

DES-1210-08P/28 / 28P / 52

MANUAL

WEB UI REFERENCE GUIDE

SMART MANAGED SWITCH

Ver. 4.20



Table of Contents

Table of Contents	i
About This Guide	1
Terms/Usage	1
Copyright and Trademarks	1
1 Product Introduction	2
DES-1210-08P	3
Front Panel	3
Rear Panel	3
DES-1210-28	4
Front Panel	4
Rear Panel	4
DES-1210-28P	4
Front Panel	5
Rear Panel	5
DES-1210-52	6
Front Panel	6
Rear Panel	6
2 Hardware Installation	7
Safety Cautions	7
Step 1: Unpacking	8
Step 2: Switch Installation	8
Desktop or Shelf Installation	8
Rack Installation	8
Step 3 – Plugging in the AC Power Cord with Power Cord Clip	9
Power Failure	12
Grounding the Switch	12
3 Getting Started	13
Management Options	13
Using Web-based Management	13
Supported Web Browsers	13
Connecting to the Switch	13
Login Web-based Management	13
Web-based Management	14
4 Configuration	15
Smart Wizard Configuration	15
IP Information	15
Password Settings	15
SNMP Settings	16
Web-based Management	17
Tool Bar > Save Menu	18
Save Configuration	18
Save Log	18
Tool Bar > Tool Menu	18
Reset	18
Reset System	18
Reboot Device	18
Configuration Backup & Restore	19

Firmware Backup and Upgrade.....	19
Tool Bar > Smart Wizard.....	20
Tool Bar > Online Help.....	20
Function Tree	21
Device Information.....	22
System > System Settings	23
System > IPv6 System Settings	23
System > IPv6 Route Settings.....	24
System > IPv6 Neighbor Settings	24
System > Password.....	25
System > Port Settings.....	25
System > Port Description.....	26
System > DHCP Auto Configuration	27
System > DHCP Relay > DHCP Relay Global Settings.....	27
System > DHCP Relay > DHCP Relay Interface Settings	29
System > DHCP Local Relay Settings	29
System > DHCPv6 Relay Settings	29
System > SysLog Host.....	30
System > Time Profile	31
System > Power Saving	31
System > IEEE802.3az EEE Settings	32
System > D-Link Discover Protocol Settings.....	33
VLAN > 802.1Q VLAN (Asymmetric VLAN).....	34
VLAN > 802.1Q VLAN PVID	35
VLAN > 802.1Q Management VLAN.....	35
VLAN > Voice VLAN > Voice VLAN Global Settings	36
VLAN > Voice VLAN > Voice VLAN Port Setting	37
VLAN > Voice VLAN > Voice Device List.....	38
VLAN > Auto Surveillance VLAN	38
L2 Functions > Jumbo Frame.....	39
L2 Functions > Port Mirroring.....	39
L2 Functions > Loopback Detection.....	40
L2 Functions > MAC Address Table > Static MAC	41
L2 Functions > MAC Address Table > Dynamic Forwarding Table	41
L2 Functions > Spanning Tree > STP Global Settings	42
L2 Functions > Spanning Tree > STP Port Settings	43
L2 Functions > Link Aggregation > Port Trunking.....	44
L2 Functions > Link Aggregation > LACP Port Settings	45
L2 Functions > Multicast > IGMP Snooping.....	45
L2 Functions > Multicast > MLD Snooping	47
L2 Functions > Multicast > Multicast Forwarding	48
L2 Functions > Multicast > Multicast Filtering Mode	48
L2 Functions > SNTP > Time Settings.....	49
L2 Functions > SNTP > TimeZone Settings.....	50
L2 Functions > LLDP > LLDP Global Settings	50
L2 Functions > LLDP > LLDP-MED Settings	51
L2 Functions > LLDP > LLDP Port Settings.....	51
L2 Functions > LLDP > 802.1 Extension TLV	52
L2 Functions > LLDP > 802.3 Extension TLV	53

L2 Functions > LLDP > LLDP Management Address Settings	54
L2 Functions > LLDP > LLDP Management Address Table	54
L2 Functions > LLDP > LLDP Local Port Table	55
L2 Functions > LLDP > LLDP Remote Port Table	55
L2 Functions > LLDP > LLDP Statistics	56
QoS > Bandwidth Control.....	57
QoS > 802.1p/DSCP/ToS.....	57
Security > Trusted Host.....	59
Security > Port Security.....	59
Security > Traffic Segmentation	60
Security > Safeguard Engine.....	60
Security > Storm Control	61
Security > ARP Spoofing Prevention	61
Security > DHCP Server Screening	62
Security > SSL Settings.....	62
Security > DoS Prevention Settings	63
Security > SSH > SSH Settings	63
Security > SSH > SSH Authmode and Algorithm Settings.....	64
Security > SSH > SSH User Authentication Lists	65
Security > Smart Binding > Smart Binding Settings.....	65
Security > Smart Binding > Smart Binding	66
Security > Smart Binding > White List.....	67
Security > Smart Binding > Black List	67
AAA > RADIUS Server	67
AAA > 802.1X > 802.1X Global Settings.....	68
AAA > 802.1X > 802.1X Port Settings.....	69
AAA > 802.1X > 802.1X User.....	70
ACL > ACL Wizard	70
ACL > ACL Access List	80
ACL > ACL Access Group.....	81
ACL > ACL Hardware Resource Status	81
PoE > PoE Global Settings (DES-1210-08P/28P only)	81
PoE > PoE Port Settings (DES-1210-08P/28P only)	82
SNMP > SNMP > SNMP Global Settings	83
SNMP > SNMP > SNMP User	84
SNMP > SNMP > SNMP Group	85
SNMP > SNMP > SNMP View	86
SNMP > SNMP > SNMP Community.....	86
SNMP > SNMP > SNMP Host.....	86
SNMP > SNMP > SNMP Engine ID	87
SNMP > RMON > RMON Global Settings	87
SNMP > RMON > RMON Statistics	87
SNMP > RMON > RMON History.....	88
SNMP > RMON > RMON Alarm	88
SNMP > RMON > RMON Event.....	89
Monitoring > Port Statistics.....	89
Monitoring > Cable Diagnostics	90
Monitoring > System Log.....	91
5 Command Line Interface.....	93

To connect a switch via TELNET:	93
Logging on to the Command Line Interface:	93
CLI Commands:	93
download	93
upload	94
config ipif system	94
logout	95
ping	95
reboot	95
reset	96
show ipif	96
show switch	96
config account admin password	97
save	97
debug info	97
Appendix A - Ethernet Technology	98
Gigabit Ethernet Technology	98
Fast Ethernet Technology	98
Switching Technology	98
Appendix B - Technical Specifications	99
Hardware Specifications	99
Key Components / Performance	99
Port Functions	99
Physical & Environment	99
Emission (EMI) Certifications	99
Safety Certifications	99
Features	99
L2 Features	99
VLAN	100
ACL	100
QoS (Quality of Service)	100
AAA	100
Security	100
OAM	100
Management	100
D-Link Green Technologies	100
Appendix C – Rack mount Instructions	101

About This Guide

This guide Provides installations to install the D-Link DES-1210 Series Smart Managed Switch (DES-1210-08P/28/28P/52) and to configure with HTTP step-by-step.



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

This guide is mainly divided into three parts:

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

Terms/Usage

In this guide, the term “Switch” (first letter capitalized) refers to the 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.

© 2012 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 Ethernet switch series blends plug-and-play simplicity with exceptional value and reliability for small and medium-sized business (SMB) networking. All models are housed in a new style rack-mount metal case with easy-to-view front panel diagnostic LEDs, and provides advance features including two combo 1000BASE-T/SFP and two additional Gigabit uplinks, network security, traffic segmentation, QoS and versatile management.

Flexible Port Configurations. The DES-1210 Series offer four models: 24/48 10/100 Base-T ports or 8/24 10/100 Base-T with PoE features. All ports of the switch support auto MDI/MDIX feature which bring inexpensive and easy Ethernet connection to the desktops. Each switch provides 4 Gigabit uplinks connection to a Gigabit backbone or servers. Two of the Gigabit ports are SFP combo ports which support both 1000M and 100M fiber connections.

Extensive Layer 2 Features. Implemented as complete Layer 2 devices, these switches include functions such as IGMP Snooping, Port Mirroring, Spanning Tree, 802.3ad LACP, SNTP, LLDP and Loopback Detection to enhance performance and network resiliency.

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 feature like 802.1X port-based authentication provides access control of the network with external RADIUS servers. ACL is a powerful tool to screen unwanted IP or MAC traffic. Storm Control keeps the network from being overwhelmed by abnormal traffic. Port Security is another simple but useful authentication method to maintain the integrity of the network device.

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 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 also come with the D-View plug-in module that works with D-View 6, SNMP Management Software which provides easy-to-use graphic interface and facilitates the operation efficiency.

DES-1210-08P

8-Port 10/100Mbps ports Smart Managed PoE Switch.

Front Panel

Figure 1.1 – DES-1210-08P Front Panel

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

Pwr Max: The Pwr Max LED lights up 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 72 Watts.

- Solid Red: When the total PoE output power achieve max power budget.
- Off: System still have spare power for new PD.

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

Link/Act LED (Ports 1-8):

- Solid Green: When there is a secure 10/100Mbps connection at the port.
- Blinking Green: Indicates that the Switch is either sending or receiving data to the port.
- Light off: No link.

Speed LED (Ports 1-8):

- Solid Green: When there is reception or transmission of data occurring at 100Mbps.
- Light off: When there is reception or transmission of data occurring at 10Mbps or no link.

PoE Mode (Ports 1-8):

- Green: Indicates that PoE mode is active.
- Amber: Indicates that there is an issue with the PoE mode activating properly.
- Light off: Indicates that PoE mode is not active.



NOTE: The LED behavior for ports 1-8 will switch between link mode and PoE mode when the PoE mode is active..



NOTE: The installation instructions clearly state that the ITE is to be connected only to PoE networks without routing toe the outside plant.

Rear Panel

Figure 1.2 – DES-1210-08P Rear Panel

48V/1.875A AC Adapter: The port is where to connect the 48V/1.875A AC adapter.

DES-1210-28

24-Port 10/100Mbps with 2 10/100/1000 BASE-T and 2 Combo 1000 BASE-T/SFP Smart Managed Switch.

Front Panel

Figure 1.3 – DES-1210-28 Front Panel

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

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

Link/Act/Speed LED (Ports 1-24):

- Solid Green: When there is a secure 100Mbps connection at the port.
- Blinking Green or Amber: Indicates that the Switch is either sending or receiving data to the port.
- Solid Amber: When there is a secure 10Mbps connection at the port.
- Light off: No link.

Link/Act/Speed Led (Port 25, 26, 27T, 28T, 27F, 28F):

- Solid Green: There is a secure 1000Mbps connection at the port.
- Blinking Green or Amber: There is reception or transmission occurring at the port.
- Solid Amber: Indicates that the port is running at 10/100Mbps.
- Light off: No link.



NOTE: On DES-1210-28, the MiniGBIC ports are shared with normal RJ-45 ports 27 and 28. When 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.

Rear Panel

Figure 1.4 – DES-1210-28 Rear Panel

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

DES-1210-28P

24-Port 10/100Mbps PoE ports plus 2 1000Base-T ports and 2 combo SFP/1000Base-T ports Smart Managed PoE Switch.

Front Panel

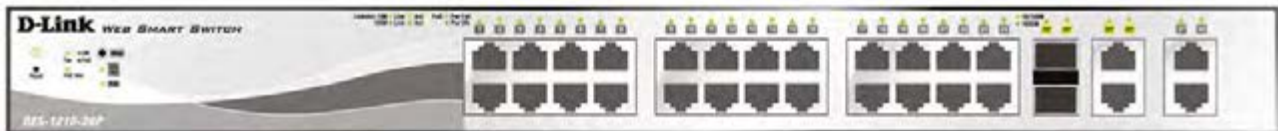


Figure 1.5 – DES-1210-28P Front Panel

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

Pwr Max: The Pwr Max LED lights up 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.

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

LED Mode Button: Pressing this button will change the LED behavior from Link mode and PoE Mode.

Fan:

- Green: All diagnostics pass. The fan is operation well.
- Amber: The fan has failed to work.

Link/Act/Speed LED (Ports 1-24):

- Solid Green: When there is a secure 100Mbps connection at the port.
- Blinking Green or Amber: Indicates that the Switch is either sending or receiving data to the port.
- Solid Amber: where there is a secure 100Mbps connection at the port.
- Light off: No link.

LinkAct/Speed LED (Ports 25T, 26T, 25F, 26F, 27, 28):

- Solid Green: There is a secure 1000Mbps connection at the port.
- Blinking Green: There is reception or transmission occurring at the port.
- Solid Amber: There is a secure 10/100Mbps connection at the port
- Light off: No link.

PoE Mode (Port 1-24):

- Green: Indicates that PoE mode is active.
- Amber: Indicates that there is an issue with the PoE mode activating properly.
- Light off: Indicates that PoE mode is not active.



NOTE: On DES-1210-28P, the MiniGBIC ports are shared with normal RJ-45 ports 25T and 26T. When 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: The installation instructions clearly state that the ITE is to be connected only to PoE networks without routing toe the outside plant.

Rear Panel



Figure 1.6 – DES-1210-28P Rear Panel

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

DES-1210-52

48-Port 10/100Mbps Smart Managed Switch with 2 10/100/1000 BASE-T and 2 Combo 1000 BASE-T/SFP Smart Managed Switch.

Front Panel

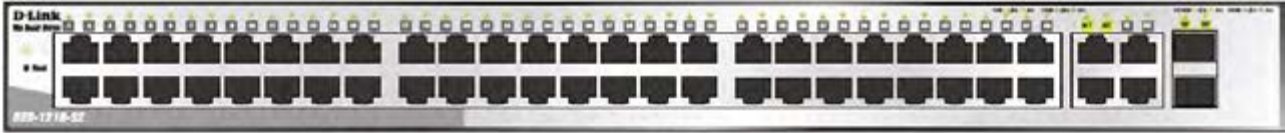


Figure 1.7 – DES-1210-52 Front Panel

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

Reset: Press the reset button to reset the Switch back to the default settings. All previous changes will be lost.

Link/Act/Speed LED (Ports 1-48):

- Solid Green: When there is a secure 100Mbps connection at the port.
- Blinking Green or Amber: Indicates that the Switch is either sending or receiving data to the port.
- Solid Amber: When there is a secure connection (or link) to 10Mbps Ethernet device at any of the ports.
- Light off: No link.

Link/Act/Speed LED (Ports 49F, 50F, 49T, 50T, 51, 52):

- Solid Green: There is a secure 1000Mbps connection at the port.
- Blinking Green: There is reception or transmission occurring at the port.
- Solid Amber: When there is a secure connection (or link) to 10/100Mbps Ethernet device at any of the ports.
- Light off: No link.



NOTE: On the DES-1210-52, the MiniGBIC ports are shared with normal RJ-45 ports 49 and 50. 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.

Rear Panel



Figure 1.8 – DES-1210-52 Rear Panel

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

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 DES-1210 Series Switch
- › One Multilingual Getting Started Guide
- › User Guide CD
- › Power cord and Power Cord Retainer or external power adapter
- › 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).

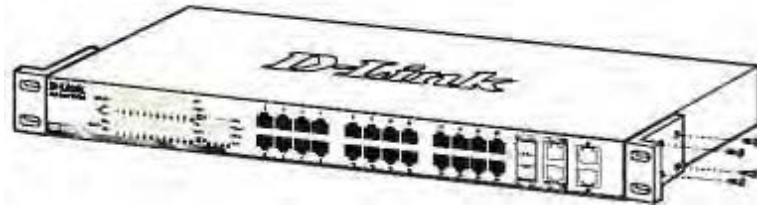


Figure 2.2 – Attach the mounting brackets to the Switch

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

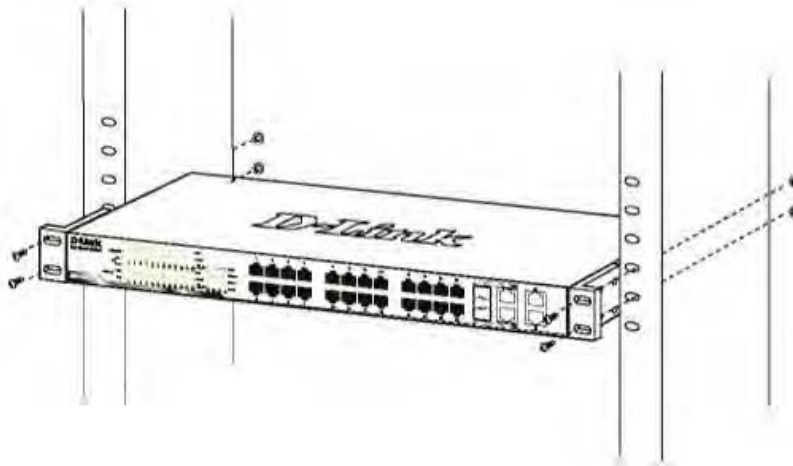


Figure 2.3 – Mount the Switch in the rack or chassis

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.

