration.

Surveillance Settings

The Surveillance Settings page allows user to configure the settings for the Surveillance VLAN. This is a VLAN dedicated for IP-Camera (IPC) and Network Video Recorders (NVR), and also can be used to manage surveillance devices on the network.

The screenshot shows the 'Surveillance Settings' configuration page. It includes the following sections:

- Surveillance VLAN Settings:** VLAN ID (2-4094) set to 4094, with an **Apply** button.
- IP Settings:** Get IP From: Static, IP Address: 10.90.90.90, Mask: 8 (255.0.0.0), Gateway: 0.0.0.0, with an **Apply** button.
- SNMP Host Settings:** Community Name/SNMPv3 User Name, Host IPv4 Address, with an **Apply** button. Below is a table with columns: Host IP Address, SNMP Version, Community Name/SNMPv3 User Name, and Delete.
- Log Server:** Host IPv4 Address set to 0.0.0.0, with an **Apply** button.
- Password Settings:** Old Password, New Password, Confirm Password, with an **Apply** button.
- Uplink Port Settings:** From Port (1), To Port (1), with an **Add** button. Below is a table with columns: Port (49, 50, 51, 52), and Delete buttons.

Figure 5.14 – Surveillance Mode > Surveillance Settings

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

Parameter	Description
VLAN ID (2-4094)	Specifies a VLAN ID for the surveillance VLAN in the range between 2 and 4094.

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

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

Parameter	Description
Get IP From	Specifies how the management IP for this VLAN is assigned to the switch. Options are: Static , DHCP or BOOTP . If Static is chosen, the following fields become available.
IP Address	Specifies the IP address for the surveillance VLAN management IP.
Mask	Specifies the netmask for the surveillance VLAN management IP.
Gateway	Specifies the gateway for the surveillance VLAN.

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

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

Parameter	Description
Community Name/SNMPv3 User Name	Specifies the community name or SNMPv3 user name to be configured.
Host Ipv4 Address	Specifies the IPv4 address of the SNP Network Management Server (NMS) which will receive SNMP Traps from this device.

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

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

Parameter	Description
Host IPv4 Address	Specifies the IPv4 address of the Syslog NMS which will receive Syslog messages from this device.
Host Ipv6 Address	Specifies the IPv6 address of the Syslog NMS which will receive Syslog messages from this device.

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

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

Parameter	Description
Old Password	Enter the old password that is used to restrict access to the device via the Web UI. Password length is a maximum of 20 characters.
New Password	Configure a new password that will be used to restrict access to the device via the Web UI. Password length is a maximum of 20 characters.
Confirm Password	Confirm the password that will be used to restrict access to the device via the Web UI. Password length is a maximum of 20 characters.

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

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

Parameter	Description
From Port	Specifies the start port in the range for Uplink Ports. These are used for connecting the surveillance VLAN with other switches.
To Port	Specifies the end port in the range for Uplink Ports. These are used for connecting the surveillance VLAN with other switches.

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

Click the Delete button to delete any entries in the list of uplink ports.

Surveillance Log

The Surveillance Log page consists of a list of Syslog messages that have been generated by the switch. Depending on whether a Syslog server has been defined in the Surveillance Settings section, these may be local to the switch or copied to an external logging server. The messages are ordered in date order with the latest message at the top of the list. Please consult an external source for more information on syslog logging levels.

Surveillance Log			
Index	Time	Severity	Log Description

Figure 5.15 – Surveillance Mode > Surveillance Log

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

Click the **Backup** button to save the information displayed in the table to a remote location.

Health Diagnostic

The Health Diagnostic page is linked-to by the Port Information and PoE Information pages and displays an overview of the port status. It contains the port number, Loopback Detection status, Cable Link status, PoE Status, Tx/Rx Error Counter, number of Discovered Surveillance Devices on the port (which links to the Group Details page) and the detected cable length. The page automatically refreshes every 30 seconds.

Health Diagnostic						
Port	Loopback Detection Status	Cable Link	PoE Status	Tx/Rx CRC Counter	Discovered Surveillance Devices	Detect Distance
1	-	-	-	-	-	<input type="button" value="Detect"/>
2	-	-	-	-	-	<input type="button" value="Detect"/>
3	-	-	-	-	-	<input type="button" value="Detect"/>
4	-	-	-	-	-	<input type="button" value="Detect"/>
5	-	-	-	-	-	<input type="button" value="Detect"/>
6	Normal	Pass	-	0/0	0	<input type="button" value="Detect"/>
7	-	-	-	-	-	<input type="button" value="Detect"/>
8	-	-	-	-	-	<input type="button" value="Detect"/>
9	-	-	-	-	-	<input type="button" value="Detect"/>
10	-	-	-	-	-	<input type="button" value="Detect"/>
11	-	-	-	-	-	<input type="button" value="Detect"/>
12	-	-	-	-	-	<input type="button" value="Detect"/>
13	-	-	-	-	-	<input type="button" value="Detect"/>
14	-	-	-	-	-	<input type="button" value="Detect"/>
15	-	-	-	-	-	<input type="button" value="Detect"/>
16	-	-	-	-	-	<input type="button" value="Detect"/>

Figure 5.16 – Surveillance Mode > Health Diagnostic

Click the **Detect All** button to initiate a cable distance test on all the ports of the Switch.