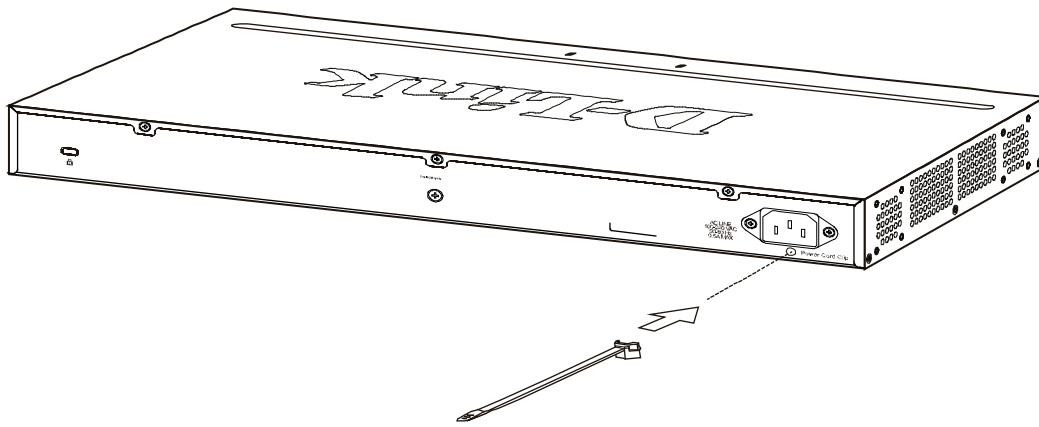


Figure 2.1 – Insert Tie Wrap to the Switch

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

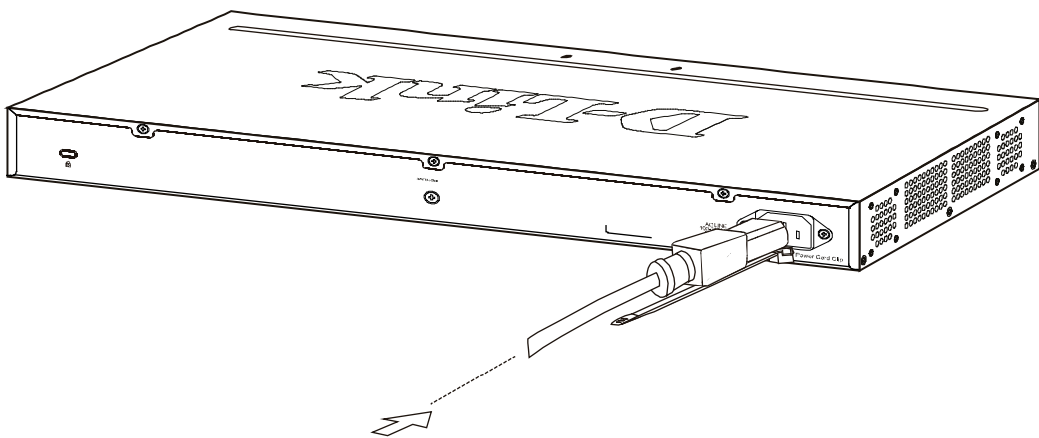


Figure 2.2 – Connect the power cord to the Switch

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

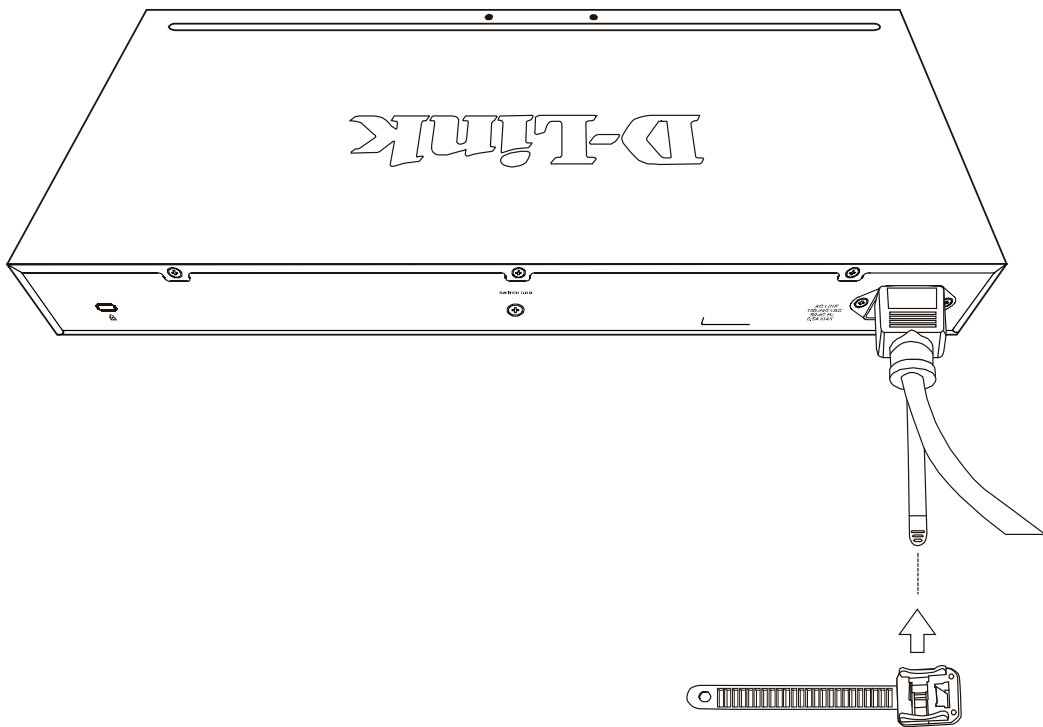


Figure 2.3 – Slide the Retainer through the Tie Wrap

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

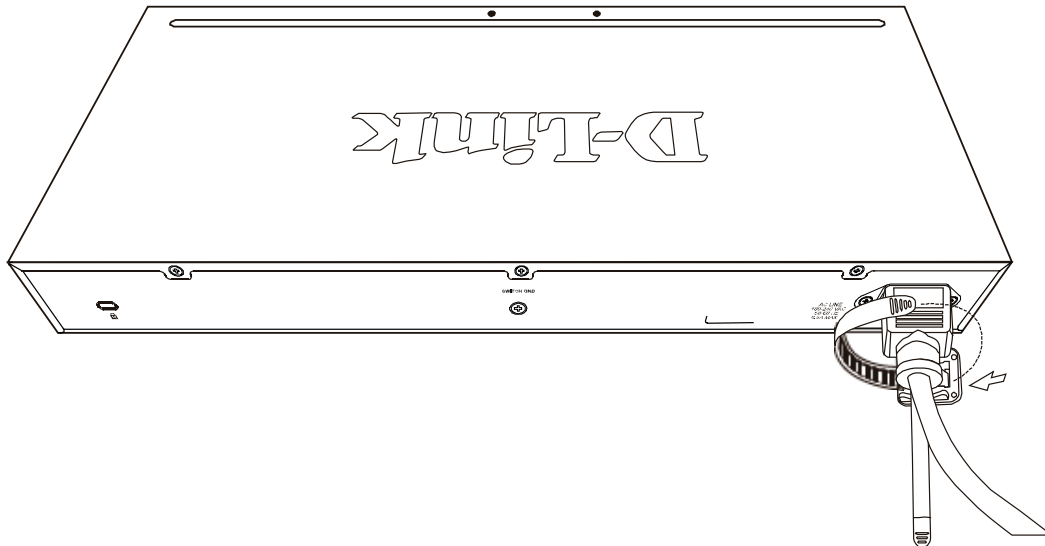


Figure 2.4 – Circle around the power cord

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

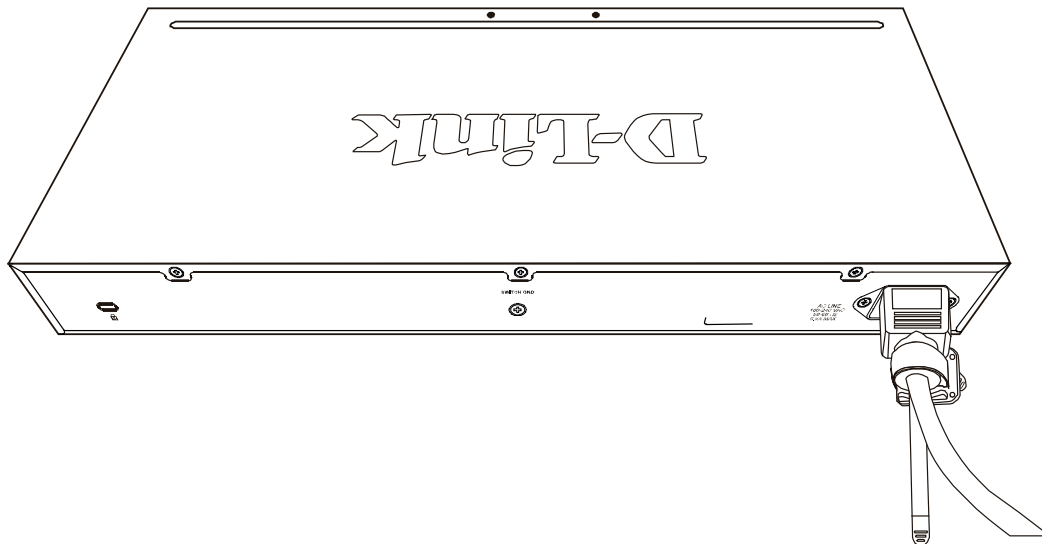


Figure 2.5 – Secure the power cord

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

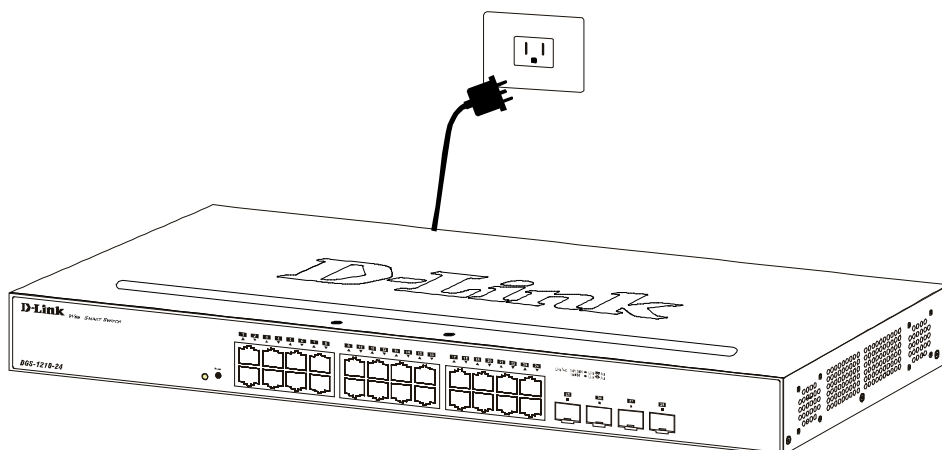


Figure 2.6 – Plugging the switch into an outlet

Power Failure

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

Grounding the Switch

This section describes how to connect the DES-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.

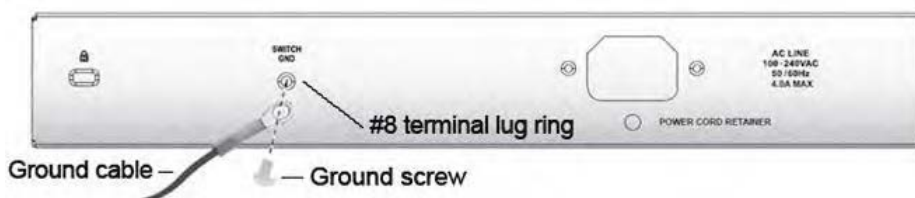


Figure 2.7 – Connect a Grounding Cable

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.

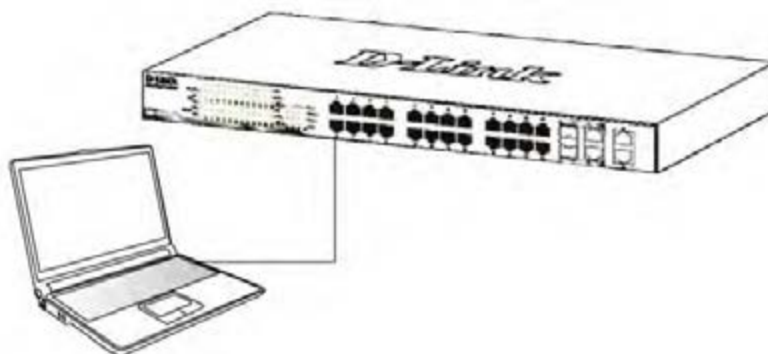


Figure 3.1 – Connected Ethernet cable

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 open the web browser and enter **10.90.90.90** (the factory-default IP address) in the address bar. Then press <Enter>.

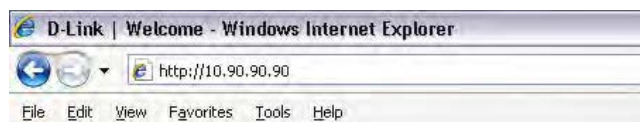


Figure 3.2 –Enter the IP address 10.90.90.90 in the web browser



NOTE: The switch's factory default IP address is 10.90.90.90 with a subnet mask of 255.0.0.0 and a default gateway of 0.0.0.0.

When the following logon dialog box appears, enter the 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

Web-based Management

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

4 Configuration

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

Smart Wizard Configuration

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

IP Information

IP Information will guide you to do basic configurations in 3 steps for the IP Information, access password, and SNMP. Select **Static**, **DHCP** or **BOOTP**, and enter the desired new **IP Address**, select the **Netmask** and enter the Gateway address, then click the Next button to enter the next Password setting page. (No need to enter **IP Address**, **Netmask** and **Gateway** if DHCP and BOOTP are selected.) The Smart Wizard is for the quick setting in IPv4 environment. For IPv6 network, please go to [System > IPv6 System Settings](#)

. If you are not changing the settings, click **Exit** button to go back to the main page. Or you can click on **Ignore the wizard next time** to skip wizard setting when the switch boots up.



The screenshot shows the 'Welcome to Smart Wizard' interface. It includes a title bar, a main content area with a D-Link logo and introductory text, and a 'Step 1 of 3' section titled 'IP Information'. This section contains three radio buttons for 'Static', 'DHCP', and 'BOOTP'. Below them are input fields for 'IP Address' (containing '10.90.90.90'), 'Netmask' (a dropdown menu showing '255.0.0.0'), and 'Gateway' (containing '0.0.0.0'). At the bottom, there is a checkbox for 'Ignore the wizard next time' and three buttons: 'Exit', 'Back', and 'Next'.

Figure 4.1 – IP Information in Smart Wizard



NOTE: The Smart Wizard supports quick settings for IPv4 network

Password Settings

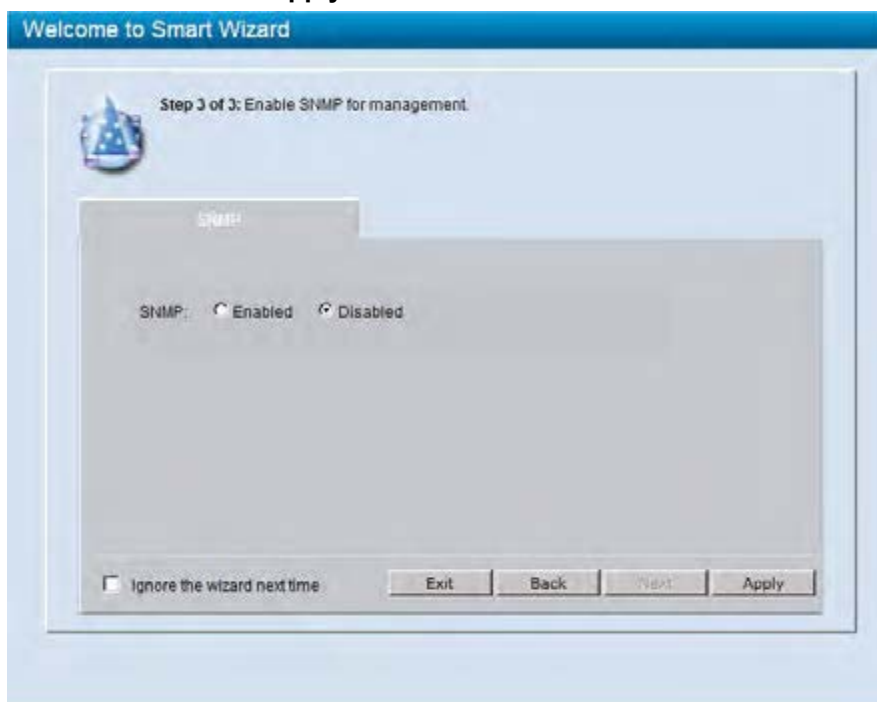
Type the desired new password in the **Password** box and again in the **Confirm Password**, then click the **Next** button to the **SNMP** setting page.



Figure 4.2 – Password setting in Smart Wizard

SNMP Settings

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.



4.3 – SNMP Setting 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.

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



Figure 4.4 – 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:

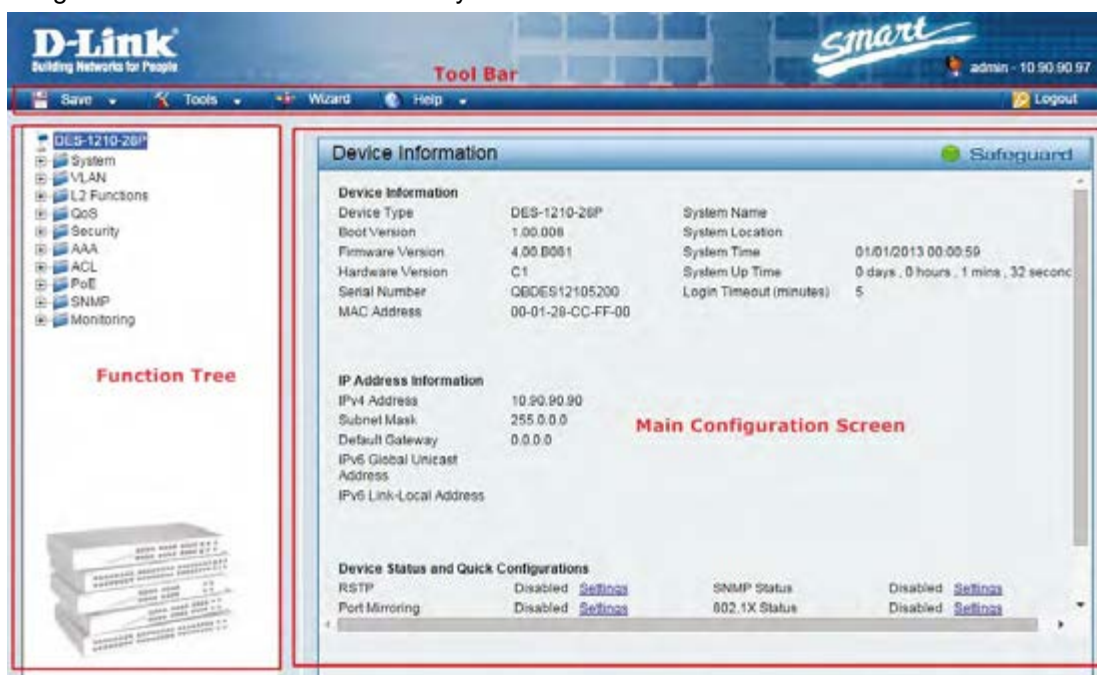


Figure 4.5 – Web-based Management

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

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

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

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

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



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

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.

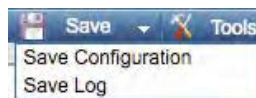


Figure 4.6 – Save Menu

Save Configuration

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



Figure 4.7 – 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).

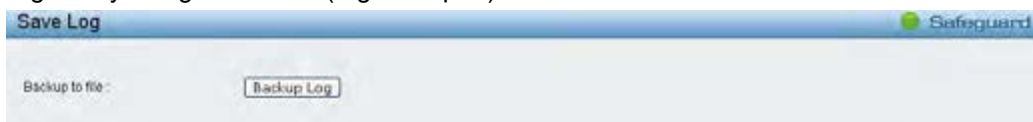


Figure 4.8 – Save Log

Tool Bar > Tool Menu

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



Figure 4.9 – 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 4.10 – Tool Menu > Reset

Reset System

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



Figure 4.11 – Tool Menu > Reset System

Reboot Device

Provide a safe way to reboot the system. Click **Apply** to restart the switch.



Figure 4.12 – Tool Menu > Reboot Device

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 the file. Two methods can be selected: **HTTP** or **TFTP**.



Figure 4.13 – Tool Menu > Configuration Backup and Restore

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

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

Click **Browse** 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. Select **IPv4** or **IPv6** and specify **TFTP Server IP Address** and **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**.



Figure 4.14 – Tool Menu > Firmware Backup and Upgrade

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

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

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

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

TFTP: Backup or upgrade the firmware to or from a remote TFTP server. Select IPv4 or IPv6 and specify **TFTP Server IP Address** and **File Name** for the configuration 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.



CAUTION: Do not disconnect the PC or remove the power cord from device until upgrade complete. Switch may crash if Firmware upgrade incompletely.

Tool Bar > Smart Wizard

By clicking the Smart 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: **Online 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.

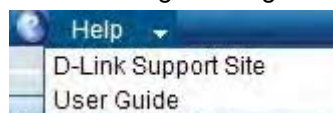


Figure 4.15 – Online Help



Figure 4.16 – User Guide Micro Site

Function Tree

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

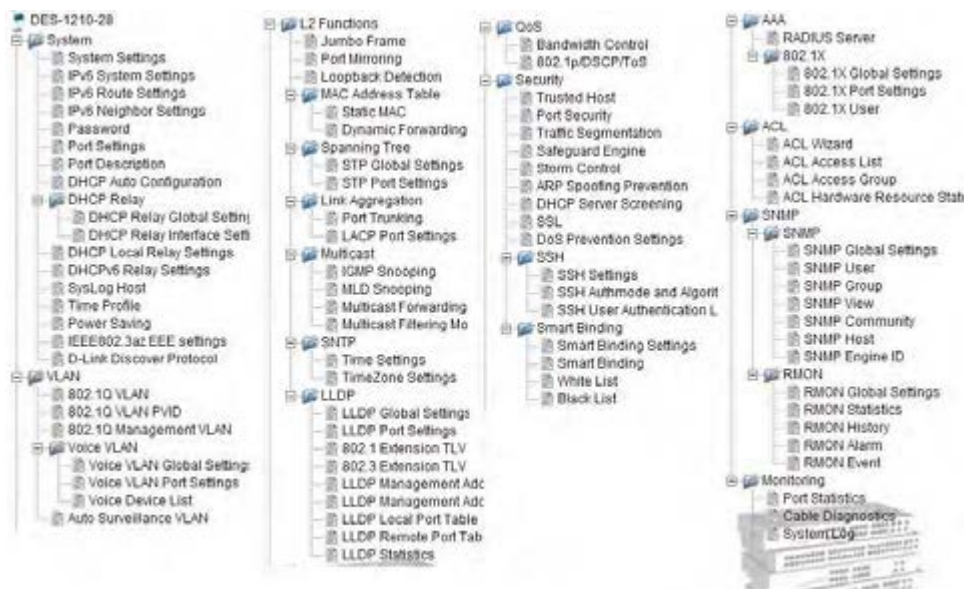


Figure 4.17 –Function Tree

Device Information

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

It also offers an overall status of common software features:

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

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

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

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

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

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

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

Safeguard Engine: Click **Setting** to link to Security > Safeguard Engine. Default is enabled.

IGMP Snooping: Click **Setting** to link to L2 Functions > Multicast > IGMP Snooping. Default is disabled.

Power Saving: Click **Setting** to link to System > Power Saving. Default is enabled.

Device Information		Safeguard	
Device Information			
Device Type	DES-1210-28P	System Name	
Boot Version	1.00.008	System Location	
Firmware Version	4.00.B001	System Time	01/01/2013 00:00:59
Hardware Version	C1	System Up Time	0 days , 0 hours , 1 mins , 32 second
Serial Number	QBDES12105200	Login Timeout (minutes)	5
MAC Address	00-01-28-CC-FF-00		
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

Figure 4.18 – Device Information

System > System Settings

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

IP 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 **IP Address**, **Subnet Mask** 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**.

System Information: By entering a **System Name** and **System Location**, the device can more easily be recognized from other Smart-Managed devices on the LAN.

Login Timeout: The Login Timeout controls the idle time-out period for security purposes, 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.

Figure 4.19 – System > System Settings

System > IPv6 System Settings

The IPv6 System Settings page allow user to configure the IPv6 system information.

Figure 4.20 – System > IPv6 System Settings

IPv6 System Settings:

Interface Name: Displays the interface name of IPv6.

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

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): 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 **Apply** for the settings to take effect.

System > IPv6 Route Settings

The IPv6 Route Settings page allows user to configure the IPv6 route settings.

Figure 4.21 – System > IPv6 Route Settings

IP Interface: Specify the IP interface which to be created.

Default Gateway: The corresponding IPv6 address for the next hop Gateway address in IPv6 format..

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

Click **Create** to accept the changes made, and click the **Delete** button to remove the entry.

System > 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.

Figure 4.22 – System > 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** for the settings to take effect.

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.

System > Password

The Password page allows user to change the login password of the device.

Figure 4.23 – System > Password

To set the Password, set the following parameters and click **Apply**:

Old Password: If a password was previously configured for this entry, enter it here in order to change it to a new password.

New Password: Enter the new password that you wish to set on the Switch to authenticate users attempting to access Administrator Level privileges on the Switch. The user may set a password of up to 20 characters.

Confirm Password: Confirm the new password entered above. Entering a different password here from the one set in the New Local Enabled field will result in a fail message.

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, effective by clicking **Apply**. Press the **Refresh** button to view the latest information.

Port	Link Status	Speed	MDI/MDIX	Flow Control
01	Link down	Auto	Auto	Disabled
02	Link down	Auto	Auto	Disabled
03	100M Full	Auto	Auto	Disabled
04	Link down	Auto	Auto	Disabled
05	Link down	Auto	Auto	Disabled
06	Link down	Auto	Auto	Disabled
07	Link down	Auto	Auto	Disabled
08	Link down	Auto	Auto	Disabled
09	Link down	Auto	Auto	Disabled
10	Link down	Auto	Auto	Disabled
11	Link down	Auto	Auto	Disabled
12	Link down	Auto	Auto	Disabled
13	Link down	Auto	Auto	Disabled
14	Link down	Auto	Auto	Disabled
15	Link down	Auto	Auto	Disabled
16	Link down	Auto	Auto	Disabled
17	Link down	Auto	Auto	Disabled

Figure 4.24 – System > Port Settings

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



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

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 configurable **MDI/MDIX** function for users. The switches can 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.

Link Status: Reporting **Down** indicates the port is disconnected.

System > Port Description

Port description can be given on this page.

Figure 4.25 – System > Port Description

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

Description: Specify the description of 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.

Figure 4.26 – System > DHCP Auto Configuration

System > DHCP Relay > DHCP Relay Global Settings

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

Figure 4.4.27 – System > DHCP Relay > DHCP Relay Global Settings

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

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

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

DHCP Relay 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 **BOOTP Relay Table** at the bottom of the following window, once the user clicks the **Add** button under the **Apply** heading. The user may add up to four server IPs per IP interface on the Switch. Entries may be deleted by clicking Delete button.

Figure 4.28 – 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.

Figure 4.29 - 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 **Apply** to implement changes made.

System > DHCPv6 Relay Settings

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

DHCPv6 Relay Settings Safeguard

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

00-01-02-03-04-05

Apply

Interface: System

Server IP:

Apply

DHCPv6 Relay Interface Table

Interface	Server Address	Delete
-----------	----------------	--------

Figure 4.30 - 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 **Apply** to implement changes made.

System > 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 remote system log server, then press **Apply** for the changes to take effect.

SysLog Host Settings Safeguard

System Log: Enabled Disabled

Apply

Server IP Address: IPv4 0.0.0.0 IPv6

Severity: All

Facility: Local 0

UDP Port (1-65535): 514

Time Stamp: Enabled

Apply

Figure 4.31 – System > SysLog Host

Server IP Address: Select IPv4 or IPv6 and specifies 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.

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.

The screenshot shows the 'Time Profile Settings' page. It includes a form with the following fields:

- Profile Name:** A text input field.
- Time(HH MM):** Two sets of dropdown menus for Start Time and End Time, each with hour and minute options.
- Weekdays:** A row of checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, and Sat.
- Date:** A checkbox labeled 'Date' followed by 'From Day' and 'To Day' dropdown menus for year, month, and day.

An 'Add' button is located to the right of the form. Below the form, it displays 'Total Entries:0' and a table with the following columns: Profile Name, Start Time, End Time, Weekdays, From Day, To Day, and Delete.

Figure 4.32 – 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.



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

System > Power Saving

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

Power Saving Settings Safeguard

Global Settings
 Cable Length Detection/Link Status Detection Enabled Disabled

Advanced Power Saving Settings
 Type: LED Shut-off State: Disabled
 Time Profile 1: None Time Profile 2: None

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

Summary

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 4.33 – System > Power Saving

Global Settings:

Cable Length Detection/Link Status Detection: Specifies to enable or disable the cable length detection function.

Advanced Power Saving Settings:

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

LED Shut-off - The LED Shut-off gets high priority. If the user select LED Shut-off, the profile function will not take effect. It means the LED can not 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 (PHY) are disabled for all ports, and energy required to power the CPU is minimal.

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

Time Profile 1: Specifies the time profile or None.

Time Profile 2: Specifies the time profile or None.

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

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

System > IEEE802.3az EEE Settings

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

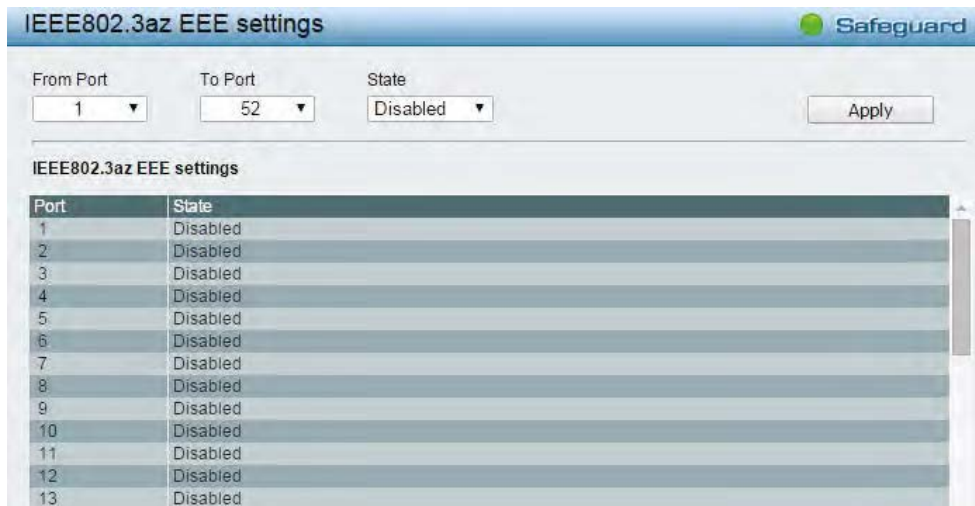


Figure 4.34 – System > IEEE802.3az EEE Settings

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 enabled.

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.

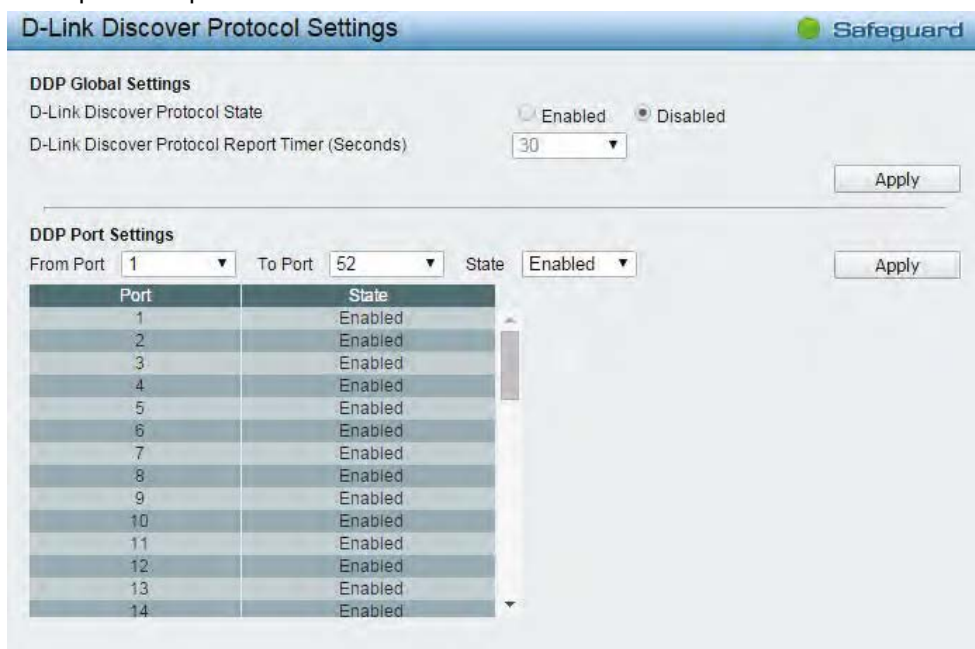


Figure 4.35 – System > D-Link Discover Protocol Settings

D-Link Discover Protocol State: Enable or disable the Discover Protocol state.