Click the **Detect** button to initiate a cable distance test on the specified port on the Switch.

Click the hyperlink in the **Discovered Surveillance Devices** column to view more information of the devices connected to the port.

After clicking the hyperlink in the **Discovered Surveillance Devices** column, the following window will appear.

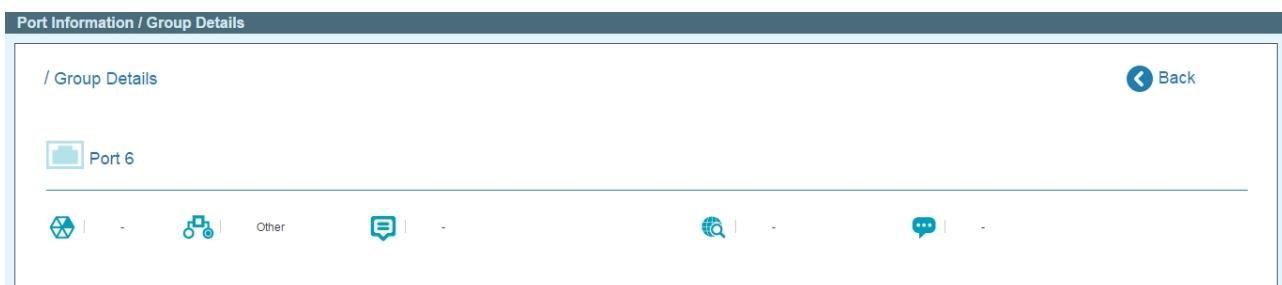


Figure 5.17 – Surveillance Mode > Health Diagnostic – Port Information / Group Details

Click **Back** to go to the previous page.

Tool Bar > Wizard

By clicking the Wizard button, you can return to the Smart Wizard if you wish to make any changes there. For the Smart Wizard configuration, you can refer to the Chapter 4 [Smart Wizard Configuration](#).

Tool Bar > Tools Menu

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



Figure 5.18 – Surveillance Mode > Tools Menu

Reset System

Provide a safe reset option of Surveillance VLAN for the Switch. All configuration settings in non-volatile RAM will be reset to factory default except for the IP address.



Figure 5.19 – Surveillance Mode > Tools Menu > Reset

Select one of the following options:

- **Warning!! The Switch will be reset to its factory defaults, and then will reboot.** – To reset the Switch's configuration to its factory default settings.
- **Warning!! The Switch will be reset to its factory defaults except IP address, and then will reboot.** – To reset the Switch's configuration to its factory default settings. This option will exclude the IP address from being changed.

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

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.

Reboot System

Do you want to save the settings ? YES NO
If you do not save the settings, all changes made in this session will be lost.

Reboot

Figure 5.20 – Surveillance Mode > Tools Menu > Reboot Device

When rebooting the Switch, any configuration changes that was made during this session, will be lost unless the **Yes** option is selected when asked to save the settings.

Click the **Reboot** button to alternatively save the settings and reboot the Switch.

Configuration Backup & 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 Backup and Restore

HTTP

Backup/Restore Config ID number : config_id 1 ▾
Backup
Choose File No file chosen
Restore

TFTP

Backup/Restore Config ID number : config_id 1 ▾
TFTP Server IP Address
IPv4
IPv6
TFTP File Name
Backup
Restore

Full-screen Strip

Figure 5.21 – Surveillance Mode > Tools Menu > Configuration Backup & Restore

The fields that can be configured with **HTTP** section are described below:

Parameter	Description
Backup/Restore Config ID number:	Select config_id 1 or config_id 2 to backup or restore the configuration file.

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.

The fields that can be configured with **TFTP** section are described below:

Parameter	Description
Backup/Restore Config ID number:	Select config_id 1 or config_id 2 to backup or restore the configuration file.
TFTP Server IP Address	Specifies the IPv4 or IPv6 Address to be used.
TFTP File Name	Choose the 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.

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

<input checked="" type="radio"/> HTTP Backup firmware to file : <input type="button" value="Image_id 1 ▾"/> <input type="button" value="Backup"/> Upgrade firmware from file : <input type="button" value="Choose File"/> No file chosen <input type="button" value="Upgrade"/>	<input type="radio"/> TFTP TFTP Server IP Address : <input type="text"/> <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 TFTP File Name : <input type="text"/> Backup firmware to file : <input type="button" value="Image_id 1 ▾"/> <input type="button" value="Backup"/> Upgrade firmware from file : <input type="button" value="Upgrade"/>
---	---

Figure 5.22 – Surveillance Mode > Tools Menu > Firmware Backup & Upgrade

The fields that can be configured with **HTTP** section are described below:

Parameter	Description
Backup firmware to file:	Select Image_id 1 or Image_id 2 to backup or restore the firmware file.

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.

The fields that can be configured with **TFTP** section are described below:

Parameter	Description
Backup/Restore Image ID number:	Select Image_id 1 or Image_id 2 to backup or restore the firmware file.
TFTP Server IP Address	Specifies the IPv4 or IPv6 Address to be used.
TFTP File Name	Choose the file name for the firmware file you want to save to / restore from.

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

The Firmware Information page displays the information of firmware. The user can specify configuration ID and image file to boot up when power on the Switch next time.