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 **Apply** to implement changes made.

VLAN > 802.1Q VLAN (Asymmetric VLAN)

This function is located in the 802.1Q Configuration page. It allows devices in different VLANs to communicate with the servers, firewalls or other shared resources in the shared VLAN. This configuration is accomplished in three steps:

- Enabling Asymmetric VLAN function
- Creating shared VLAN and access VLAN
- Configuring the PVID of access VLAN

Asymmetric VLAN is especially effective when used in a small network where a L3 routing device is absent, or if the resource to be shared is not capable of supporting tagged VLAN (for example, a printer).

The example below is a typical application of Asymmetric VLAN. Servers and firewall are located in shared VLAN (default VLAN), and PCs 1, 2 and 3 are located in different VLAN. Because VLANs remain separate, PCs 1, 2, and 3 cannot communicate with each other; but all of them need to access the servers or the Internet behind the firewall.

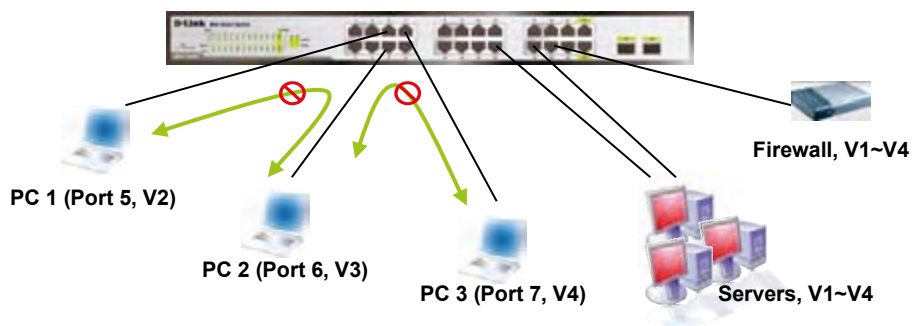


Figure 4.36 – VLAN > 802.1Q VLAN > Asymmetric VLAN Example

1. Enable Asymmetric VLAN

Enable Asymmetric VLAN and click **Apply** button. The overlapping VLAN cannot be configured unless this function is enabled.



Figure 4.37 – VLAN > 802.1Q VLAN

2. Configure the shared VLAN (VLAN 1) and access VLANs (VLAN 2, 3, 4)

In this case, the default VLAN is used as shared VLAN, and the ports that are shared in the network are:

- Ports 15-18 are connected to the server
- Port 20 is connected to the firewall

The group of shared ports needs to be included for all the VLANs. Ports 15-18, 20 already belong to VLAN 1, therefore no changes are needed.

VLAN 2 is configured to include ports 15-18, 20 (shared VLAN ports) and the set of ports to be separated from the other VLANs (for example, port 5). VLAN 3 and 4 are then configured to include shared ports and the set of ports to be separated from the other VLANs (for example, port 6 and 7 respectively). Therefore we have three VLANs that share some common ports, but their original membership ports are still separated from each other (for example, port 5, 6, and 7).

The VLAN settings of this example are:

- VLAN 1: default VLAN 1, including all ports with untagged.
- VLAN 2: Member ports are untagged port 5, 15-18, 20.
- VLAN 3: Member ports are untagged port 6, 15-18, 20.
- VLAN 4: Member ports are untagged port 7, 15-18, 20.

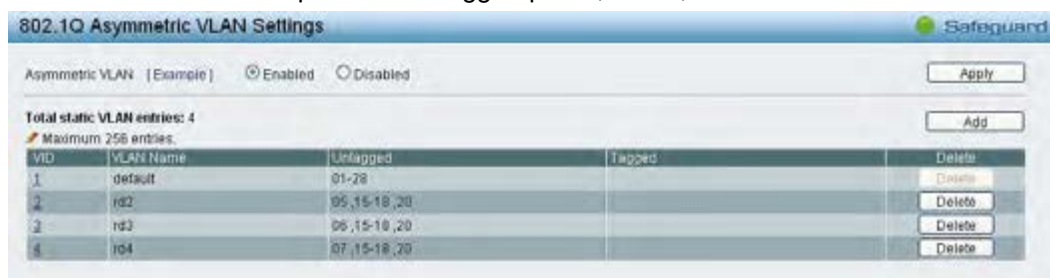


Figure 4.38 – VLAN > 802.1Q VLAN – Create VLANs

VLAN > 802.1Q VLAN PVID

The 802.1Q VLAN PVID setting allows user to configure the PVID for each ports. The purpose of assigning PVID is to make sure the untagged packets will be transmitted correctly. Click **Apply** to implement changes made.



Figure 4.39 – VLAN > 802.1Q VLAN PVID



Note: When Asymmetric VLAN is enabled, IGMP Snooping, Management VLAN, and MAC address table will be reset to default.

VLAN > 802.1Q Management VLAN

The 802.1Q Management VLAN setting allows you to transfer the authority of the switch from the default VLAN to others created by users. This allows managing the whole network more flexible.

By default, the Management VLAN is disabled. You can select any existing VLAN as the management VLAN when this function is enabled. There can only be one management VLAN at a time. Click **Apply** to implement changes made.

Figure 4.40 – VLAN > 802.1Q Management VLAN

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 4.41 – VLAN > Voice VLAN > Voice VLAN Global Setting

Voice VLAN State: 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: Enter a period of time in hours to remove a port from voice VLAN if the port is an automatic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after expiration of voice VLAN aging timer. Selectable range is from 1 to 120 hours and default is 1 hour.

Click **Apply** to implement changes made.

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

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

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

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

User defined OUI: You can manually create a Telephony OUI with a description. The maximum number of user defined OUIs is 10. It will occupy one ACL rule when selecting user defined OUI by default, and to configure one user-defined OUI will take extra one ACL rule. System will auto generate an ACL profile (Profile ID: 51) for all the Voice VLAN rules.

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



Note: The default OUI for 3COM, Cisco, Veritel, Pingtel, Siemens, NEC/Philips, Huawei3COM, and Avaya is not common for all of their VoIP devices.

VLAN > Voice VLAN > Voice VLAN Port Setting

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.

Port	Auto Detection	Tagged / Untagged	Current State	Status
01	Disabled	Untagged	None	None
02	Disabled	Untagged	None	None
03	Disabled	Untagged	None	None
04	Disabled	Untagged	None	None
05	Disabled	Untagged	None	None
06	Disabled	Untagged	None	None
07	Disabled	Untagged	None	None
08	Disabled	Untagged	None	None
09	Disabled	Untagged	None	None
10	Disabled	Untagged	None	None
11	Disabled	Untagged	None	None
12	Disabled	Untagged	None	None
13	Disabled	Untagged	None	None
14	Disabled	Untagged	None	None
15	Disabled	Untagged	None	None
16	Disabled	Untagged	None	None
17	Disabled	Untagged	None	None

Figure 4.42 – VLAN > Voice VLAN > Voice VLAN Port Setting

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.

Figure 4.43 – 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

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.

Figure 4.44 – VLAN > Auto Surveillance VLAN Settings

Auto Surveillance VLAN Global Settings:

Auto Surveillance VLAN State: Select enable or disable Auto Surveillance VLAN. The default is *Disabled*.

VLAN ID: By default, the VLAN ID 4094 was created as Auto Surveillance VLAN and all ports are member ports. You also can create another Auto Surveillance VLAN by selecting a VLAN ID that you have created a VLAN from the 802.1Q VLAN page. The member port you configured in 802.1Q VLAN setting page will be the static member port of Auto Surveillance VLAN.

Priority: The 802.1p priority levels of the traffic in the Auto Surveillance VLAN. The possible values are 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.

Click **Apply** to implement changes of Auto Surveillance VLAN global settings.

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 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: Specifies the description for the component type.

MAC/OUI: You can manually create an MAC or OUI address for the surveillance component. The maximum number of user defined MAC address is 5. System will auto generate an ACL profile (Profile ID: 56) for all the Auto Surveillance VLAN rules.

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

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 9216 bytes (tagged). Default is disabled, Select **Enabled** then click **Apply** to turn on the jumbo frame support.



Figure 4.45 – 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.

Figure 4.46 – L2 Functions > Port Mirroring

Select **Enabled** and specifies the **Target port**.

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 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 a time. You may enable or disable this function using the pull-down menu.

Port	State	Loop Status
01	Disabled	Normal
02	Disabled	Normal
03	Disabled	Normal
04	Disabled	Normal
05	Disabled	Normal
06	Disabled	Normal
07	Disabled	Normal
08	Disabled	Normal
09	Disabled	Normal
10	Disabled	Normal
11	Disabled	Normal

Figure 4.47 – L2 Functions > Loopback Detection

Loopback Detection State: Specifies 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 effected 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.

Click **Apply** to implement changes made.

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 **Apply** to implement changes made or click **Refresh** to renew the page.

L2 Functions > MAC Address Table > Static MAC

This feature provides two distinct functions. The **Disable Auto 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 Off (disabled).

Figure 4.48 – L2 Functions > MAC Address Table > Static Mac

To initiate the removal of auto-learning for any of the uplink ports, click **On** to enable this feature, and then select the port(s) for auto learning to be disabled.

The **Static MAC Address Setting** table displays the static MAC addresses connected, as well as the VID. Click **Add** to add a new MAC address, you also need to select the assigned Port number, enter both the Mac Address and VID and Click **Apply**. Click **Delete** to remove one entry or click **Delete all** to clear the list. You can also copy a learned MAC address from **Dynamic Forwarding Table** (please refer to **L2 Functions > MAC Address Table > Dynamic Forwarding Table** for details).

By disabling Auto Learning capability and specify 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 to Static MAC** checkbox, and then click **Apply** associated with the identified address.



Figure 4.49 – Security > MAC Address Table > Dynamic Forwarding Table

L2 Functions > Spanning Tree > STP Global Settings

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

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.

After enabling STP, setting the STP Global Setting includes the following options:

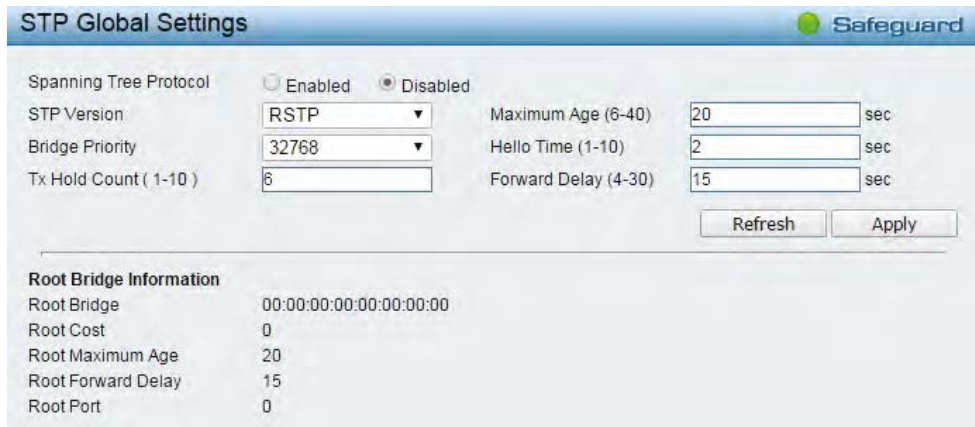


Figure 4.50 – L2 Functions > Spanning Tree > STP Global Settings

STP Version: You can choose RSTP or STP Compatible. The default setting is RSTP.

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 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 **Apply** for the settings to take effect. 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 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	Port Status
01								
02								
03								
04								
05								
06								
07								
08								
09								
10								
11								

Figure 4.51 – 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: Specify the priority of each port. Selectable range is from 0 to 240, and the default setting is 128. The lower the number, the greater the probability the port will be chosen as a root port.

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

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

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

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

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

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 can be consisted of 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.

The screenshot shows the 'Port Trunking' configuration page. At the top, there's a 'Safeguard' logo. Below it, 'Link Aggregation' is set to 'Disabled' with an 'Apply' button. Under 'Link Aggregation Settings', 'Group' is '01' and 'Type' is 'LACP', also with an 'Apply' button. A grid of 52 ports (01-52) is displayed, each with a checkbox. A note indicates 'Maximum 8 ports in static group and 8 ports in LACP group.' At the bottom, a 'Trunking list' table is visible with columns: Group, Type, Ports, and Delete.

Figure 4.52 – 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

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)

Figure 4.53 –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: Specify the administrative LACP timeout. The possible field values are:

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

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

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

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 settings of IGMP snooping is set by each VLAN individually.

IGMP Snooping Configuration Safeguard

IGMP Snooping Global Settings

IGMP Snooping Enabled Disabled Report to all ports

Host Timeout (130-153025) sec Router Timeout (60-600) sec

Robustness Variable (2-255) sec Last Member Query Interval (1-25) sec

Query Interval (60-600) sec Max Response Time (10-25) sec

When Querier state is enabled, the Host Timeout is calculated as the formula :
 (Host Timeout = Robustness Variable * Query Interval + Max Response Time) Apply

IGMP Snooping VLAN Settings

VLAN ID	VLAN Name	State	Querier State	Fast Leave	Router Ports	Multicast Entries
1		Enabled	Disabled	Disabled		View
2	2	Enabled	Disabled	Disabled		View
3	3	Enabled	Disabled	Disabled		View

Page Back Next

Figure 4.54 – L2 Functions > Multicast > IGMP Snooping Configuration

By default, IGMP is disabled. If enabled, the IGMP Global Settings will need to be entered, It is recommended to keep Report to all ports enable to ensure the functionality of SmartConsole Utility.

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 no Query control messages are received for 'Router Port Purge Interval' time, the learned router port entry will be purged. Default is 125 seconds.

Last Member Query Interval (1-25 sec): The Last Member Query Interval is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages. This value may be adjusted to modify the "leave latency" of the network. A reduced value results in reduced time to detect the loss of the last member of a group. Default is 1 second.

Max Response Time (10-25 sec): The Max Response Time specifies the maximum allowed time before sending a responding report message. Adjusting this setting effects the "leave latency", or the time between the moment the last host leaves a group and when the multicast server is notified that there are no more members. It also allows adjustments for controlling the frequency of IGMP traffic on a subnet. Default is 10 seconds.

To enable IGMP snooping for a given VLAN, select enable and click on the **Apply** button. Then press the **Edit** button under **Router Port Setting**, 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.

IGMP Snooping VLAN Settings Safeguard

VLAN ID: 1
 VLAN Name:
 State: Enabled ▾
 Querier State: Disabled ▾
 Fast Leave: Disabled ▾ 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
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

Back Apply

Figure 4.55 – L2 Functions > Multicast > IGMP Router port Settings

State: Specify 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: Specify the Fast Leave feature to be enabled or disabled.

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

Multicast Entry Table Safeguard

Back Delete All

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	16	Delete

Figure 4.56 – 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

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 settings of IGMP snooping is set by each VLAN individually.

VLAN ID	VLAN Name	State	Querier State	Fast Leave	Router Ports	Multicast Entries
1		Enabled	Disabled	Disabled		View
2	2	Enabled	Disabled	Disabled		View
3	3	Enabled	Disabled	Disabled		View

Figure 4.57 – L2 Functions > Multicast > MLD Snooping

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**.

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"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
None	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input 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"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
None	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

VID	MAC Address	Member Ports	Delete
Total Static Entries: 0			

Figure 4.58 – 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 Table	
Forwarding List	1-52
Filtering List	1-52

Figure 4.59 – 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 un-register group will be filtered.

Click **Apply** to make the change effective.

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.

Figure 4.60 – L2 Functions > SNTP > Time Settings

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

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

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

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

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

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

SNTP Second Server: Select IPv4 or IPv6 then specify the IP address of 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.

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

Manually Time Settings: Users input the system **Date** and **Time** manually.

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

Click **Apply** to implement changes made.

L2 Functions > SNMP > TimeZone Settings

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

Figure 4.61 – L2 Functions > SNMP > TimeZone Settings

Daylight Saving Time State: Use this drop-down menu to 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 from 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 and days of week DST will start on, each year.

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

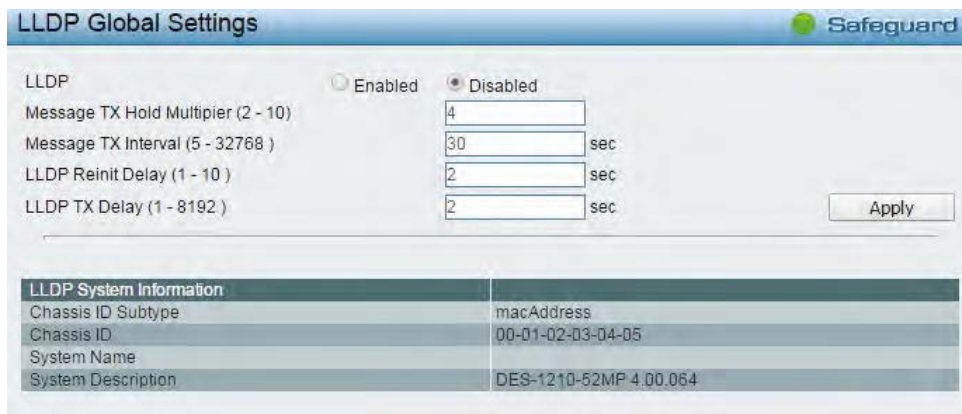
To: Month/Day: Enter the month and date DST will end on, each year.

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

Click **Apply** to implement changes made.

L2 Functions > LLDP > LLDP Global Settings

LLDP (Link Layer Discovery Protocol) supports an IEEE 802.1AB standard-based method for switches. This function allows the switches to advertise themselves to the neighboring devices and learn about the neighboring LLDP devices. The Switch will store that information in the Management Information Base (MIB); SNMP utilities can learn about the network topology by getting the MIB information from each LLDP device.



LLDP Global Settings Safeguard

LLDP Enabled Disabled

Message TX Hold Multiplier (2 - 10)

Message TX Interval (5 - 32768) sec

LLDP Reinit Delay (1 - 10) sec

LLDP TX Delay (1 - 8192) sec

LLDP System Information	
Chassis ID Subtype	macAddress
Chassis ID	00-01-02-03-04-05
System Name	
System Description	DES-1210-52MP 4.00.064

Figure 4.62 – L2 Functions > LLDP > LLDP Global Settings

LLDP: Specify the LLDP state to be enabled or disabled. By default, the LLDP state is Disabled.

Message TX Hold Multiplier (2-10): Set the **Time-to-Live** for the LLDP advertisements transmitted. If the **Time-to-Live** of LLDP advertisements expire, the advertised data will be deleted from the neighboring Switch's MIB. The default value is 4 hops.

Message TX Interval (5-32768): Set the time interval to transmit the LLDP advertisement. The default value is 30 seconds.

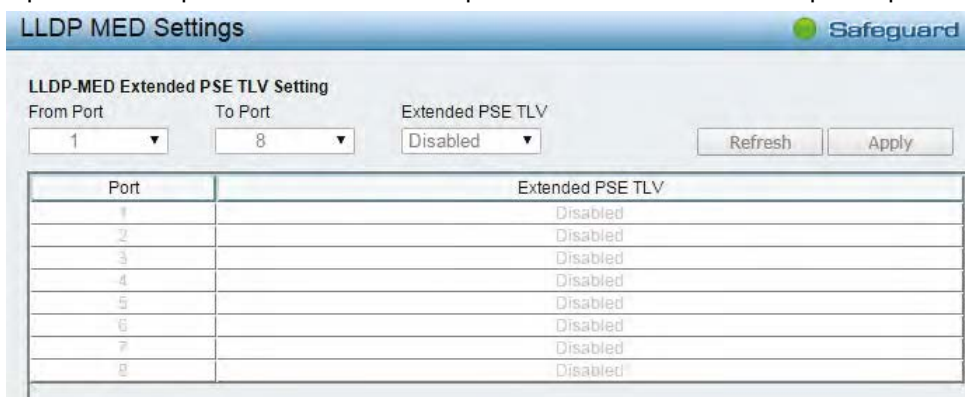
LLDP Reinit Delay(1-10): Enter a time delay for the LLDP port. This LLDP port will wait for a specific interval before it re-initializes. The default is 2 seconds.

LLDP TX Delay(1-8192): Configure the minimum time delay interval for any LLDP port which transmits successive LLDP advertisements due to changes in the LLDP MIB content. The default value is 2 seconds.

Click **Apply** to implement changes made.

L2 Functions > LLDP > LLDP-MED Settings

By selecting a range of ports (**From Port** and **To Port**), the power PSE TLV type can be enabled for all selected ports to indicate the power source equipment (PSE) switch to transmit high power (15.4 to 30 Watts) to the pre-standard of 802.3at power devices via LLDP MDI TLV. Through this feature, the PSE can provide precise output power to the pre-standard of 802.3at power devices and achieve optimal power management.



LLDP MED Settings Safeguard

LLDP-MED Extended PSE TLV Setting

From Port To Port Extended PSE TLV

Port	Extended PSE TLV
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled

Figure 4.63 – 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.

Basic LLDP Port Settings Safeguard

From Port: 1 To Port: 52 Notification State: Disabled Admin Status: TX_Only Port Description: Disabled System Name: Disabled System Description: Disabled System Capabilities: Disabled

Refresh Apply

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
12	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
13	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
14	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled
15	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled

Figure 4.64 – 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 **Apply** 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.

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)

Figure 4.65 – L2 Functions > LLDP > 802.1 Extension TLV

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 **Apply** 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

Figure 4.66 – 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 **Apply** 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.

From Port	To Port	Address Type	Address	Port State
01	52	IPv4		Disabled

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

Figure 4.67 – 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: Specify the LLDP address type on the port. The value is always IPv4.

Address: Specify the address.

Port State: Specify whether the Port State is enabled in the port. The possible field values are:

Enabled – Enables the port state configured on the port.

Disabled – Disables the port state configured on the port.

Click **Apply** to 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 4.68 – L2 Functions > LLDP > LLDP Management Address Table

Management Address: Specifies IPv4 or IPv6 then enter the IP address. Click **Search** and the table will update and display the values required.

Subtype: Displays the managed address subtype. For example, IPv4 or IPv6.

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.



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 4.69 – 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 Normal** or **View Detailed** to display more information.

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.

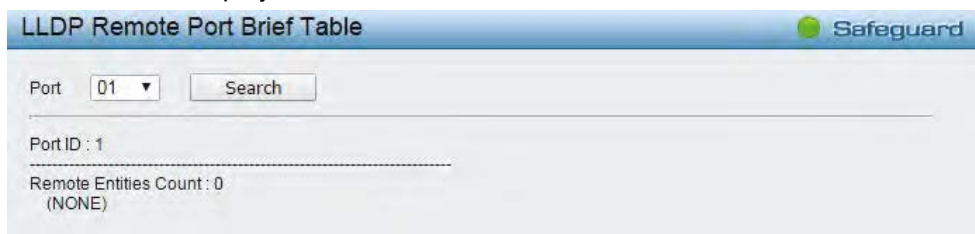


Figure 4.70 – L2 Functions > LLDP > LLDP Remote Port Table

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



Figure 4.71 – L2 Functions > LLDP > LLDP Remote Port Information(Normal)

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



Figure 4.72 – L2 Functions > LLDP > LLDP Remote Port Table(Detailed)

L2 Functions > LLDP > LLDP Statistics

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

LLDP Statistics System

Last Change Time	0
Number of Table Insert	0
Number of Table Delete	0
Number of Table Drop	0
Number of Table Age Out	0

LLDP Port Statistics

Refresh Clear

Port	TxPort Frames	RxPortFrames Discarded	RxPort FramesErrors	RxPort Frames	RxPortTLVs Discarded	RxPortTLVs 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	0	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

Figure 4.73 – 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 is also displays the time elapsed since last change was detected.

Number of Table Insert – Displays the number of new entries inserted since switch reboot.

Number of Table Delete – Displays the number of new entries deleted since switch reboot.

Number of Table Drop – Displays the number of LLDP frames dropped due to that the table was full.

Number of Table Age Out – Displays the number of entries deleted due to Time-To-Live expiring.

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

TxPort FramesTotal – Displays the total number of LLDP frames transmitted on the port.

RxPort FramesDiscarded – Displays the total discarded frame number of LLDP frames received on the port.

RxPort FramesErrors – Displays the Error frame number of LLDP frames received on the port.

RxPort Frames – Displays the total number of LLDP frames received on the port.

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

RxPortTLVsUnrecognized – Displays the number of well-formed TLVs, but with an known type value.

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

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

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

Figure 4.74 – 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.

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



NOTE: For DES-1210-52, the TX rate for Gigabit ports can only be configured in multiples of 1850kbps. If any other value is used, the system automatically rounds it down to the lower multiple of 1850.

For DES-1210-28, the TX rate for Gigabit ports can only be configured in multiples of 63kbps. If any other value is used, the system automatically rounds it down to the lower multiple of 63.

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.

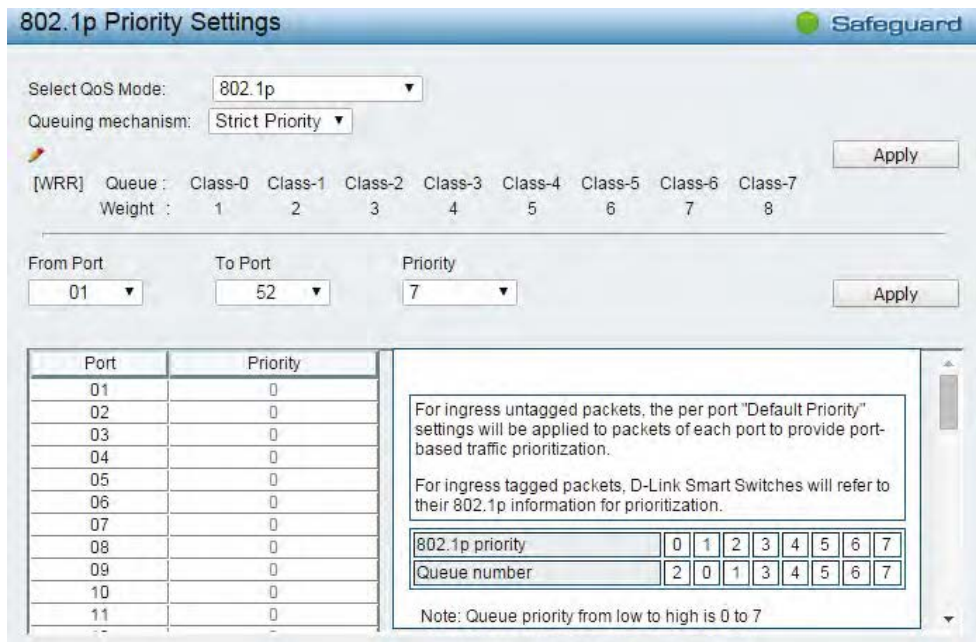


Figure 4.75 – QoS > 802.1p Default Priority

By selecting the DSCP priority, the web pages will changes as seen below:

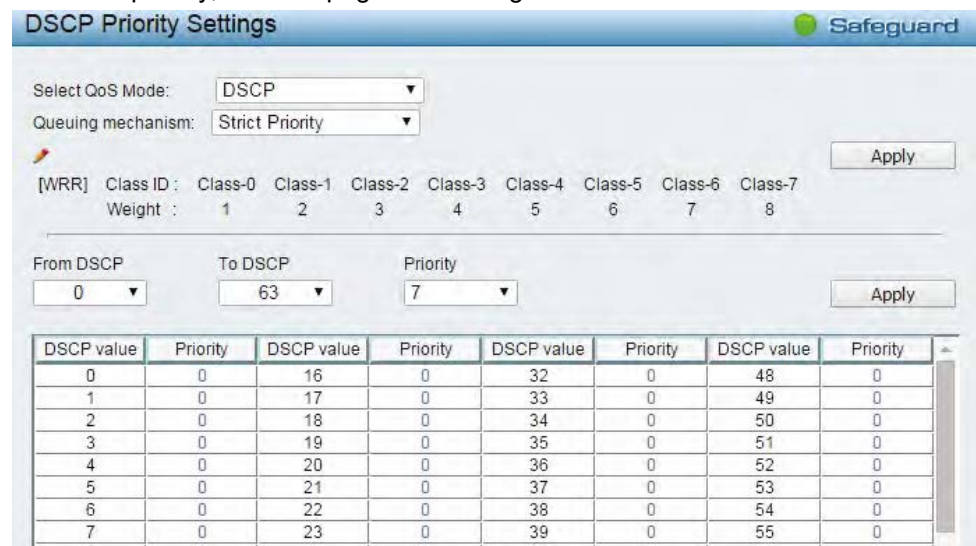


Figure 4.76 – QoS > DSCP Priority Settings

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.

By selecting the ToS priority, the web pages will changes as seen below:

ToS Priority Settings Safeguard

Select QoS Mode:
 Queuing mechanism:

[WRR] Class ID : Class-0 Class-1 Class-2 Class-3 Class-4 Class-5 Class-6 Class-7
 Weight : 1 2 3 4 5 6 7 8

From ToS: To ToS: Priority:

ToS	Priority
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0

Figure 4.77 – QoS > ToS Priority Settings

In ToS mode, you can configure the global default priority value by using **From ToS / To ToS**.

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.

Trusted Host Settings Safeguard

Trusted Host: Enabled Disabled

IPv4 Address: Netmask:

IPv6 Address: Prefix:

Please add your local host IP address first to make it trusted. Otherwise, the connection will be stopped.

Trusted Host Table
 Maximum 10 entries.

ID	IP Address	Netmask/Prefix	Delete
----	------------	----------------	--------

Figure 4.78 Security > Trusted Host

Trusted Host: Specify 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 cannot be changed once the port is enabled. Using the drop-down menu, change **Admin State** to **Enabled**, input the **Max Learning Address**, and then click **Apply** to confirm the setting.

Port Security Safeguard

From Port: 01 To Port: 52 Admin State: Disabled Max Learning Address (0-64): 0 [Apply]

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

Figure 4.79 – 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.

Traffic Segmentation Settings Safeguard

Forwarding Port Settings: Enabled Disabled [Apply]

From Port: All [Select All] [Clear] [Apply]

To 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
To 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

Port	Forwarding Port
1	1-52
2	1-52
3	1-52
4	1-52
5	1-52

Figure 4.80 – Security > Traffic Segmentation

Click **Apply** to enable or disable this feature.

To configure traffic segmentation specify a port or All ports from the switch, using the **From Port** pull-down menu and select To Port then click **Apply** to enter the settings into the Switch's **Forwarding Port** 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 Smart Managed Switch from being interrupted by malicious viruses or worm attacks. This option is enabled by default.



Figure 4.81 – 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.

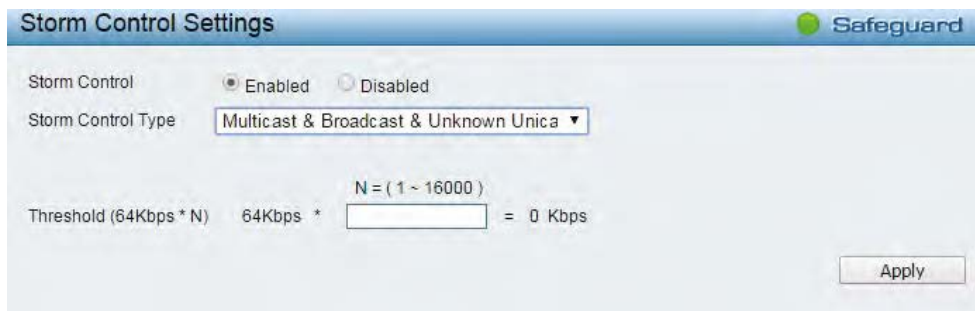


Figure 4.82 – Security > Storm Control

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

Threshold (64Kbps * N): If storm control is enabled (default is disabled), the threshold is from of 64 ~ 1,024,000 Kbit per second, with steps (N) of 64Kbps. N can be from 1 to 16000.

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

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.



Figure 4.83 – 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 you 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. Select ports and then click **Apply** to enable the function.

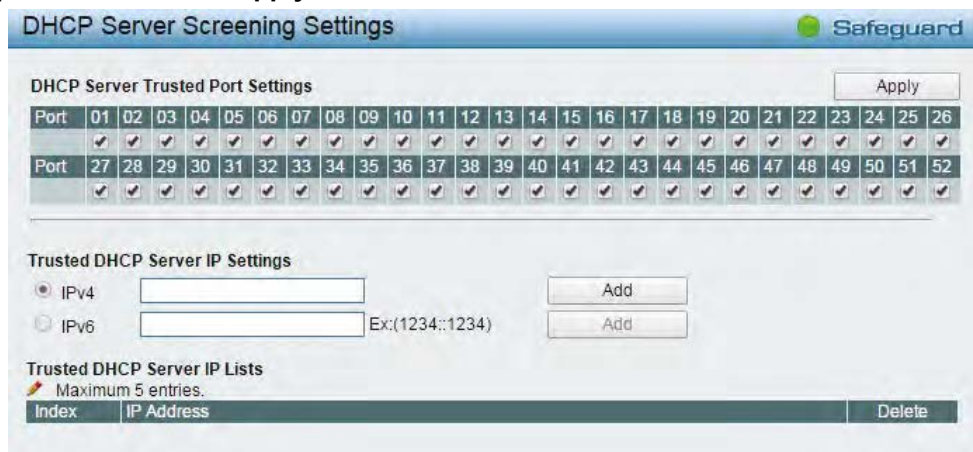


Figure 4.84 – Security > DHCP Server Screening

Trusted DHCP Server IP Settings: Select IPv4 or IPv6 and specify the IP address then click Apply to create Trusted DHCP Server.