Firmware Information

Firmware Information

ID	Version	Size (B)	Update Time	From	User
*c1	6.10.007	10608880	01/01/2017 00:06:15	10.90.90.66	admin (Web)
2	6.00.006	12288000	N/A	N/A	Anonymous (factory)

Please select the boot up image and config of device.

config_id 1 ▼
Image_id 1 ▼
Apply

*: Boot up firmware
 (SSH) : Firmware update through SSH
 (Web) : Firmware update through Web
 (SNMP) : Firmware update through SNMP
 (Telnet) : Firmware update through Telnet

Figure 5.23 – Surveillance Mode > Tools Menu > Firmware Information

Flash Information

The Flash Information displays the flash detail information of the Switch.

Flash Information

Flash Information

Flash ID	MX25L25635F			
Flash Size	32MB			
Boot	1000000	1000000	0	100
Image1	9744416	14155776	4411360	68
Image2	9744416	14155776	4411360	68
Jffs2	276528	3932160	3653632	7

Figure 5.24 – Surveillance Mode > Tools Menu > Flash Information

Tool Bar > Save

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. Or 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 Configuration

Please press the button to save the config of device. config_id 1 ▼ **Save Config**

Save Log : **Backup Log**

Figure 5.25 – Surveillance Mode > Save

Specifies the configuration ID 1 or 2 to be saved and click the **Save Config** button to implement changes made.

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

Tool Bar > Help

By clicking the Wizard button to access the built-in Surveillance Help window.

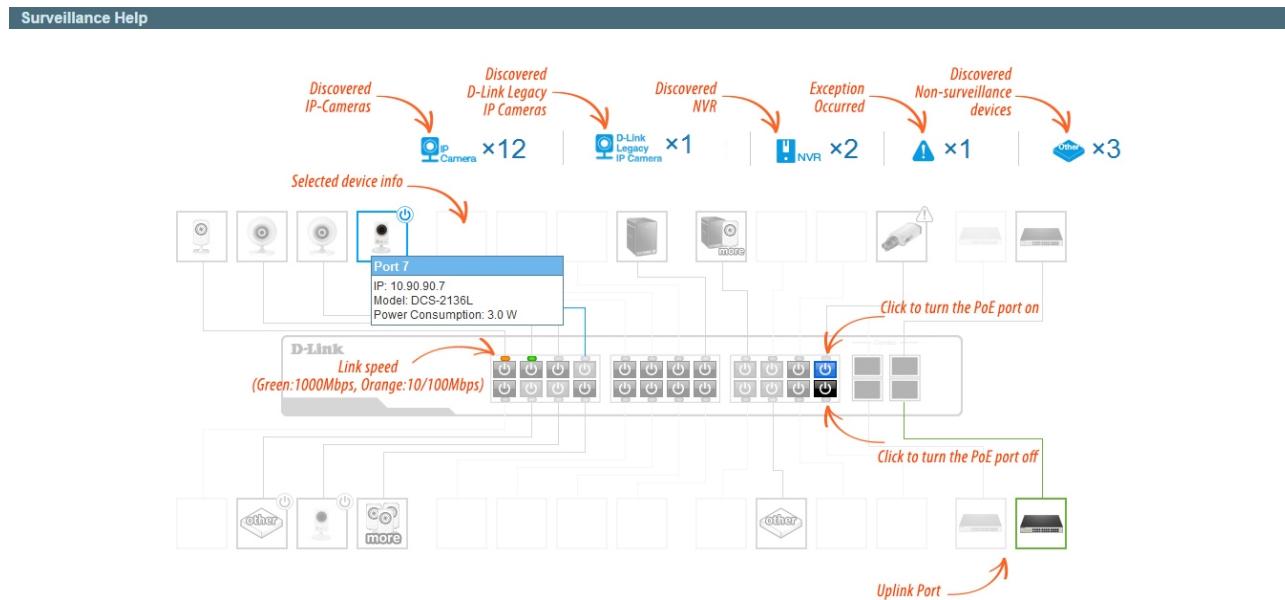


Figure 5.26 – Surveillance Mode > Help - Diagram

Device Status

Icon	Description	Icon	Description	Icon	Description
	The device is operational but is not powered by PoE.		The device is operational and is powered by PoE.		The device may malfunction. Some problem detected on this port or device.

IPC/NVR Status

Icon	Description	Icon	Description	Icon	Description
	One D-Link ONVIF IP-Camera discovered on this port. For D-Link IP-Camera, a specific icon will be displayed.		One ONVIF IP-Camera discovered on this port.		Multiple ONVIF IP-Cameras discovered on this port.
	One NVR discovered on this port. Any device connect to IP-Camera via HTTP, HTTPS and RTSP will be recognized as an NVR.		Multiple NVRs discovered on this port.		One ONVIF IP-Camera and one NVR discovered on this port.
	Multiple ONVIF IP-Cameras and one NVR discovered on this port.		One ONVIF IP-Camera and multiple NVRs discovered on this port.		Multiple ONVIF IP-Cameras and multiple NVRs discovered on this port.
	The port is up and no ONVIF IP-Camera, NVR, or other surveillance device has been discovered on this port.		This port is set as uplink port and the port status is up. Uplink port joins all VLANs and surveillance discovery process is disabled on this port.		This port is set as uplink port and the port status is down.

Figure 5.27 – Surveillance Mode > Help - Table

Tool Bar > Online Help

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



Figure 5.28 – Surveillance Mode > Online Help

Tool Bar > Standard Mode

By this option to access the **Standard Mode** Web UI available on the Switch.



NOTE: The **Web Mode** can only be changed to the **Standard Mode** when one user session is connected to the Web UI of the Switch.

6 Command Line Interface

The D-Link Smart Managed Switch allows a computer or terminal to perform some basic monitoring and configuration tasks by using the Command Line Interface (CLI) via TELNET protocol.

To connect a switch via TELNET:

1. Make sure the network connection between the switch and PC is active.
2. To connect, launch any terminal software like **HyperTerminal** in Microsoft Windows, or just use the command prompt by typing the command *telnet* followed by the switch IP address, eg. *telnet 10.90.90.90*.
3. The logon prompt will appear.

Logging on to the Command Line Interface:

Enter your User Name and Password to log in. The default user name and password is **admin**. Note that the user name and password are case-sensitive. Press **Enter** in both the Username and Password fields. The command prompt will appear as shown below (**DGS-1210-52MP>**):

```
DGS-1210-52MP> login: admin
Password:
DGS-1210-52MP>
```

Figure 6.1 – Command Prompt

The user session is automatically terminated if idle for the login timeout period. The default login timeout period is 5 minutes.

CLI Commands:

The Basic Switch commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
?	
download	{firmware_fromTFTP {<ipaddr>} <ipv6addr>} <path_filename (64)> cfg_fromTFTP {<ipaddr>} <ipv6addr>} <path_filename (64)> config_id <integer (1-2)>}
upload	{firmware_toTFTP {<ipaddr>} <ipv6addr>} <path_filename (64)> image_id <integer 1-2> cfg_toTFTP {<ipaddr>} <ipv6addr>} <path_filename (64)> config_id<integer (1-2)>}
config firmware	image_id <integer (1-2)> boot_up
config configuration	config_id <integer (1-2)> {delete boot_up}
config ipif	<ipif_name> { ipaddress <ip-address> <subnet-mask> gateway <gw-address> dhcp bootp }
config ipif	<ipif_name> { ipv6 ipv6address <ipv6networkaddr> dhcpcv6_client [enable disable] }
logout	
ping	<ip_addr>
ping6	<ipv6addr>
reboot	

Command	Parameter
reset config	
show boot_file	
show firmware information	
show flash information	
show ipif	[<ipif_name>]
show switch	
show route	{ipv4 ipv6}
config account	admin password <passwd>
save	[config config_id <integer (1-2)>]
debug info	

Each command is listed in detail, as follows:

?	
Purpose	To display a list of commands.
Syntax	?
Description	The ? command displays a list of commands of the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display a list of commands of the switch:

```
DGS-1210-52MP login: admin
Password:

DGS-1210-52MP> ?
USEREXEC commands :
  config account admin password <passwd>
  config configuration config_id <integer (1-2)> {delete | boot_up }
  config firmware image_id <integer (1-2)> boot_up
  config ipif <ipif_name> { ipaddress <ip-address> <subnet-mask> gateway <gw-add
ress> | dhcp | bootp }
  config ipif <ipif_name> { ipv6 ipv6address <ipv6networkaddr> | dhcipv6_client {
enable | disable}}
  debug info
  download {firmware_fromTFTP {<ipaddr>| <ipv6addr>} <path_filename (64)> | cfg_
fromTFTP {<ipaddr>| <ipv6addr>} <path_filename (64)> config_id <integer (1-2)>}
  logout
  ping <ip_addr>
```

```

ping6 <ipv6addr>
reboot
reset config
save [config config_id <integer (1-2)> ]
show boot_file
show firmware information
show flash information
show ipif [<ipif_name>]
show route { ipv4 | ipv6 }
show switch
upload {firmware_toTFTP {<ipaddr>|<ipv6addr>} <path_filename (64)> image_id <
<integer 1-2> | cfg_toTFTP {<ipaddr>|<ipv6addr>} <path_filename (64)> config_id
<integer (1-2)>}
DGS-1210-52MP>

```

download

Purpose	To download and install a firmware, boot, or switch configuration file from a TFTP server.
Syntax	download {firmware_fromTFTP {<ipaddr> <ipv6addr>} <path_filename (64)> cfg_fromTFTP {<ipaddr> <ipv6addr>} <path_filename (64)> config_id <integer (1-2)>}
Description	The download command downloads a firmware, boot, or switch configuration file from a TFTP server.
Parameters	<p><i>firmware_fromTFTP</i> – Download and install new firmware on the Switch from a TFTP server.</p> <p><i>cfg_fromTFTP</i> – Download a switch configuration file from a TFTP server.</p> <p><i><ipaddr></i> – The IPv4 address of the TFTP server.</p> <p><i><ipv6addr></i> – The IPv6 address of the TFTP server.</p> <p><i><path_filename 64></i> – The filename of the firmware or switch configuration file on the TFTP server. You need to specify the DOS path if the file is not at the root directory of the TFTP server.</p> <p><i>config_id <integer 1-2></i> - Specifies the configuration id to be configured.</p>
Restrictions	None.