Security > SSL Settings

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

This page allows you to configure the SSL global state 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**.

Figure 4.85 – Security > SSL Settings



NOTE: When SSL is enabled, it will take longer time to open a web page due to encryption. After saving configuration, please wait around 10 seconds for the system summary page.

Security > DoS Prevention Settings

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

DoS Type	State
Land Attack	Disabled
Blat Attack	Disabled
Tcp Null Scan	Disabled
Tcp Xmascan	Disabled
Tcp Synfin	Disabled
Tcp Syn Srcport less 1024	Disabled

Figure 4.86 – Security > DoS Prevention Settings

State: Specify the state to be enabled or disabled. Click **Apply** 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.

Figure 4.87 – 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*.

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.

Figure 4.88 – 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 **Apply** 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.



Figure 4.89 – 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 IP: Enter the corresponding IP 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 the access to a switch to a number of authorized users. Authorized clients can access a switch's port by either checking the pair of IP-MAC address with the pre-configured database or if DHCP snooping has been enabled in which case the switch will automatically learn the IP/MAC pairs by snooping DHCP packets and saving them to the Smart Binding white list. If an unauthorized client tries to access a Smart Binding enabled port, the system will block the access by dropping the packet. The IP network layer uses IPv4 address. The maximum number of IPv4 entries is 512 by ARP inspection and 128 by ARP+IP inspection.

Users can enable or disable the **Packet Inspection** and **DHCP Snooping** on the Switch.

Smart Binding Settings Safeguard

From Port: 01 To Port: 52 State: Disabled

Packet Inspection: ARP Inspection DHCP Snooping: Disabled

IMPB Setting

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
14	Disabled	Disabled	Disabled
15	Disabled	Disabled	Disabled
16	Disabled	Disabled	Disabled

Figure 4.90 – 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 Smart 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: There are two options for IP packets inspection.

ARP Inspection: When the ARP inspection function is enabled, the legal ARP packets are forwarded, while the illegal packets are dropped.

ARP+IP Inspection: When the ARP+IP inspection function is enabled, all IP packets are checked. The legal IP packets are forwarded, while the illegal IP packets are dropped.

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.

Click **Apply** to make configurations make effects.

Security > Smart Binding > Smart Binding

The Smart Binding Settings page allows the user to create Static Smart Binding entries on the Switch.

Smart Binding Safeguard

Manual Binding

IP Address: MAC Address: Port:

Auto Scan

Enter a range of IP address to scan all devices in the network.

IP Address From: To:

VLAN	IP Address	MAC Address	Port	Binding
------	------------	-------------	------	---------

Figure 4.91 – Security > Smart Binding > Smart Binding

The Manual Binding Settings contains the following fields:

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.

Port: Specify the switch ports for which to configure this IP-MAC binding entry (IP Address + MAC Address). Click **Add** to add a new entry.

Auto Scan: Specifies to scan connected devices in a range of IP address.

IP Address From/To: Specifies the range of IP Address to scan all devices in the network.

Click **Scan** and the search results will be listed in below table.

Binding: check the box to select desired binding devices.

Select All: to check the boxes of Binding for all found devices.

Clear All: to cancel the box of Binding.

Apply: click **Apply** to set Smart Binding entries.

Security > Smart Binding > White List

The White List displays the authorized clients set by Manual Binding Settings or Auto Scan Settings.

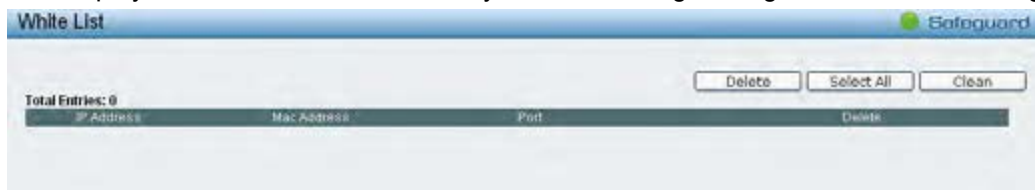


Figure 4.92 – Security > Smart Binding > White List

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 displays the unauthorized clients that have been blocked by the restrictions of Manual Binding Settings or Auto Scan Settings.



Figure 4.93 – Security > Smart Binding > Black List

By giving conditions, desired devices information can be screened out below then click **Find** to search for a list of the entry:

VID: Enter the VLAN ID number of the device.

IP Address: Enter the IP Address of the device.

MAC Address: Enter the MAC Address of the device.

Port: Enter the port number which the device connects.

Check a box of **Delete** column to release an entry from the forbidden list then click **Apply** to delete an entry from the list.

Click **Select All** to select all entries, or click **Clean** to select none of the entries.

AAA > RADIUS Server

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

Authentication RADIUS Server Safeguard

Index:

IP Address: IPv4 IPv6

Authentication Port (1-65535):

Accounting Port (1-65535):

Timeout (1-255): sec

Retransmit (1-255): times

Key: For key, the maximum number of character is 32.

Confirm Key:

RADIUS Server List

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

Figure 4.94 – AAA > RADIUS Server

Index: Choose the desired RADIUS server to configure: 1, 2 or 3.

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

Authentication Port (1 - 65535): Set the RADIUS authentic server(s) UDP port. The default port is 1812.

Accounting Port (1 - 65535): Set the RADIUS account server(s) UDP port. The default port is 1813.

Timeout (1 – 255 sec): This field will set the time the Switch will wait for a response of authentication from the user. The user may set a time between 1 and 255 seconds. The default setting is 5 seconds.

Retransmit (1 – 255 times): This command will configure the maximum number of times the Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the Switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet and web users will be disconnected from the Switch. The user may set the number of attempts from 1 to 255. The default setting is 2.

Key: Set the key the same as that of the RADIUS server.

Confirm Key: Confirm the shared key is the same as that of the RADIUS server.

Click **Apply** to implement configuration changes.

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.

802.1X Global Settings Safeguard

Authentication State: Enabled Disabled

Forward EAPOL PDU: Enabled Disabled

Authentication Protocol:

Figure 4.95 – AAA > 802.1x Global Settings

Authentication State: Specify 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 **Apply** to implement configuration changes.

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.

Port	AdmDir	Oper CntDir	Port Control	TxPeriod	Quiet Period	Supp-Timeout	Server-Timeout	MaxReq	ReAuth Period	ReAuth	Capability	Port Status	Session Time	Use
1	Both	Both	ForceAuthorized	30	60	30	30	2	3600	Disabled	None	Unauthorized	0	...
2	Both	Both	ForceAuthorized	30	60	30	30	2	3600	Enabled	None	Unauthorized	0	...
3	Both	Both	ForceAuthorized	30	60	30	30	2	3600	Disabled	None	Unauthorized	0	...
4	Both	Both	ForceAuthorized	30	60	30	30	2	3600	Disabled	None	Unauthorized	0	...
5	Both	Both	ForceAuthorized	30	60	30	30	2	3600	Enabled	None	Unauthorized	0	...
6	Both	Both	ForceAuthorized	30	60	30	30	2	3600	Disabled	None	Unauthorized	0	...
7	Both	Both	ForceAuthorized	30	60	30	30	2	3600	Disabled	None	Unauthorized	0	...
8	Both	Both	ForceAuthorized	30	60	30	30	2	3600	Enabled	None	Unauthorized	0	...
9	Both	Both	ForceAuthorized	30	60	30	30	2	3600	Disabled	None	Unauthorized	0	...
10	Both	Both	ForceAuthorized	30	60	30	30	2	3600	Enabled	None	Unauthorized	0	...

Figure 4.96 – 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 – Specify the Authenticator settings to be applied on a per-port basis.

None – Disable 802.1X functions on the port.

SuppTimeout (1 – 65535 sec): This value determines timeout conditions in the exchanges between the Authenticator and the client. Default is 30 seconds.

MaxReq (1 – 10): This parameter specifies the maximum number of times that the switch retransmits an EAP request (md-5challenge) to the client before it times out the authentication session. Default is 2 times.

ReAuthPeriod (1 – 65535 sec): A constant that defines a nonzero number of seconds between periodic reauthentication of the client. The default setting is 3600 seconds.

Port Control: This allows user to control the port authorization state.

Select **ForceAuthorized** to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client.

If **ForceUnauthorized** is selected, the port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. The Switch cannot provide authentication services to the client through the interface.

If **Auto** is selected, it will enable 802.1X and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server.

The default setting is *Auto*.

Direction: Sets the administrative-controlled direction on the port. The possible field values are:

Both – Specify the control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field.

In – Disables the support in the present firmware release.

Click **Apply** to implement configuration changes.

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.

User Name	Password	Delete
Total Entries: 0		

Figure 4.97 - AAA > 802.1X > 802.1X User

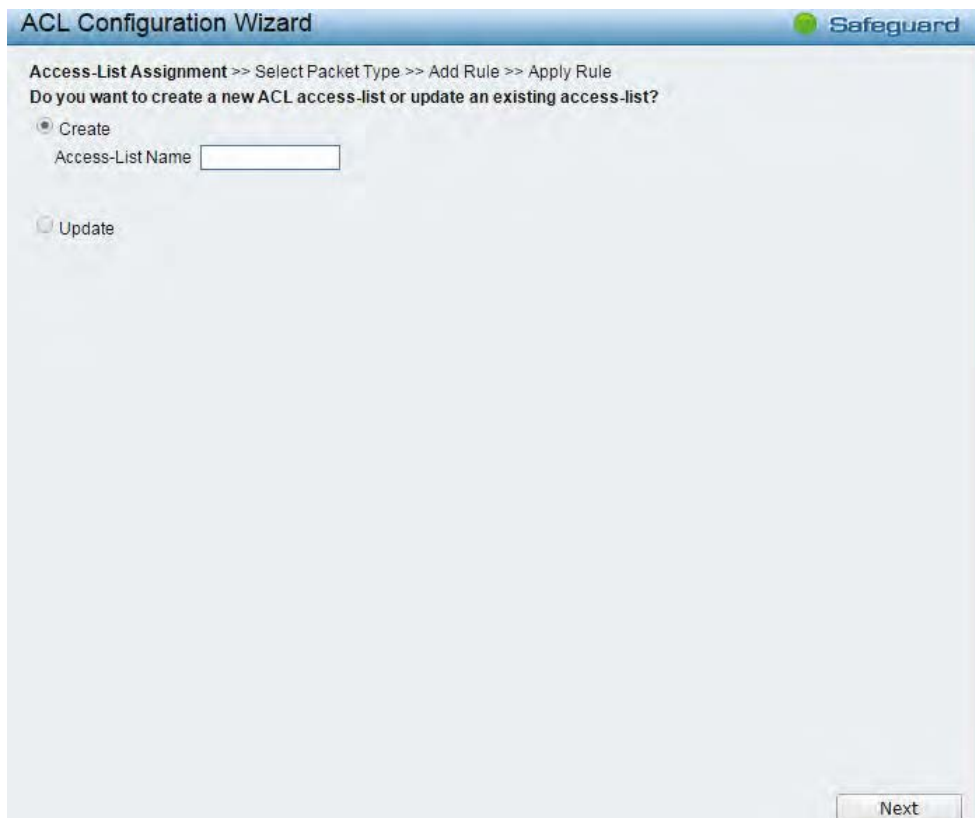
Click **Add** to add a new 802.1X user.

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 ingress ACL profiles and 1280 ingress ACL rules.

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

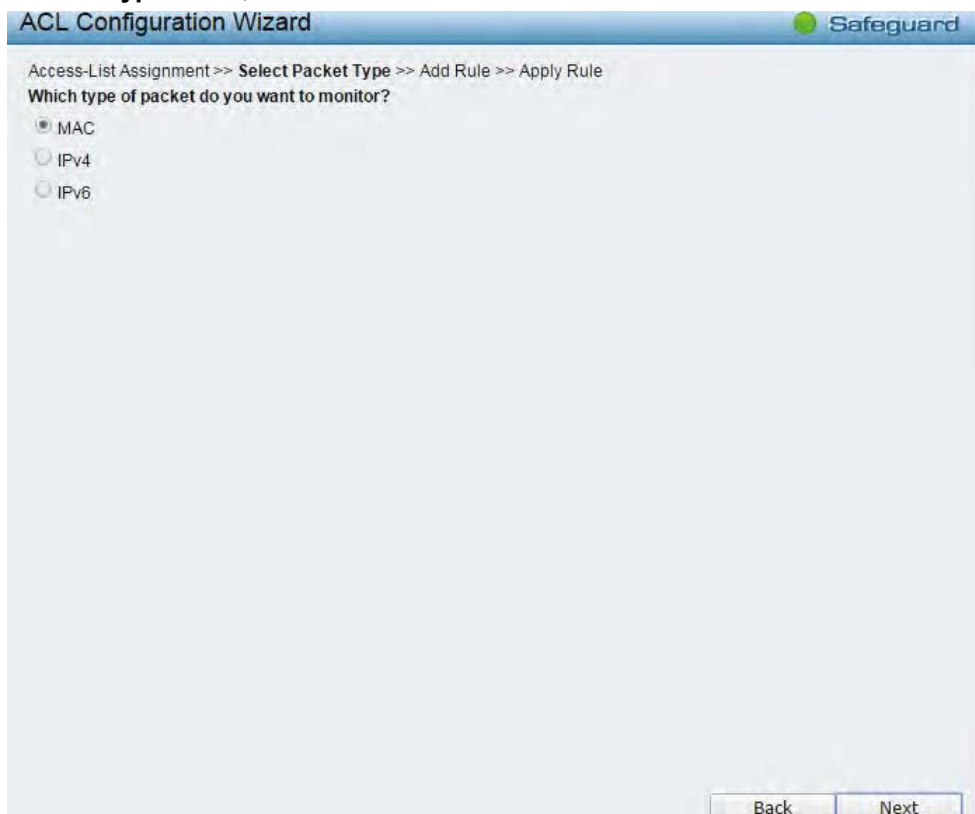


The screenshot shows the 'ACL Configuration Wizard' window with the 'Safeguard' logo in the top right corner. The breadcrumb trail is 'Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Rule'. The main question is 'Do you want to create a new ACL access-list or update an existing access-list?'. There are two radio button options: 'Create' (which is selected) and 'Update'. Below the 'Create' option is a text input field labeled 'Access-List Name'. A 'Next' button is located at the bottom right of the window.

Figure 4.98 - 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**.



The screenshot shows the 'ACL Configuration Wizard' window with the 'Safeguard' logo in the top right corner. The breadcrumb trail is 'Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Rule'. The main question is 'Which type of packet do you want to monitor?'. There are three radio button options: 'MAC' (which is selected), 'IPv4', and 'IPv6'. At the bottom of the window, there are 'Back' and 'Next' buttons.

Figure 4.99 - 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 4.100 – Add Access Rule - MAC

Assign sequence number:

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

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

Assign Rule Criteria: Specify 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): Specify 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: Specify the ACL forwarding action matching the rule criteria. **Permit** forwards packets if all other ACL criteria are met. **Deny** drops packets if all other ACL criteria is met.

Priority (0-7): Specify 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 Rule: Select **IPv4** with **ICMP** click **Next** button. The updates to show the follows:

Figure 4.101 - Add Access Rule – IPv4 ICMP

Assign sequence number:

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

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

Assign Rule Criteria: Specify the IPv4 ACL settings.

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

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

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

IPv4 Address: Specify 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 is added.

To define the IPv4 ACL IGMP Rule: Select **IPv4 ACL** with **IGMP** and click **Next** button. The updates to show the follows:

The screenshot shows the 'ACL Configuration Wizard' window with the 'Safeguard' logo in the top right. The progress bar indicates the current step: 'Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Rule'. Below the progress bar, it says 'Please assign a sequence number to create a new rule.' There are two radio buttons: 'Sequence No. (1-65535)' with an empty text box, and 'Auto Assign' which is selected. Under 'Assign rule criteria', there are four tabs: 'L2 Header', 'TOS', 'IPv4 Address', and 'Protocol'. The 'Protocol' tab is active. In this tab, the 'ToS' checkbox is checked. Below it are three radio buttons: 'ToS (0-7)', 'DSCP (0-63)', and 'Protocol'. The 'Protocol' radio button is selected. Under 'IPv4 Address', there are two rows: 'Source' and 'Destination'. Each row has a 'Specify' dropdown menu, an 'Address' text box, and a 'Mask' text box. Under 'Protocol', the 'Protocol Type' dropdown is set to 'IGMP'. Below it are several text boxes for 'Protocol ID (0-255)', 'Source Port', 'Source Port Mask', 'Destination Port', 'Destination Port Mask', 'ICMP Type (0-255)', 'Code (0-255)', and 'IGMP (0-255)'. The 'Action' dropdown is set to 'Permit'. At the bottom, there are two checkboxes: 'Priority (0-7)' and 'Replace Priority', both of which are unchecked.

Figure 4.102 - 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** with **TCP** and click **Next** button. The updates to show the follows:

The screenshot shows the 'ACL Configuration Wizard' interface with the 'Safeguard' logo in the top right corner. The breadcrumb trail is 'Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Rule'. Below this, it says 'Please assign a sequence number to create a new rule.' There are two radio buttons: 'Sequence No. (1-65535)' (unselected) and 'Auto Assign' (selected). Under 'Assign rule criteria', there are four tabs: 'L2 Header', 'TOS', 'IPv4 Address', and 'Protocol'. The 'TOS' tab is active. It contains several options: 'ToS' (checked), 'ToS (0-7)' (unselected), and 'DSCP (0-63)' (unselected). Below these are two input fields. The 'IPv4 Address' section has 'Source' and 'Destination' options, each with a 'Specify' dropdown, 'Address' input, and 'Mask' input. The 'Protocol' section has 'Protocol' (checked), 'Protocol Type' (dropdown set to 'TCP'), 'Protocol ID (0-255)' (input), 'Source Port' (input) and 'Source Port Mask' (input), 'Destination Port' (input) and 'Destination Port Mask' (input), 'ICMP Type (0-255)' (input) and 'Code (0-255)' (input), and 'IGMP (0-255)' (input). The 'Action' dropdown is set to 'Permit'. At the bottom, there are 'Priority (0-7)' (input) and 'Replace Priority' (checkbox) options. 'Back' and 'Next' buttons are at the bottom right.

Figure 4.103 - 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** with **UDP** and click **Next** button. The updates to show the follows:

ACL Configuration Wizard Safeguard

Access-List Assignment >> Select Packet Type >> **Add Rule** >> Apply Rule

Please assign a sequence number to create a new rule.

Sequence No. (1-65535) Auto Assign

Assign rule criteria

L2 Header TOS IPv4 Address Protocol

ToS

ToS (0-7)

DSCP (0-63)

IPv4 Address

Source Specify Address Mask

Destination Specify Address Mask

Protocol

Protocol Type

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

Priority (0-7)

Replace Priority

Figure 4.104 - 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.



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:

ACL Configuration Wizard Safeguard

Access-List Assignment >> Select Packet Type >> **Add Rule** >> Apply Rule
 Please assign a sequence number to create a new rule.

Sequence No. (1-65535) Auto Assign

Assign rule criteria

L2 Header Traffic Class Next Header IPv6 Address

Traffic Class
 IPv6 Class (0-255)

Next Header
 Protocol Type
 Protocol ID (0-255)

Source Port Source Port Mask
 Destination Port Destination Port Mask
 ICMPv6 Type (0-255) Code (0-255)

IPv6 Address

Source Address Prefix Length
 Destination Address Prefix Length

Action

Priority (0-7)
 Replace Priority

Figure 4.105 - Add Access Rule – IPv6 ICMP

IPv6 Class (0-255): Specify 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:bfd4:0, use mask 128.

Action: Specify the ACL forwarding action matching the rule criteria. **Permit** forwards packets if all other ACL criteria are met. **Deny** drops packets if all other ACL criteria is met.

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'. Below this, it prompts the user to 'Please assign a sequence number to create a new rule.' There are two options: 'Sequence No. (1-65535)' with an input field, and 'Auto Assign' with a radio button. The 'Assign rule criteria' section has four tabs: 'L2 Header', 'Traffic Class', 'Next Header', and 'IPv6 Address'. The 'Traffic Class' tab is selected. Under this tab, there are several fields: 'Traffic Class' (checked), 'IPv6 Class (0-255)' (input field), 'Next Header' (checked), 'Protocol Type' (dropdown menu set to 'TCP'), 'Protocol ID (0-255)' (input field), 'Source Port' (input field), 'Source Port Mask' (input field), 'Destination Port' (input field), 'Destination Port Mask' (input field), 'ICMPv6 Type (0-255)' (input field), and 'Code (0-255)' (input field). The 'IPv6 Address' section has 'Source' and 'Destination' dropdowns set to 'Specify', each followed by 'Address' (input field) and 'Prefix Length' (input field). The 'Action' section has 'Action' (dropdown menu set to 'Permit'), 'Priority (0-7)' (input field), and 'Replace Priority' (checkbox). At the bottom right, there are 'Back' and 'Next' buttons.

Figure 4.106 - Add Access Rule – IPv6 TCP

Source Port: Specify 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: Specify 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:

ACL Configuration Wizard Safeguard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Rule

Please assign a sequence number to create a new rule.

Sequence No. (1-65535) Auto Assign

Assign rule criteria

L2 Header Traffic Class Next Header IPv6 Address

Traffic Class
IPv6 Class (0-255)

Next Header
Protocol Type
Protocol ID (0-255)

Source Port Source Port Mask

Destination Port Destination Port Mask

ICMPv6 Type (0-255) Code (0-255)

IPv6 Address

Source Address Prefix Length

Destination Address Prefix Length

Action

Priority (0-7)

Replace Priority

Back Next

Figure 4.107 - Add Access Rule – IPv6 UDP

Source Port: Specify 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: Specify 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.

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

ACL Configuration Wizard Safeguard

Access-List Assignment >> Select Packet Type >> Add Rule >> Apply Rule

Port Based

Which port(s) do you want to apply the Access-List?

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

Figure 4.108 - 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 4.109 - 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.



Figure 4.110 - ACL > ACL Access List

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

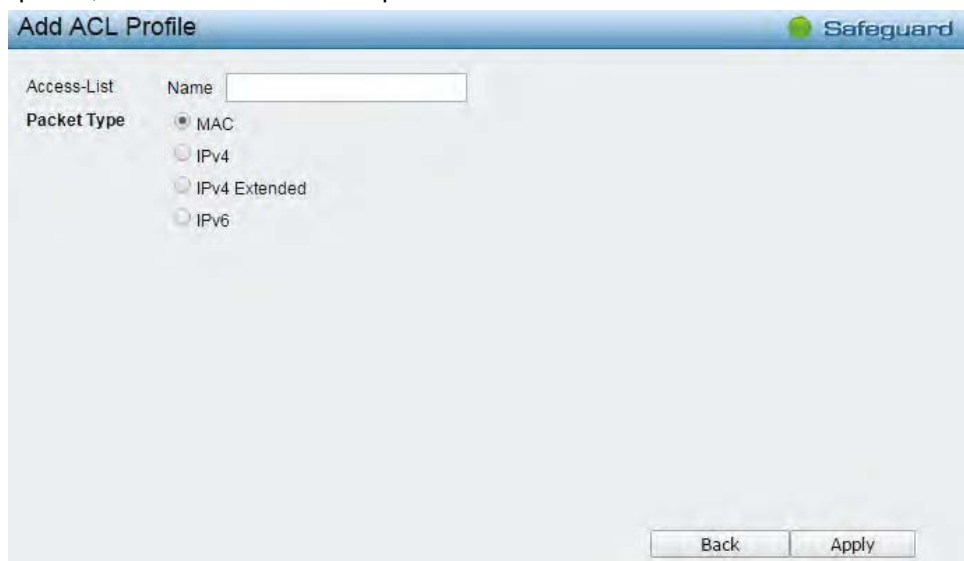


Figure 4.111 - ACL > ACL Access List – Add ACL Profile

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

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

To modify an existing rule, please click on the Sequence No. hyperlink.

Figure 4.112 - 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.

Figure 4.113 - ACL > ACL Access Group

Port: Specify 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 **Apply** to make the configurations take effects.

ACL > ACL Hardware Resource Status

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

Hardware Profile ID	Access-List Name	Consumed/Total Entries
1	IMPV4	2 / 1280
2	IMPV6	2 / 1280
3		0 / 1280
4		0 / 1280
5		0 / 1280
6		0 / 1280

Figure 4.114 - ACL > ACL Hardware Resource Status

PoE > PoE Global Settings (DES-1210-08P/28P only)

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

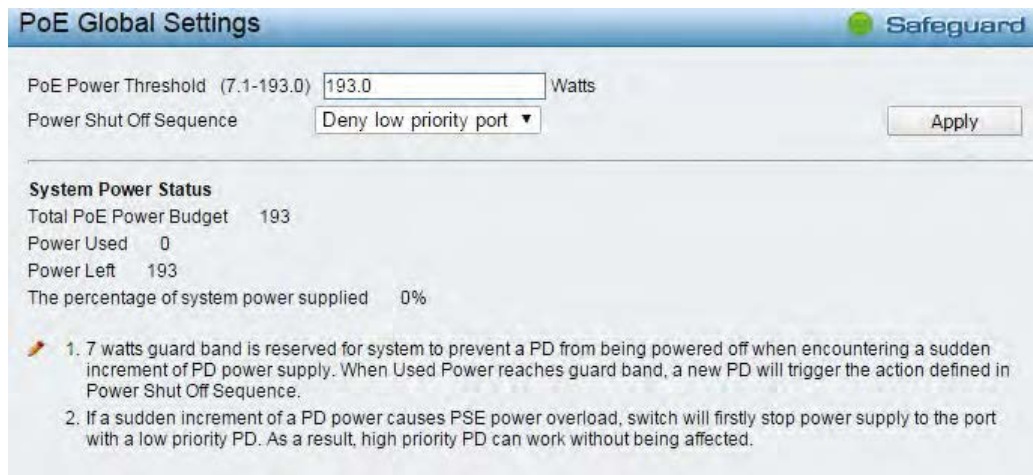


Figure 4.115 – PoE > PoE Global Setting

System Power Threshold: Manually configure the system power budget 7.1 ~ 193.0 watts for DES-1210-28P, 72 watts for DES-1210-08P.

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 **Apply** to make the configurations take effects.

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 (DES-1210-08P/28P only)

DES-1210-08P/28P supports Power over Ethernet (PoE) as defined by the IEEE specification. It supplies power to PD device up to 15.4W for all ports or 30W, meeting IEEE802.3af standards and pre-802.3at standards.

DES-1210-08P/28P works with all D-Link 802.3af or 802.3at capable devices. The Switch also works in PoE mode with all non-802.3af capable D-Link AP, IP Cam and IP phone equipment via the PoE splitter DWL-P50.

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

Class	Usage	Output power limit by PSE
0	Default	15.4W
1	Optional	4.0W
2	Optional	7.0W
3	Optional	15.4W
4	Reserved	30W

The PoE port table will display the PoE status including, Port Enable, Power Limit, Power (W), Voltage (V), Current (mA), Classification, Port Status. You can select **From Port / To Port** to control the PoE functions of a port. DES-1210-08P/28P 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: 1 To Port: 24 State: Enabled Time Range: N/A Priority: Normal Power Limit: Auto Watts

Refresh Apply

1. The port 1 to port 4 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.

2. The port 5 to port 24 can be set a power limit between 1W and 15.4W. Max power used by PSE: Class 1: 4W, Class 2: 7W, Class 3: 15.4W.

Port	State	Time Range	Priority	Power Limit	Power (W)	Voltage (V)	Current (mA)	Classification	Status
1	Enab...	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF
2	Enab...	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF
3	Enab...	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF
4	Enab...	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF
5	Enab...	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF
6	Enab...	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF
7	Enab...	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF
8	Enab...	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF
9	Enab...	N/A	Normal	Auto	0.0	0.0	0.0	N/A	POWER OFF

Figure 4.116 – 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**.

Power Limit: This function allows you to manually set the port power current limitation to be given to the PD. To protect the DGS-1210-28P 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).

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.

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 enabled. Select Enable and click **Apply** to enable the SNMP function.

Figure 4.117 – 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.

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.

Loopback Detection occurring / recovery: Information of occurring or 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.

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 4.118 – SNMP > SNMP > SNMP User

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

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

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

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

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

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

SNMP > SNMP > SNMP Group

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	Read View	Write View	Notify View	Security Model	Security Level	Delete
ReadOn...	ReadWr...	---	ReadWr...	v1	NoAuthNoPriv	Delete
ReadOn...	ReadWr...	---	ReadWr...	v2c	NoAuthNoPriv	Delete
ReadWr...	ReadWr...	ReadWr...	ReadWr...	v1	NoAuthNoPriv	Delete
ReadWr...	ReadWr...	ReadWr...	ReadWr...	v2c	NoAuthNoPriv	Delete

Figure 4.119 – SNMP > SNMP > SNMP Group

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

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

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

Security Model: Select the SNMP security model.

SNMPv1 - SNMPv1 does not support the security features.

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

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

Security Level: This function is only available when 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: Specify a SNMP group name for users that can receive SNMP trap messages generated by the Switch's SNMP agent.

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

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 4.120 – 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: Specify 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	User Name	Delete
public	ReadOnly	Delete
private	ReadWrite	Delete

Figure 4.121 – SNMP > SNMP > SNMP Community

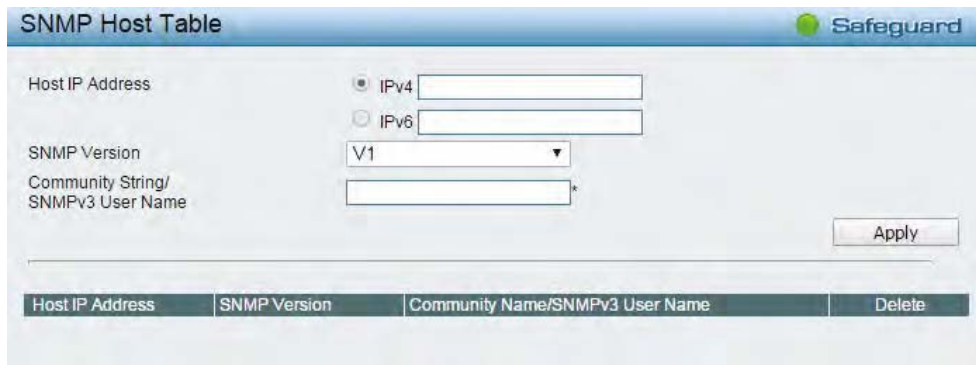
Community Name: Name of the community string

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

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

SNMP > SNMP > SNMP Host

This page is to configure the SNMP trap recipients.



The screenshot shows the 'SNMP Host Table' configuration page. It features a 'Safeguard' logo in the top right corner. The main configuration area includes:

- Host IP Address:** Two radio buttons for 'IPv4' (selected) and 'IPv6', each followed by a text input field.
- SNMP Version:** A dropdown menu currently set to 'V1'.
- Community String/SNMPv3 User Name:** A single text input field.
- An 'Apply' button is located to the right of the input fields.

 Below the configuration area is a table with the following columns: 'Host IP Address', 'SNMP Version', 'Community Name/SNMPv3 User Name', and 'Delete'.

Figure 4.122 – SNMP > SNMP > SNMP Host

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

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

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

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.



The screenshot shows the 'SNMP Engine ID' configuration page. It features a 'Safeguard' logo in the top right corner. The main configuration area includes:

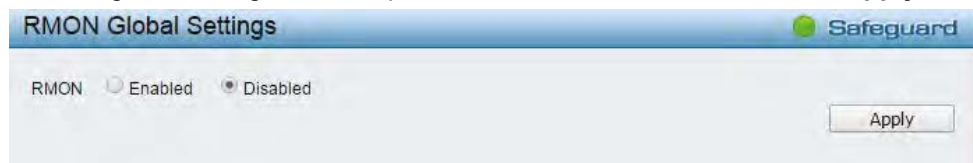
- Engine ID:** A text input field containing the hexadecimal value '4445532a313231302d32389c643438028'.
- 'Default' and 'Apply' buttons are located to the right of the input field.
- A note at the bottom states: 'Engine ID length is 10-64, the accepted character is from 0 to F.'

Figure 4.123 – SNMP > SNMP > SNMP Engine ID

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

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.



The screenshot shows the 'RMON Global Settings' configuration page. It features a 'Safeguard' logo in the top right corner. The main configuration area includes:

- RMON:** Two radio buttons, 'Enabled' and 'Disabled', with 'Disabled' selected.
- An 'Apply' button is located to the right of the radio buttons.

Figure 4.124 – 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.



The screenshot shows the 'RMON Ethernet Statistics Settings' configuration page. It features a 'Safeguard' logo in the top right corner. The main configuration area includes:

- Index (1-65535):** A text input field with an asterisk indicating mandatory data.
- Port:** A text input field with an asterisk indicating mandatory data.
- Owner:** A text input field.
- A note below the input fields states: '* Indicates mandatory data.'
- 'Refresh' and 'Add' buttons are located to the right of the input fields.

 Below the configuration area is a table with the following columns: 'Index', 'Port', 'Drop Events', 'Cdebs', 'Packets', 'Broadcast Packets', 'Multicast Packets', 'Owner', and 'Delete'.

Figure 4.125 – SNMP > RMON > RMON Statistics

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 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.

Figure 4.126 – SNMP > RMON > RMON History

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 **Add** to make the configurations take effects.

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.

Figure 4.127 – SNMP > RMON > RMON Alarm

The configuration contains the following fields:

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

Variable: Specify the selected MIB variable value.

Rising Threshold (0 ~ 2³¹-1): 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.