Example usage:

To download a firmware file:

```
DGS-1210-52MP> download firmware_fromTFTP 1.1.1.23 1\ds_1210-10032.ros image_id 1
01-Jan-2000 01:19:48 %COPY-I-FILECPY: Files Copy – source URL tftp://1.1.1.23 /1\
ds_1210—10032.ros destination URL Unit all flash://image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
01–Jan–2000 01:22:49 %COPY-W-TRAP:
The copy operation was completed successfully
!
3920460 bytes copied in 00:03:01 [hh:mm:ss]

DGS-1210-52MP>
```



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

upload

Purpose	To upload the firmware file or a Switch configuration file to a TFTP server.
Syntax	<code>upload {firmware_toTFTP {<ipaddr> <ipv6addr>} <path_filename (64)> image_id <integer 1-2> cfg_toTFTP {<ipaddr> <ipv6addr>} <path_filename (64)>} config_id<integer (1-2)></code>
Description	The upload command uploads the Switch's current settings to a TFTP server.
Parameters	<p><i>firmware_toTFTP</i> – Upload the firmware on the Switch from a TFTP server.</p> <p><i>cfg_toTFTP</i> – Specifies that the Switch's current settings will be uploaded to the TFTP server.</p> <p><i><ipaddr></i> – The IPv4 address of the TFTP server.</p> <p><i><ipv6addr></i> – The IPv6 address of the TFTP server.</p> <p><i><path_filename 64></i> – The filename of the firmware or switch configuration file on the TFTP server. You need to specify the DOS path if the file is not at the root directory of the TFTP server.</p> <p><i>image_id <integer 1-2></i> - Specifies the image id to be configured.</p> <p><i>config_id <integer 1-2></i> - Specifies the configuration id to be</p>

	configured.
Restrictions	None.

Example usage:

To upload a firmware file:

```
DGS-1210-52MP>upload firmware_toTFTP 1.1.1.23 1\running--config image_id 1
01-Jan-2000 01:26:11 %COPY-I-FILECPY: Files Copy - source URL running-config
destination URL tftp://1.1.1.23/1\running--config
.....01-Jan-2000 01:26:16 %COPY-W-TRAP: The copy operation was completed success
fully
!
158 bytes copied in 00:00:05 [hh:mm:ss]
DGS-1210-52MP>
```

config firmware

Purpose	To configure which firmware image to be boot up.
Syntax	config firmware image id <integer (1-2)> boot_up
Description	The config firmware image id command configures the firmware image to be boot up on the Switch.
Parameters	<integer (1-2)> – Specifies the image 1 or 2 to be configured. boot_up – Specifies the specified image to be boot up.
Restrictions	None.

Example usage:

To configure the firmware image id 1 to be used when boot up on the Switch:

```
DGS-1210-52MP> config firmware image_id 1 boot_up
DGS-1210-52MP>
```

config configuration

Purpose	To specify which configuration file to be configured.
Syntax	config configuration config_id <integer (1-2)> {delete boot_up}
Description	The config configuration command configures the configuration image to be deleted or boot up on the Switch.
Parameters	<i>config_id <integer (1-2)></i> – Specifies the image 1 or 2 to be configured. <i>{delete boot_up}</i> – Specifies the configuration image to be deleted or boot up.
Restrictions	None.

Example usage:

To configure the configuration image id 1 to be used when boot up on the Switch:

```
DGS-1210-52MP> config configuration config_id 1 boot_up
```

Success.

```
DGS-1210-52MP>
```

config ipif system

Purpose	To configure the System IP interface.
Syntax	config ipif <ipif_name> { ipaddress <ip-address> <subnet-mask> gateway <gw-address> dhcp bootp }
Description	The config ipif system command configures the System IP interface on the Switch.
Parameters	<p><ipif_name> – Specifies the ipif name to be configured.</p> <p><i>ipaddress <ip-address> <subnet-mask></i> – The IP address and subnet mask to be created. Users need to specify the address and mask information using the traditional format (for example,10.1.2.3/255.0.0.0)</p> <p><i>gateway <gw-address></i> – The IP address of the router or gateway.</p> <p><i>dhcp</i> – Allows the selection of the DHCP protocol for the assignment of an IP address to the Switch's System IP interface.</p> <p><i>bootp</i> – Allows the selection of the BOOTP to the switch.</p>
Restrictions	None.

Example usage:

To configure the IP interface System:

```
DGS-1210-52MP> config ipif System ipaddress 10.48.74.122/8
```

Success.

```
DGS-1210-52MP>
```

config ipif system

Purpose	To configure the System IPv6 interface.
Syntax	config ipif <ipif_name> { ipv6 ipv6address <ipv6networkaddr> dhcpv6_client [enable disable] }
Description	The config ipif system command configures the System IPv6 interface on the Switch.
Parameters	<p><ipif_name> – Specifies the ipif name to be configured.</p> <p><i>ipv6 ipv6address <ipv6networkaddr></i> – Use this parameter to statically assign an IPv6address to this interface. This address should define a host address and a network prefix length. Multiple IPv6 addresses can be configured for a single IP interface. Ex: 3ffe:501:ffff:100::1/64. The /64 represents the prefix length of the IPv6 addresses.</p> <p><i>dhcpv6_client [enable disable]</i> – Specifies the DHCPv6 client to be disabled or enabled.</p>

Restrictions	None.
--------------	-------

Example usage:

To configure the IPv6 interface System:

```
DGS-1210-52MP> config ipif System ipv6 ipv6address 3ffe:501:ffff:100::1/64
```

Success.

```
DGS-1210-52MP>
```

logout

Purpose	To log out a user from the Switch's console.
Syntax	logout
Description	The logout command terminates the current user's session on the Switch's console.
Parameters	None.
Restrictions	None.

Example usage:

To terminate the current user's console session:

```
DGS-1210-52MP> logout
```



NOTE: Save your configuration changes before logging out.

ping

Purpose	To test the connectivity between network devices.
Syntax	ping <ip_addr>
Description	The ping command checks if another IP address is reachable on the network. You can ping the IP address connected to through the managed VLAN (VLAN 1 by default), as long as there is a physical path between the switch and the target IP equipment. By default, Switch sends five pings to the target IP.
Parameters	<ip_addr> – The IPv4 address of the host.
Restrictions	None.

Example usage:

To ping the IP address 10.90.90.91:

```
DGS-1210-52MP> ping 10.90.90.91
Reply Received From :10.90.90.91, TimeTaken : 20 msecs
Reply Received From :10.90.90.91, TimeTaken : 20 msecs
Reply Received From :10.90.90.91, TimeTaken : 20 msecs
```

```
--- 10.90.90.91 Ping Statistics ---
```

```
3 Packets Transmitted, 3 Packets Received, 0% Packets Loss
```

```
DGS-1210-52MP>
```

ping6

Purpose	To test the connectivity between network devices.
Syntax	ping6 <ipv6addr>
Description	The pingv6 command checks if another IP address is reachable on the network. You can ping the IP address connected to through the managed VLAN (VLAN 1 by default), as long as there is a physical path between the switch and the target IP equipment. By default, Switch sends five pings to the target IP.
Parameters	<ip6addr> – The IPv6 address of the host.
Restrictions	None.

Example usage:

To ping the IPv6 address 3000::1:

```
DGS-1210-52MP> ping6 3000 ::1
```

```
Reply Received From : 3000 ::1, TimeTaken : 20 msecs
```

```
Reply Received From : 3000 ::1, TimeTaken : 20 msecs
```

```
Reply Received From : 3000 ::1, TimeTaken : 20 msecs
```

```
--- 3000 ::1 Ping Statistics ---
```

```
3 Packets Transmitted, 3 Packets Received, 0% Packets Loss
```

```
DGS-1210-52MP>
```

reboot

Purpose	To reboot the Switch. If the Switch is a member of a stack, it may be rebooted individually, without affecting the other members of the stack.
Syntax	reboot
Description	The reboot command reboots the system. All network connections are terminated and the boot code executes.
Parameters	None.
Restrictions	None.

Example usage:

To restart the Switch:

```
DGS-1210-52MP> reboot
```

```
% Device will reboot, please wait a few minutes to re-login.
```

```
DGS-1210-52MP>
```

reset config

Purpose	To reset the Switch to the factory default settings.
Syntax	reset config
Description	All configurations will be reset to the default settings.
Parameters	None.
Restrictions	None.

Example usage:

To restore all of the Switch's parameters to their default values:

```
DGS-1210-52MP> reset config
% Device will reboot after reset configuration successfully.

DGS-1210-52MP>
```

show boot_file

Purpose	To display the information of the boot file on the Switch.
Syntax	show boot_file
Description	The show boot_file command displays the current information of boot file on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To the information of the boot file on the Switch:

```
DGS-1210-52MP> show boot_file
Bootup Firmware : image_1
Bootup Configuration : config_1

DGS-1210-52MP>
```

show firmware information

Purpose	To display the firmware information on the Switch.
Syntax	show firmware information
Description	The show firmware information command displays the current firmware information on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To the firmware information on the Switch:

```
DGS-1210-52MP> show firmware information
```

IMAGE ONE:

Version : 6.10.007
Size : 10608880 Bytes
Updated Time : 01/01/2017 00:06:15
From : 10.90.90.66
User : admin (web)

IMAGE TWO:

Version : 6.00.006
Size : 12288000 Bytes
Updated Time : 01/01/1970 00:00:00
From : 10.90.90.90
User : Anonymous (unknown)

DGS-1210-52MP>

show flash information

Purpose	To display the flash information on the Switch.
Syntax	show flash information
Description	The show flash information command displays the current flash information on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To the flash information on the Switch:

DGS-1210-52MP> show flash information

Flash ID : MX25L25635F

Flash size : 32MB

Partition	Used	Available	Use%
Boot	1000000	0	100
Image1	9744416	4411360	68
Image2	9744416	4411360	68
FileSystem	315392	3616768	8

DGS-1210-52MP>

show ipif

Purpose	To display the configuration of an IP interface on the Switch.
Syntax	show ipif [<ipif_name>]
Description	The show ipif command displays the current IP address of the switch.
Parameters	<ipif_name> – Specifies the IP interface name to be displayed.
Restrictions	None.