Figure 4.128 – SNMP > RMON > RMON Event

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 Statistics screen displays the status of each port packet count.

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	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	3707	4588	0	0

Figure 4.129 – Monitoring > 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.

TX		RX	
OutOctets	2441740	InOctets	1087431
OutUcastPkts	3712	InUcastPkts	2758
OutNUcastPkts	144	InNUcastPkts	1982
OutErrors	0	InDiscards	0
LateCollisions	0	InErrors	0
ExcessiveCollisions	0	FCSErrors	0
InternalMacTransmitErrors	0	FrameTooLongs	0
		InternalMacReceiveErrors	0

Figure 4.130 – 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 of the copper cable quality. It rapidly determines the type of cable errors occurred in the cable.

Select a port and then click the **Test Now** button to start the diagnosis.

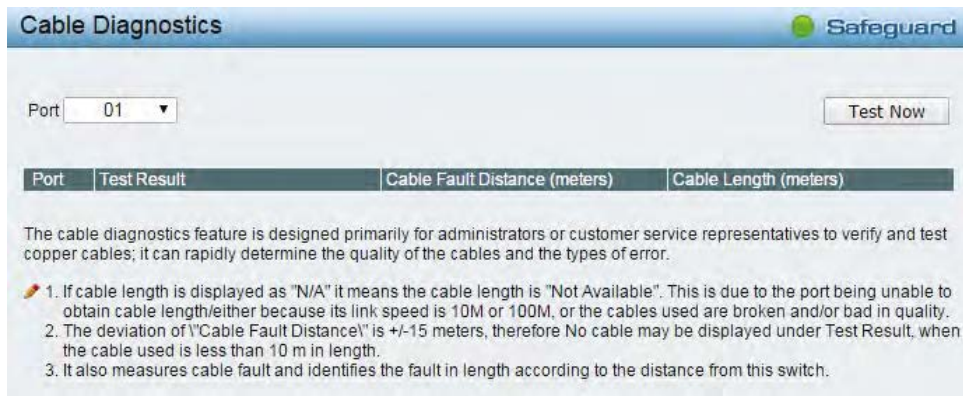


Figure 4.131 – Monitoring > Cable Diagnostics

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.
- **Mismatched** means some other errors occurred during cable diagnostics. Please select the same port and test again.
- **Line Driver:** The high impedance is detected. Out scenario is the cable plug to a power down link partner.

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 and >100 meters.



NOTE: Cable length detection is effective on Gigabit ports only. The cable length reported is the length is where Short/Open/Impedance mismatch/Line driver is detected. The cable length estimation may have around +/-15 meter inaccuracy if user use more than 30 meter cable for testing. By the way, if use less than 30 meter cable, it may have +/-20 meter inaccuracy.



NOTE: If the port state of DES-1210-08P just changed from link up to link down, please wait 5 seconds to execute the cable diagnostic test or the test result might be incorrect.

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.

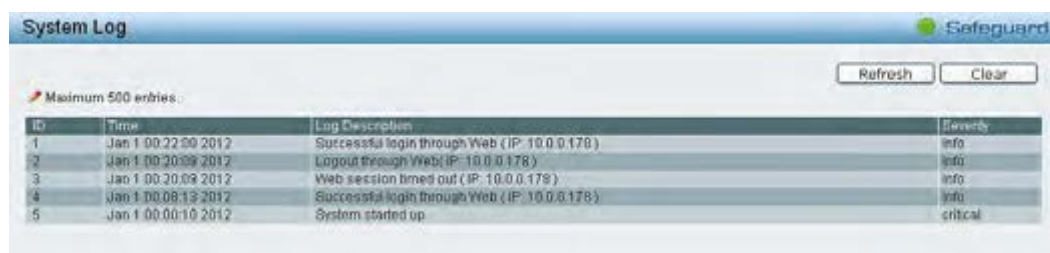


Figure 4.132 – Monitoring > System Log

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.

5 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 (**DES-1210-28**):

```
DES-1210-28 login: admin
Password:
DES-1210-28>
```

Figure 5.1 – Command Prompt

The user session is automatically terminated if idle for the login timeout period. The default login timeout period is 5 minutes. To change the login timeout session please refers to chapter 5.

CLI Commands:

There are a number of helpful features included in the CLI. Enter the **?** command will display a list of commands.

```
DES-1210-28> ?
USEREXEC commands :
  config account admin password <passwd>
  config ipif System { ipaddress <ip-address> <subnet-mask> gateway <gw-
address>
  | dhcp | bootp}
  config ipif System { ipv6 ipv6address <ipv6networkaddr> |
dhcpv6_client {enabl
e | disable}}
  create ipv6route default <ipv6addr>
  debug info
  delete ipv6route default
  download { firmware_fromTFTP | cfg_fromTFTP} {<ipaddr>|<ipv6addr>}
<path_filename>
  logout
  ping <ip_addr>
  ping6 <ipv6addr>
  reboot
  reset config
  save
  show ipif
  show switch
  upload { firmware_toTFTP | cfg_toTFTP} {<ipaddr>|<ipv6addr>}
<path_filename>
DES-1210-28>
```

Figure 5.2 – The ? command

download

The **download** command is used to download and install new firmware or a Switch configuration file from a TFTP server.

Syntax

```
download {firmware_fromTFTP | cfg_fromTFTP} {<ipaddr>|<ipv6addr>}
<path_filename>
```

Parameters

Parameter	Description
firmware_fromTFTP	Download and install new firmware on the Switch from a TFTP server.
cfg_fromTFTP	Download a switch configuration file from a TFTP server.
<ipaddr> <ipv6addr>	The IPv4 or IPv6 address of the TFTP server.
path_filename	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.



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

upload

The **upload** command is used to upload the firmware file or a Switch configuration file to a TFTP server.

Syntax

```
upload {firmware_toTFTP | cfg_toTFTP} {<ipaddr> | <ipv6addr>}
<path_filename>
```

Parameters

Parameter	Description
firmware_toTFTP	Upload the firmware on the Switch from a TFTP server.
cfg_toTFTP	Specifies that the Switch's current settings will be uploaded to the TFTP server.
<ipaddr> <ipv6addr>	The IPv4 or IPv6 address of the TFTP server.
path_filename	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.

config ipif system

The **config ipif system** command sets the IP address of the switch.

Syntax

```
config ipif system {ipaddress <ip-address> <subnet-mask> gateway <gw-
address> | dhcp | bootp}
```

```
config ipif system {ipv6 ipv6address <ipv6networkaddr> | dhcpv6_client
[enable | disable]}
```

Parameter

Parameter	Description
ipaddress <ip-address> <subnet-mask>	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).
gateway <gw-address>	The IP address of the router or gateway.
dhcp	Allows the selection of the DHCP protocol for the assignment of an IP

	address to the Switch's System IP interface.
bootp	The BOOTP protocol allows IP addresses, network masks, and default gateways to be assigned by a central BOOTP server.
ipv6 ipv6address <ipv6networkaddr>	Use this parameter to statically assign an IPv6 address 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.
dhcpv6_client[enable disable]	Specify the DHCPv6 client to be disabled or enabled.

Example

```
DES-1210-28> config ipif system ipaddress 172.17.5.214 255.255.255.0
gateway 172.17.5.214
% The IP setting mode change to static will cause CLI disconnect.
```

Figure 5.3 – The config ipif system command

logout

This command closes the current connection.

Syntax

logout

Example

```
DES-1210-28> logout
```

Figure 5.4 – The logout command

ping

This 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.

Syntax

ping [<ipaddr> | <ipv6addr>]

Parameter

Parameter	Description
<ipaddr> <ipv6addr>	The IPv4 or IPv6 address of the target station.

Example

```
DES-1210-28> 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
DES-1210-28>
```

Figure 5.5 – The ping command

reboot

This command reboots the system. All network connections are terminated and the boot code executes.

Syntax**reboot****Example**

```
DES-1210-28> reboot
% Device will reboot, please wait a few minutes to re-login.
DES-1210-28>
```

Figure 5.6 – The reboot command**reset**

All configurations will be reset to the default settings.

Syntax**reset config****Example**

```
DES-1210-28> reset config
% Device will reboot after reset configuration successfully.
DES-1210-28>
```

Figure 5.7 – The reset config command**show ipif**

The command displays the current IP address of the switch.

Syntax**show ipif****Example**

```
DES-1210-28> show ipif
IP Setting Mode           : Static
IP Address                : 10.90.90.90
Subnet Mask               : 255.0.0.0
Default Gateway           : 0.0.0.0

DES-1210-28>
```

Figure 5.8 – The show ipif command**show switch**

The command displays the status of the switch.

Syntax**show switch****Example**

```
DES-1210-28> show switch
System name               :
System Contact            :
System Location           :
System up time            : 0 days, 6 hrs, 32 min, 17 secs
System Time               : 07/07/2012 06:32:19
System hardware version   : B1
System firmware version   : 3.10.003
System boot version       : 1.00.008
System Protocol version   : 2.001.004
System serial number      : 1MB1733K0000A
MAC Address               : 00-18-E7-48-85-50

DES-1210-28>
```

Figure 5.9 – The show switch command

config account admin password

The command sets the administrator password.

Syntax

```
config account admin password <passwd>
```

Parameter

Parameter	Description
<passwd>	The new password of the administrator.

Example

```
DES-1210-28> config account admin password admin
DES-1210-28>
```

Figure 5.10 – The config account admin password command

save

The command saves the configuration changes to the memory.

Syntax

```
save
```

Example

```
DES-1210-28> save
Building configuration ...
[OK]
DES-1210-28>
```

Figure 5.11 – The save command

debug info

This command displays the ARP table and MAC FDB of the Switch.

Syntax

```
debug info
```

Example

```
DES-1210-28> debug info
% ARP table :

Address          Hardware Address  Type  Interface  Mapping
-----
172.17.5.85      00:18:8b:bf:75:30 ARPA  vlanMgmt   Dynamic
172.17.5.254     00:19:5b:14:3d:c4 ARPA  vlanMgmt   Dynamic

% MAC table :
s
Vlan   Mac Address          Type    Ports
-----
1      00:00:00:00:00:26    Learnt  Fa0/4
1      00:00:48:bf:f3:01    Learnt  Fa0/4
1      00:03:1b:66:66:5c    Learnt  Fa0/4
1      00:03:64:00:01:23    Learnt  Fa0/4

Total Mac Addresses displayed: 4
DES-1210-28>
```

Figure 5.12 – The debug info command

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 to help solving network bottlenecks that frequently develop 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. And with expected advances in the coming years in silicon technology and digital signal processing that will enable Gigabit Ethernet to eventually operate over unshielded twisted-pair (UTP) cabling, outfitting your network with a powerful 1000-Mbps-capable backbone/server connection which will create a flexible foundation for the next generation of network technology products.

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

Hardware Specifications

Key Components / Performance

- › Switching Capacity:
 - DES-1210-08P: 1.6Gbps
 - DES-1210-28/28P: 12.8Gbps
 - DES-1210-52: 17.6Gbps
- › Max. Forwarding Rate
 - DES-1210-08P: 1.19Mpps
 - DES-1210-28/28P: 9.5Mpps
 - DES-1210-52: 13.1Mpps
- › Forwarding Mode: Store and Forward
- › Packet Buffer memory:
 - DES-1210-08P/28/28P: 4.1 Mbits
 - DES-1210-52: 12.1Mbits
- › DDRIII for CPU: 128M Bytes
- › Flash Memory: 16M Bytes

Port Functions

- › 24 or 48 10/100BaseT ports comply with the following standards:
 - IEEE 802.3
 - IEEE 802.3u
 - Supports Half/Full-Duplex operations
 - Auto-negotiation
 - Auto MDI/MDIX
 - IEEE 802.3x Flow Control support for Full-Duplex mode
- › 4 1000Base-T ports of DES-1210-28/28P/52 comply with the following standards:
 - IEEE 802.3
 - IEEE 802.3u
 - IEEE 802.3ab
 - Supports Full-Duplex operations
 - IEEE 802.3x Flow Control support for Full-Duplex mode, back pressure when Half-Duplex mode, and Head-of-line blocking prevention
- › 2 combo SFP ports of DES-1210-28/28P/52 comply with the following standards:
 - IEEE 802.3z
 - Supports Full-Duplex operations
- › SFP transceivers supported
 - 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)

- DEM-302S-LX (1000Base-LX, Single-mode, 2km)
- DEM-210 (100BASE-FX, 15km)
- DEM-211 (100BASE-FX, 2km)

WDM Transceivers Supported:

- 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)
- DEM-220T (100Base-BX, TX-1550/RX-1310nm, 20km)
- DEM-220R (100Base-BX, TX-1310/RX-1550nm, 20km)

Physical & Environment

- › AC input, 100~240 VAC, 50/60Hz, internal universal power supply
- › Acoustic Value:
 - DES-1210-08P/28/52: 0dB (Fan-less)
 - DES-1210-28P : 49.7dB(A) (3 pcs Smart Fan)
- › Operation Temperature:
 - DES-1210-08P: -5~45°C
 - DES-1210-28/28P/52: -5~50°C
- › Storage Temperature -40~70°C
- › Operation Humidity:
 - DES-1210-08P/28/28P/52: 10%~95% RH
- › Storage Humidity:
 - DES-1210-08P/28/28P/52: 5%~95% RH

Emission (EMI) Certifications

- › FCC class A
- › CE Class A
- › VCCI Class A
- › C-Tick Class A

Safety Certifications

- › cUL, LVD

Features

L2 Features

- › MAC address table:
 - DES-1210-08P/28/28P: 8K
 - DES-1210-52:16K
- › IGMP snooping: supports 256 multicast group

- › 802.3x when full duplex
- › 802.1D Spanning Tree
- › 802.1w Rapid Spanning Tree
- › Loopback Detection
- › IEEE 802.3ad Link Aggregation:
 - › - DES-1210-08P: Up to 4 groups per device, up to 8 ports per group
 - › - DES-1210-28/28P: Up to 8 groups per device, up to 8 ports per group
 - › - DES-1210-52: Up to 16 groups per device, up to 8 ports per group
- › Port mirroring
- › LLDP
- › Multicast Filtering
- › Jumbo Frame: Up to 9 KB
- › IGMP Snooping
 - Supports IGMP v1, v2 and v3 snooping
 - Supports at least 64 static multicast addresses

VLAN

- › 802.1Q VLAN standard (VLAN Tagging)
- › Up to 256 static VLAN groups
- › Asymmetric VLAN
- › Management VLAN
- › Auto Surveillance VLAN
- › Auto-Voice VLAN

ACL

- › Max 50 ingress ACL profiles, 1280 ingress ACL rules
- › Supports following ACL policy packet contents:
 - 802.1p priority
 - VLAN
 - MAC address
 - Ethernet Type
 - IPv4 and IPv6 address
 - LLC mask
 - DSCP
 - Protocol type
 - TCP/UDP port number
 - IPv6 Traffic Class

QoS (Quality of Service)

- › 802.1p priority, DSCP priority queue mapping
- › Up to 8 queues per port
- › Supports Strict / WRR mode in queue handling
- › Bandwidth Control

AAA

- › 802.1X:
 - Supports IPv4/IPv6 RADIUS Server
 - Supports Port-based access Control

- Supports EAP, OTP, TLS, TTLS and PEAP
- Supports MD5 authentication
- Supports 802.1X session timeout attribute
- › Guest VLAN:
 - Port-based Guest VLAN
- › RADIUS:
 - Support IPv4/IPv6 RADIUS server
 - Maximum is 5 RADIUS servers

Security

- › Port Security: support 64 MACs per port
- › IP and MAC ACL
- › Broadcast Storm Control
- › Traffic Segmentation
- › D-Link Safeguard Engine
- › Trusted Host
- › DHCP Server Screening: maximum 5 entries
- › SSLv1/v2/v3 (IPv4/v6)
- › SShHv2 (IPv4/v6)
- › DoS attack Prevention
- › Smart Binding

OAM

- › Cable Diagnostics
- › Factory Reset

Management

- › IPv4/IPv6 Management: HTTP, Telnet, SSL, SNMP
- › D-Link proprietary CLI
- › D-Link Discovery Protocol
- › DHCP Auto Configuration
- › Firmware backup or restore via HTTP
- › RMONv1, Group 1, 2, 3, 9
- › Reset and reboot

D-Link Green Technologies

- › Power saving by cable length
- › Power saving by link status
- › Power saving by Time-Based PoE
- › Power saving by LED Shut-Off
- › Power saving by Port Shut-Off
- › Power saving by System Hibernation

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).

Copyright and Trademarks

Information in this document is subjected to change without notice.

© 2016 D-Link Corporation. All rights reserved.

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

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

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

FCC Warning

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

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

CE EMI Class A Warning

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

VCCI Warning

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

BSMI Notice

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

Safety Compliance

Warning: Class 1 Laser Product.

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

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

Networks pluggable optical modules meet the following regulatory requirements:

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

D-Link[®]
Building Networks for People