Example usage:

To display IP interface settings:

DGS-1210-52MP> show ipif

IP Setting Mode	: Static
Interface Name	: System
Interface VLAN Name	: default
IP Address	: 10.90.90.90
Subnet Mask	: 255.0.0.0
Default Gateway	: 0.0.0.0
DHCPv6 Client State	: Disabled

DGS-1210-52MP>

show switch

Purpose	To display the information of the Switch.
Syntax	show switch
Description	The show switch command displays the status of the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the switch information:

DGS-1210-52MP> show switch

System name	:
System Contact	:
System Location	:
System up time	: 0 days, 0 hrs, 19 min, 0 secs
System Time	: 01/01/2017 01:14:50
System hardware version	: F1

System firmware version	: 6.10.007
System boot version	: 1.00.010
System serial number	: QBDES12105200
MAC Address	: 00-01-02-03-04-05

DGS-1210-52MP>

show route

Purpose	To display the routing status of IPv4 or IPv6 on the Switch.
Syntax	show route {ipv4 ipv6}
Description	The show route command displays the routing status of IPv4 or IPv6 on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the IPv4 & IPv6 route status on the Switch:

DGS-1210-52MP> show route ipv4

IPv4 Static Route State : Disable

DGS-1210-52MP> show route ipv6

IPv6 Static Route State : Disable

DGS-1210-52MP>

config account admin password

Purpose	To display the configuration of an IP interface on the Switch.
Syntax	config account admin password <passwd>
Description	The config account admin password command sets the administrator password.
Parameters	<passwd> – The new password of the administrator.
Restrictions	None.

Example usage:

To configure the account admin password:

DGS-1210-52MP> config account admin password 1234

DGS-1210-52MP>

Save

Purpose	To save changes in the Switch's configuration to non-volatile RAM.
Syntax	save [config config_id <integer (1-2)>]
Description	The save command saves the configuration changes to the memory.
Parameters	None.
Restrictions	None.

Example usage:

To save the Switch's current configuration to non-volatile RAM:

```
DGS-1210-52MP> save config config_id 2
Building configuration ...
[OK]
DGS-1210-52MP>
```

debug info

Purpose	To display the ARP table and MAC FDB information of the Switch.
Syntax	debug info
Description	The debug info command displays the ARP table and MAC FDB of the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the ARP table and MAC FDB information of the Switch:

```
DGS-1210-52MP> debug info
% sgementation fault log file :

File doesn't exist !!!
% ARP table :

Address      Hardware Address   Type    Interface Mapping
-----      -----
10.0.0.0      ff-ff-ff-ff-ff-ff      ARPA   vlan1     Static
10.90.90.90   4a-6f-6e-01-01-01      ARPA   vlan1     Static
10.90.90.96   3c-97-0e-e5-76-4d      ARPA   vlan1     Dynamic
10.255.255.255 ff-ff-ff-ff-ff-ff      ARPA   vlan1     Static
```

% MAC table :

Vlan	Mac Address	Type	Ports
1	3c:97:0e:e5:76:4d	Learnt	Gi0/5

Total Mac Addresses displayed: 1

% POE MCU VERSION :

PoeVersion : 24 (0x18)
PoeExtVersion : 33 (0x21)

DGS-1210-52MP>

Appendix A - Ethernet Technology

This chapter will describe the features of the D-Link Smart Managed 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: 14.88Mpps DGS-1210-10P: 14.88Mpps DGS-1210-10MP: 14.88Mpps DGS-1210-20: 29.8Mpps DGS-1210-26: 38.7Mpps DGS-1210-28: 41.7Mpps DGS-1210-28P: 41.7Mpps DGS-1210-28MP: 41.7Mpps DGS-1210-52: 77.4Mpps DGS-1210-52MP: 77.4Mpps
Forwarding Mode	Store and Forward
Packet Buffer memory	DGS-1210-10: 4.1Mbits DGS-1210-10P: 4.1Mbits DGS-1210-10MP: 4.1Mbits DGS-1210-20: 4.1Mbits DGS-1210-26: 4.1Mbits DGS-1210-28: 4.1Mbits DGS-1210-28P: 4.1Mbits DGS-1210-28MP: 4.1Mbits DGS-1210-52: 12Mbits DGS-1210-52MP: 12Mbits
DDRIII for CPU	128M bytes
Flash Memory	32M bytes
Priority Queues	8
Port Functions	
10/100/1000BASE-TX	8 x 10/100/1000BaseT ports for DGS-1210-10/10P/10MP

Ethernet ports	<p>16 x 10/100/1000BaseT ports for DGS-1210-20 24 x 10/100/1000BaseT ports for DGS-1210-26/28/28P/28MP 48 x 10/100/1000BaseT ports for DGS-1210-52/52MP</p> <p>1000Base-T ports compliant to following standards:</p> <ul style="list-style-type: none"> - IEEE 802.3 compliance - IEEE 802.3u compliance - IEEE 802.3ab compliance <p>Support Half/Full-Duplex operations</p> <ul style="list-style-type: none"> - IEEE 802.3x Flow Control support for Full-Duplex mode - Back Pressure for Half-Duplex mode - Head-of-line blocking prevention <p>Support manual/auto MDI/MDIX configuration Support Auto-Negotiation for each port</p>
SFP ports	<p>Port 9 ~ 10 for DGS-1210-10/10P/10MP Port 25 ~ 26 for DGS-1210-26</p> <p>SFP ports comply with following standards:</p> <ul style="list-style-type: none"> - IEEE 802.3u compliance (Support 100M transceivers) - IEEE 802.3z compliance - IEEE 802.3ah compliance <p>Support Transceivers:</p> <ul style="list-style-type: none"> - 100M/1000M SFP Transceivers - WDM SFP Transceivers - 1000BASE-T Transceivers
Combo ports	<p>4 combo 1000BASE-T/SFP ports for DGS-1210-20/28/28P/28MP/52/52MP</p> <p>SFP Transceivers Supported:</p> <ul style="list-style-type: none"> - 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-LH, 50km) - DEM-315GT (1000BASE-ZX, 80km) - DEM-312GT2 (1000BASE-SX, 2km) <p>WDM Transceivers Supported:</p> <ul style="list-style-type: none"> - 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)
Physical & Environment	
	<p>DGS-1210-10: Maximum power consumption: 6.33 Watts Standby power consumption: 2.07 Watts</p> <p>DGS-1210-10P: Maximum power consumption: 81.9 Watts (PoE On), 7.6 Watts (PoE Off) Standby power consumption: 2.5 Watts</p> <p>DGS-1210-10MP: Maximum power consumption: 152.3 Watts (PoE On), 9.4 Watts (PoE Off) Standby power consumption: 5.2 Watts</p> <p>DGS-1210-20: Maximum power consumption: 13.08 Watts Standby power consumption: 5.56 Watts</p> <p>DGS-1210-26: Maximum power consumption: 15.22 Watts Standby power consumption: 5.06 Watts</p> <p>DGS-1210-28: Maximum power consumption: 17.32 Watts Standby power consumption: 6.55 Watts</p> <p>DGS-1210-28P: Maximum power consumption: 263.9 Watts (PoE On), 30.6 Watts (PoE Off) Standby power consumption: 19.6 Watts</p> <p>DGS-1210-28MP: Maximum power consumption: 446.1 Watts (PoE On), 29.8 Watts (PoE Off) Standby power consumption: 18.5 Watts</p> <p>DGS-1210-52: Maximum power consumption: 34.85 Watts Standby power consumption: 13.9 Watts</p> <p>DGS-1210-52MP: Maximum power consumption: 478.9 Watts (PoE On), 54.4 Watts (PoE Off) Standby power consumption: 32 Watts</p>
Power Consumption	
Power Supply	AC input, 100~240 VAC, 50/60Hz, internal universal power supply AC input, 100~240 VAC, 50/60Hz, DC 54V/1.574A external desktop power adapter (only DGS-1210-10P)
Fans	DGS-1210-10: Fanless DGS-1210-10P: Fanless DGS-1210-10MP: Fanless

	DGS-1210-20: Fanless DGS-1210-26: Fanless DGS-1210-28: Fanless DGS-1210-28P: 2pcs Smart Fan DGS-1210-28MP: 2pcs Smart Fan DGS-1210-52: Fanless DGS-1210-52MP: 3pcs Smart Fan
Operating Temperature	-5~50°C
Storage Temperature	-20~70°C
Humidity	Storage: 0%~95% non-condensing
Dimensions	DGS-1210-10: 280mm x 126mm x 44mm DGS-1210-10P: 280mm x 126mm x 44mm DGS-1210-10MP: 330mm x 180mm x 44mm DGS-1210-20: 280mm x 180mm x 44mm DGS-1210-26: 440mm x 140mm x 44mm DGS-1210-28: 440mm x 140mm x 44mm DGS-1210-28P: 440mm x 250mm x 44mm DGS-1210-28MP: 440mm x 250mm x 44mm DGS-1210-52: 440mm x 210mm x 44mm DGS-1210-52MP: 440mm x 431mm x 44mm
Weight	DGS-1210-10: 0.98kg DGS-1210-10P: 0.95kg DGS-1210-10MP: 1.77kg DGS-1210-20: 1.75kg DGS-1210-26: 2.06kg DGS-1210-28: 2.15kg DGS-1210-28P: 3.75kg DGS-1210-28MP: 3.94kg DGS-1210-52: 3.46kg DGS-1210-52MP: 6.26kg
EMI	CE, FCC/IC, VCCI, BSMI, C-Tick, CCC
Safety	UL, CB, BSMI, CCC

Features**L2 Features**

- Supports up to 8K MAC address for DGS-1210-10/10P/10MP/20/26/28/28P/28MP, and 16K for DGS-1210-52/52MP
- 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 256 static multicast groups
- MLD Snooping:
 - Supports max. 256 MLD Snooping groups
 - Supports 256 static MLD groups per device
- 802.1D Spanning Tree
- 802.1w Rapid Spanning Tree
- 802.1s MSTP
- Loopback Detection
- 802.3ad Link Aggregation:
 - DGS-1210-10/10P/10MP: Supports max 4 groups per device and 8 ports per group
 - DGS-1210-20/26/28/28P/28MP: Supports max 8 groups per device and 8 ports per group
 - DGS-1210-52/52MP: Supports max 16 groups per device and 8 ports per group
- 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

VLAN

- 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

AAA

- 802.1X port-based access control
- Support RADIUS server

ACL

- 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

OAM

- › Cable Diagnostics
- › Reset button (reset to factory default)

Management

- › 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 (T_{ma}) specified by the manufacturer.
- B) Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
- C) Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- D) Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- E) Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).



D-Link[®]
Building Networks for People